معاونت آموزش و پژوهش
اداره کل آموزش
آشنایی با تعاریف سیستم های
نرم افزاری و شبکه
تحقیق و گردآوری : غلامرضا امیریان
Network Security
جلد سه
امنیت شبکه
واحد طراحی و ارزشیابی
بخش فناوری آموزشی
Tel : 22014746
Fax : 22014684
Email : training-dept@iribu.com
Application
Presentation
Session
Transport
Network
Data
Physical

بخش پنجم : تهدیدهای امنیتی و روشهای مقابله با آنها **صفحه**

- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۱ ..... ۸
- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۲ ..... ۱۲
- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۳ ..... ۱۶
- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۴ ..... ۲۴
- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۵ ..... ۲۸
- رویکرد علمی و امنیت شبکه لایه بندی شده قسمت ۶ ..... ۳۴
- مقدمه ای بر تشخیص نفوذ (Intrusion Detection)..... ۳۷
- مقایسه تشخیص نفوذ و پس گیری از نفوذ..... ۴۲
- حملات DOS ۴۷
- عدم پذیرش سرویس ۱..... ۵۱
- عدم پذیرش سرویس۲ انواع حملات..... ۵۶
- عدم پذیرش سرویس۳ روش های مقابله..... ۶۴
- روش معمول حمله به کامپیوتر (۱) ۷۱
- روش معمول حمله به کامپیوتر (۲) ۷۶
- ازکوکی چه می دانید؟..... ۸۲
- کوکی ها و مسائل امنیتی..... ۸۸
- محتویات فعال و کوکی ۹۴
- داده های حساس..... ۹۸
- SPAM..... ۱۰۷
- SPYWARE..... ۱۱۱
- نرم افزارهای جاسوسی و مقابله با آنها (۱) ۱۱۵

- نرم افزارهای جاسوسی و مقابله با آنها (۲) ۱۲۰
- نرم افزارهای جاسوسی و مقابله با آنها (۳) ۱۲۴
- حملات مبتنی بر مهندسی اجتماعی..... ۱۳۰
- شناسائی مزاحم کامپیوتری..... ۱۳۴
- ضمائم نامه های الکترونیکی..... ۱۳۸
- برنامه های IM و Chat..... ۱۴۱
- انتخاب و محافظت از کلمات عبور..... ۱۴۵
- سیاست های امنیتی..... ۱۵۱
- سه محور اصلی در کنترل دسترسی در شبکه ۱۵۵
- روشهای پنهان سازی سرورهای وب برای افزایای ایمنی..... ۱۶۰
- بستن درگاه های بدون استفاده از حفاظت ۱۶۷
- امضای دیجیتال..... ۱۷۲
- بیومتریک و تجهیزات مربوطه قسمت اول ۱۷۵
- بیومتریک و تجهیزات مربوطه قسمت دوم..... ۱۸۰
- BCC و ضرورت استفاده از آن..... ۱۸۴
- مقدمه ای بر شبکه خصوصی مجازی(VPN) ۱۸۷
- مقدمه ای بر .IPSec ۱۹۱
- امنیت در شبکه های بیسیم ۱..... ۱۹۵
- امنیت در شبکه های بیسیم ۲..... ۱۹۹
- امنیت در شبکه های بیسیم۳..... ۲۰۳
- امنیت در شبکه های بیسیم۴..... ۲۰۷
- امنیت در شبکه های بیسیم۵..... ۲۱۱
- امنیت در شبکه های بیسیم۶..... ۲۱۵
- امنیت در شبکه های بیسیم۷..... ۲۱۹

- ۱۰ نکته برای حفظ امنیت..... ۲۲۳

بخش ششم : رمزنگاری Encryption

صفحه

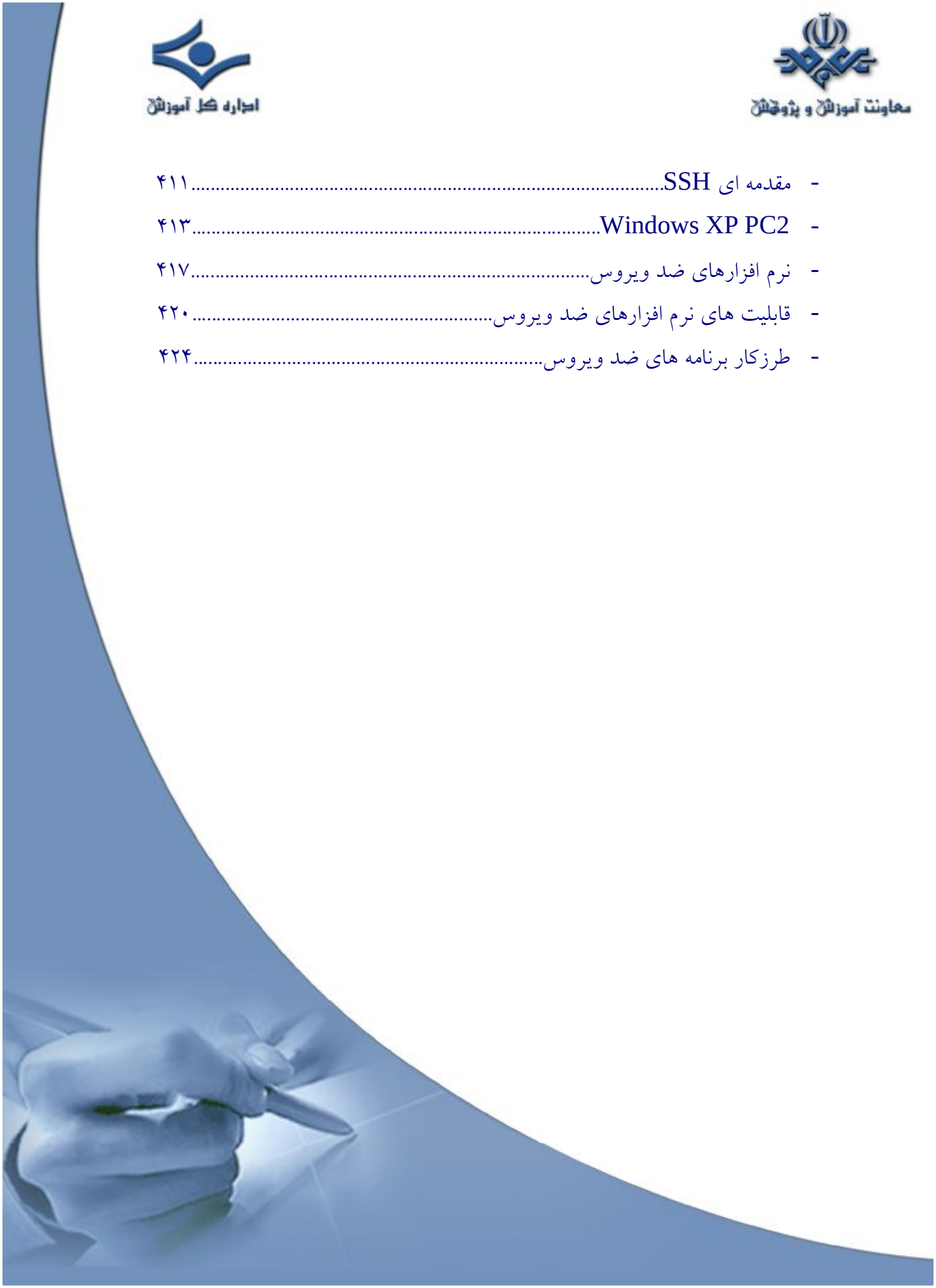
- رمزنگاری ۲۳۰
- کلیدها در رمزنگاری..... ۲۳۶
- رمزنگاری اطلاعات، حفاظت از اطلاعات حساس..... ۲۴۰
- شکستن کلیدهای رمزنگاری..... ۲۴۸
- پروتکل های انتقال فایل امن..... ۲۵۱
- رمزنگاری در پروتکل های انتقال..... ۲۵۶

بخش هفتم : Internet Security

- حفاظت کامپیوترقبل ازاتصال به اینترنت ۱..... ۲۶۳
- حفاظت کامپیوترقبل ازاتصال به اینترنت ۲..... ۲۶۷
- حفاظت کامپیوترقبل ازاتصال به اینترنت ۳..... ۲۷۳
- امنیت تجهیزات شبکه ۲۷۸
- امنیت در اینترنت..... ۲۹۰
- محافظت در مقابل خطرات ایمیل ۱..... ۲۹۳
- محافظت در مقابل خطرات ایمیل ۲..... ۲۹۹

- پراکسی سرور ۳۰۴
- کاربرد پراکسی در امنیت شبکه ۱..... ۳۰۹
- کاربرد پراکسی در امنیت شبکه ۲..... ۳۱۴
- کاربرد پراکسی در امنیت شبکه ۳..... ۳۱۹
- فایروال قسمت اول..... ۳۲۶
- فایروال قسمت دوم..... ۳۳۳
- Ethereal .Tool securety قسمت اول..... ۳۴۰
- Ethereal قسمت دوم..... ۳۴۴
- Ethereal قسمت سوم..... ۳۴۹
- Tool securety Super scan قسمت اول..... ۳۵۶
- Super scan قسمت دوم..... ۳۶۳
- WinDump قسمت اول..... ۳۶۸
- WinDump قسمت دوم..... ۳۷۳
- Honypot قسمت (۱) ۳۷۸
- Honypot قسمت (۲)..... ۳۸۲
- keylogger ابزاری برای جاسوسی..... ۳۸۸
- آشنائی با PGP..... ۳۹۳
- Nessus پویش گره ساده و قدرتمند..... ۳۹۶
- SNORT نمونه ای از یک ابزار تشخیص نفوذ شبکه ای..... ۴۰۲
- Retina Network Security Scanner..... ۴۰۶
- حفاظت شخصی Zone Alarm..... ۴۰۸

- مقدمه ای SSH..... ۴۱۱
- Windows XP PC2..... ۴۱۳
- نرم افزارهای ضد ویروس..... ۴۱۷
- قابلیت های نرم افزارهای ضد ویروس..... ۴۲۰
- طرزکار برنامه های ضد ویروس..... ۴۲۴



بخش پنجم

تهدیدهای امنیتی و روشهای مقابله با آنها

رویکردی عملی به امنیت شبکه لایه بندی شده قسمت (۱)

مقدمه

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. دربسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.

در این قسمت رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد.

رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد.

۱- پیرامون

۲- شبکه

۳- میزبان

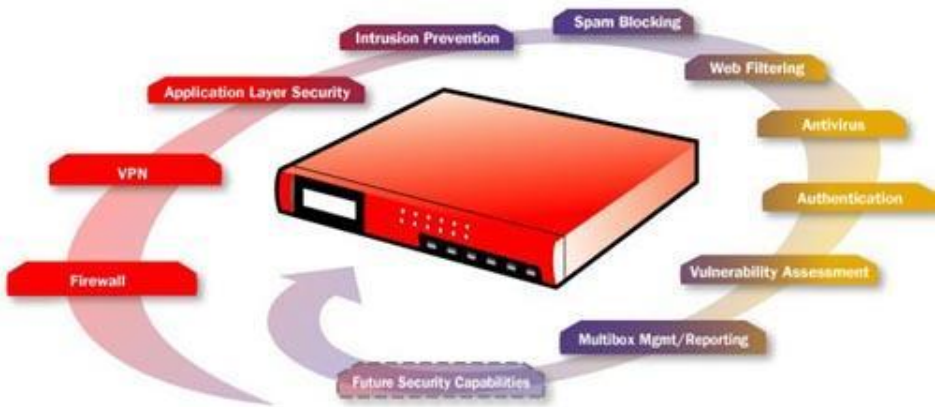
۴- برنامه کاربردی

۵- دیتا

و یک دید کلی از ابزارها و سیستمهای امنیتی گوناگون که روی هریک عمل می کنند، ارائه می شود. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک

رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. مخاطبان این سلسله مقالات متخصصان فناوری اطلاعات، مدیران تجاری و تصمیم گیران سطح بالا هستند.

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.



افزودن به ضریب عملکرد هکرها

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید.

تکنولوژی های بحث شده در این سری مقالات مجموعاً رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی شما را به نمایش می گذارند. در یک دنیای ایده آل، شما بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم هایی که بحث می کنیم خواهید داشت. اما متأسفانه در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه تان را ارزیابی کنید – چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره – و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

مدل امنیت لایه بندی شده

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. این تکنولوژی ها با جزئیات بیشتر در قسمتهای بعدی مورد بحث قرار خواهند گرفت.

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	رمزنگاری کنترل دسترسی/ تایید هویت کاربر

در قسمت قبل به لایه های این نوع رویکرد به اختصار اشاره شد. طی این قسمت و قسمت بعد به هریک از این لایه ها می پردازیم.

سطح ۱: امنیت پیرامون

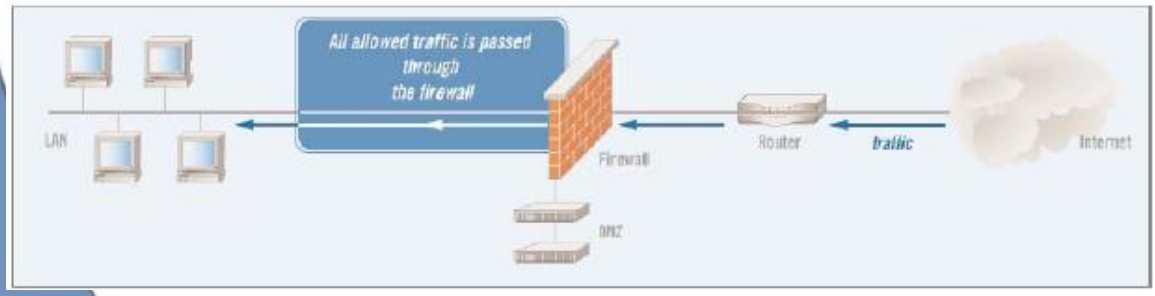
منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (demilitarized zone) شناخته میشود. DMZ معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها در DMZ می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد.

پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست.

تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

- **فایروال** ـ معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳- نقطه پایانی VPN. فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN (که بعداً بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.
- **آنتی ویروس شبکه** ـ این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

- **VPN**ـ یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. VPN اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.



مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند. بعضی از فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

ملاحظات

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

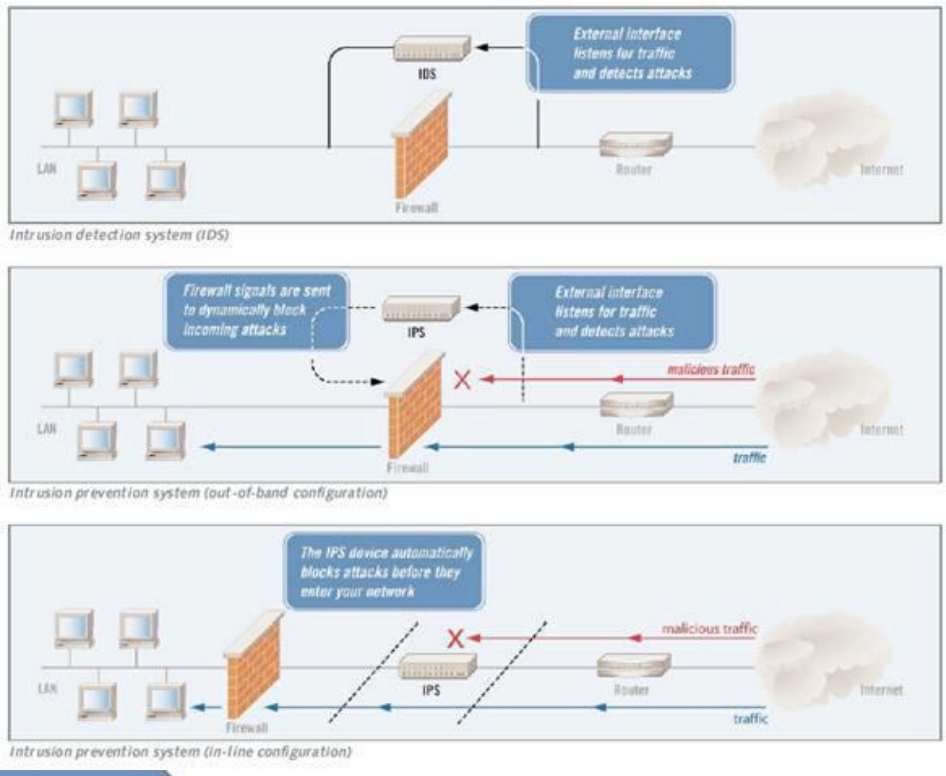
در قسمت قبلی به اولین لایه که لایه پیرامون است، اشاره شد، در این قسمت به لایه امنیت شبکه می پردازیم.

سطح ۲- امنیت شبکه

سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل میشوند.تکنولوژی های ذیل امنیت را درسطح شبکه برقرارمی کنند:

- **IDS ها (سیستم های تشخیص نفوذ) و IPSها (سیستم های جلوگیری از نفوذ)** ـ تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و

بصورت خودکار ترافیک آسیب رسان را مسدود می کنند. IDSها و IPSها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPSها در هسته خود یک IDS دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند. پیکربندی های IDS و IPS استاندارد در شکل نشان داده شده اند:



Intrusion detection system (IDS)

Intrusion prevention system (out-of-band configuration)

Intrusion prevention system (in-line configuration)

مدیریت آسیب پذیری – سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲) روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی VA (تخمین آسیب پذیری) نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید.

همچنانکه از نامش برمی آید، سیستم مدیریت آسیب پذیری شامل ویژگیهایی است که روند بازسازی را مدیریت می کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می کند.

- **تابعیت امنیتی کاربر انتهایی** – روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند،

رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم های ناامن کارمندان و ابزارهای VPN و RAS می گیرد.

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

- **کنترل دسترسی\تأیید هویت** – کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

نکته: در این سلسله مباحث، به کنترل دسترسی و تأیید هویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد. اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

مزایا

تکنولوژی های IDS، IPS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاءدادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید.

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچانکه پدیده های اخیر چون Mydoom، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

معایب

IDSها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان false positives نیز شناخته می شوند. در حالیکه IDS ممکن است که یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDS باید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند.

سطح خودکار بودن در IPSها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستمهایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود.

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند.

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند. برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد. چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد.

ملاحظات

موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS ، مدیریت آسیب پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصالی بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد.

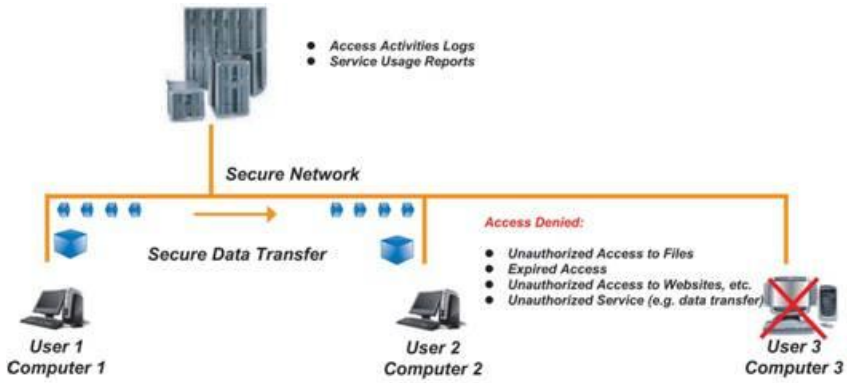
وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

رویکردی عملی به امنیت شبکه لایه بندی شده قسمت (۴)

در قسمت قبل به دومین لایه که لایه شبکه است، اشاره شد، در این قسمت به لایه میزبان به عنوان سومین لایه می پردازیم.

سطح ۳- امنیت میزبان

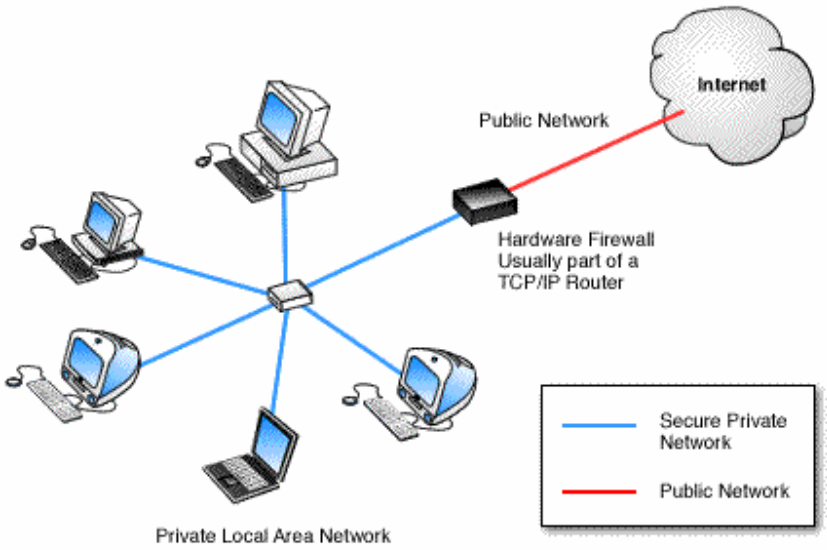
سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.



تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

- **IDS در سطح میزبان** ـ IDSهای سطح میزبان عملیاتی مشابه IDSهای شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDSهای سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.
- **VA (تخمین آسیب پذیری) سطح میزبان** – ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پویش می کنند. دقت آنها نسبتا بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، درصورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.
- **تابعیت امنیتی کاربر انتهایی** – روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.

- **آنتی ویروس** – هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند، لایه اضافه ای برای محافظت فراهم می کنند.
- **کنترل دسترسی\تصدیق هویت**– ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.



مزایا

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند.

دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

معایب

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصب شان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

ملاحظات

بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود.

رویکردی عملی به امنیت شبکه لایه بندی شده قسمت (۵)

در قسمت قبل به سومین لایه که لایه میزبان است، اشاره شد. در این قسمت به لایه برنامه کاربردی بعنوان چهارمین لایه و لایه دیتا بعنوان پنجمین لایه می پردازیم.

سطح ۴- امنیت برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

- **پوشش محافظ برنامه** – از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شـــفاف است و با درجـــه بالایی با سیستم یکپارچه می شود.

یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

- **کنترل دسترسی/تصدیق هویت**– مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.
- **تعیین صحت ورودی** – ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در

جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربرمی تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!

به عنوان مثال، یک فرم وبی با یک بخش zip code را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:

- کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «insert»، باید بررسی و در صورت نیاز مسدود شوند.
- فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

مزایا

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

معایب

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

ملاحظات

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

سطح ۵ - امنیت دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا

حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

- **رمزنگاری** – طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/ رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل PKI، PGP و RSA هستند.
- **کنترل دسترسی / تصدیق هویت** – مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

مزایا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

معایب

بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

ملاحظات

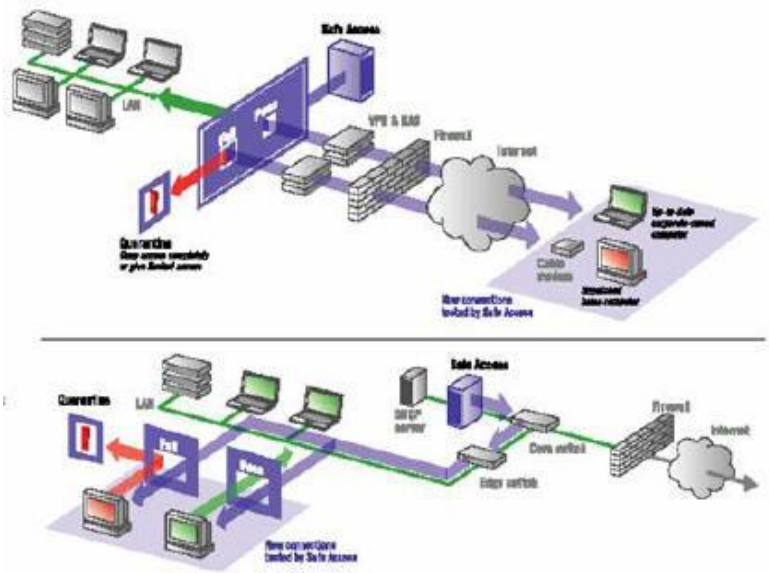
رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری بایـــد برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است.

رویکردی عملی به امنیت شبکه لایه بندی شده قسمت (٦) : جمع بندی

در **قسمت های** قبل (۱، ۲، ۳، ۴ و ۵) به لایه های مختلف در امنیت شبکه لایه بندی شده پرداختیم. در این شماره به اختصار به جمع بندی مباحث فوق می پردازیم.

دفاع در مقابل تهدیدها و حملات معمول

قسمت گذشته نشان می دهد که چگونه رویکرد امنیت لایه بندی شده در مقابل تهدیدها و حملات معمول از شبکه شما محافظت می کند و نشان می دهد که چگونه هر سطح با داشتن نقشی کلیدی در برقراری امنیت شبکه جامع و مؤثر، شرکت می کند.



بعضی حملات معمول شامل موارد زیر می شود:

- **حملات به وب سرور** ـ حملات به وب سرور دامنه زیادی از مشکلاتی را که تقریباً برای هر وب سرور ایجاد می شود، در برمی گیرد. از دستکاری های ساده در صفحات گرفته تا در اختیار گرفتن سیستم از راه دور و تا حملات DOS. امروزه حملات به وب سرور یکی از معمول ترین حملات هستند. Code Red و Nimda به عنوان حمله کنندگان به وب سرورها از شهرت زیادی! برخوردارند.
- **بازپخش ایمیل ها بصورت نامجاز** ـ سرورهای ایمیلی که بصورت مناسب پیکربندی نشده اند یک دلیل عمده برای ارسال هرزنامه ها بشمار می روند. بسیاری از شرکت های هرزنامه ساز در پیدا کردن این سرورها و ارسال صدها و هزاران پیام هرزنامه به این سرورها، متخصص هستند.
- **دستکاری میزبان دور در سطح سیستم** ـ تعدادی از آسیب پذیری ها، یک سیستم را از راه دور در اختیار حمله کننده قرار می دهند. بیشتر این نوع کنترل ها در سطح سیستم است و به حمله کننده اختیاراتی برابر با مدیر محلی سیستم می دهد.
- **فراهم بودن سرویس های اینترنتی غیرمجاز** ـ توانایی آسان بکارگیری یک وب سرور یا سرویس اینترنتی دیگر روی یک کامپیوتر ریسک افشای سهوی اطلاعات را بالا می برد. اغلب چنین سرویس هایی کشف نمی شوند، در حالی که در شعاع رادار دیـــگران قرار می گیرند!
- **تشخیص فعالیت ویروسی** ـ در حالی که برنامه ضدویروس در تشخیص ویروس ها مهارت دارد، این نرم افزار برای تشخیص فعالیت ویروسی طراحی نشده است. در این

شرایط بکارگیری یک برنامه تشخیص نفوذ یا IDS شبکه برای تشخیص این نوع فعالیت بسیار مناسب است.

نتیجه گیری

هکرها و تروریست های فضای سایبر به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی به امنیت ـ یعنی یک فایروال در ترکیب با یک آنتی ویروس ـ در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است.

اما شما می توانید با برقراری امنیت شبکه با استفاده از رویکرد لایه بندی شده دفاع مستحکمی ایجاد کنید. با نصب گزینشی ابزارهای امنیتی در پنج سطح موجود در شبکه تان (پیرامون، شبکه، میزبان، برنامه و دیتا) می توانید از دارایی های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.

مقدمه ای بر تشخیص نفوذ (Intrusion Detection)

تشخیص نفوذ عبارت است از پردازه تشخیص تلاشهایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می شوند.در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام حملات پیدا کرد. سپس بنابر درک بدست آمده، روشی دو مرحله ای را برای متوقف کردن حملات برگزید. اول این که مطمئن شوید که الگوی عمومی فعالیتهای خطرناک تشخیص داده شده است. دوم این که اطمینان حاصل کنید که با حوادث مشخصی که در طبقه بندی مشترک حملات نمی گنجند، به سرعت رفتار می شود.به همین دلیل است که بیشتر سیستم های تشخیص نفوذ (IDS)بر مکانیزمهایی جهت بروزرسانی نرم افزارشان متکی هستند که جهت جلوگیری از تهدیدات شبکه به اندازه کافی سریع هستند. البته تشخیص نفوذ به تنهایی کافی نیست و باید مسیر حمله را تا هکر دنبال کرد تا بتوان به شیوه مناسبی با وی نیز برخورد کرد.

انواع حملات شبکه ای با توجه به طریقه حمله

یک نفوذ به شبکه معمولا یک حمله قلمداد می شود. حملات شبکه ای را می توان بسته به چگونگی انجام آن به دو گروه اصلی تقسیم کرد. یک حمله شبکه ای را می توان با هدف نفوذگر از حمله توصیف و مشخص کرد. این اهداف معمولا از

کار انداختن سرویس (DOS یا Denial of Service) یا دسترسی غیرمجاز به منابع شبکه است.

۱- حملات از کار انداختن سرویس

در این نوع حملات، هکر استفاده از سرویس ارائه شده توسط ارائه کننده خدمات برای کاربرانش را مختل می کند. در این حملات حجم بالایی از درخواست ارائه خدمات به سرور فرستاده می شود تا امکان خدمات رسانی را از آن بگیرد. در واقع سرور به پاسخگویی به درخواستهای بی شمار هکر مشغول می شود و از پاسخگویی به کاربران واقعی باز می ماند.

۲- حملات دسترسی به شبکه

در این نوع از حملات، نفوذگر امکان دسترسی غیرمجاز به منابع شبکه را پیدا می کند و از این امکان برای انجام فعالیتهای غیرمجاز و حتی غیرقانونی استفاده می کند. برای مثال از شبکه به عنوان مبدا حملات DOS خود استفاده می کند تا درصورت شناسایی مبدا، خود گرفتار نشود. دسترسی به شبکه را می توان به دو گروه تقسیم کرد.

الف– دسترسی به داده : در این نوع دسترسی، نفوذگر به داده موجود بر روی اجزاء شبکه دسترسی غیرمجاز پیدا می کند. حمله کننده می تواند یک کاربر داخلی یا یک فرد خارج از مجموعه باشد. داده های ممتاز و مهم معمولا تنها در اختیار بعضی کاربران شبکه قرار می گیرد و سایرین حق دسترسی به آنها را

ندارند. در واقع سایرین امتیاز کافی را جهت دسترسی به اطلاعات محرمانه ندارند، اما می توان با افزایش امتیاز به شکل غیر مجاز به اطلاعات محرمانه دسترسی پیدا کرد. این روش به تعدیل امتیاز یا Privilege Escalation مشهور است.

ب- دسترسی به سیستم : این نوع حمله خطرناکتر و بدتر است و طی آن حمله کننده به منابع سیستم و دستگاهها دسترسی پیدا می کند. این دسترسی می تواند شامل اجرای برنامه ها بر روی سیستم و به کار گیری منابع آن در جهت اجرای دستورات حمله کننده باشد. همچنین حمله کننده می تواند به تجهیزات شبکه مانند دوربینها، پرینترها و وسایل ذخیره سازی دسترسی پیدا کند. حملات اسب تروا، Brute Force و یا استفاده از ابزارهایی جهت تشخیص نقاط ضعف یک نرم افزار نصب شده بر روی سیستم از جمله نمونه های قابل ذکر از این نوع حملات هستند.

فعالیت مهمی که معمولا پیش از حملات DoS و دسترسی به شبکه انجام می شود، شناسایی یا reconnaissance است. یک حمله کننده از این فاز جهتی افتن حفره های امنیتی و نقاط ضعف شبکه استفاده می کند. این کار می تواند به کمک بعضی ابزارها آماده انجام پذیرد که به بررسی پورتهای رایانه های موجود برروی شبکه می پردازند و آمادگی آنها را جهت انجام حملات مختلف بر روی آنها بررسی می کنند.

انواع حملات شبکه ای با توجه به حمله کننده

حملات شبکه ای را می توان با توجه به حمله کننده به چهار گروه تقسیم کرد:

۱- حملات انجام شده توسط کاربر مورد اعتماد (داخلی): این حمله یکی از مهمترین و خطرناکترین نوع حملات است، چون از یک طرف کاربر به منابع مختلف شبکه دسترسی دارد و از طرف دیگر سیاستهای امنیتی معمولا محدودیتهای کافی درباره این کاربران اعمال نمی کنند.

۲- حملات انجام شده توسط افراد غیر معتمد (خارجی): این معمولترین نوع حمله است که یک کاربر خارجی که مورد اعتماد نیست شبکه را مورد حمله قرار می دهد. این افراد معمولا سخت ترین راه را پیش رو دارند زیرا بیشتر سیاستهای امنیتی درباره این افراد تنظیم شده اند

۳- حملات انجام شده توسط هکرهای بی تجربه : بسیاری از ابزارهای حمله و نفوذ بر روی اینترنت وجود دارند. در واقع بسیاری از افراد می توانند بدون تجربه خاصی و تنها با استفاده از ابزارهای آماده برای شبکه ایجاد مشکل کنند.

٤- حملات انجام شده توسط کاربران مجرب : هکرهای با تجربه و حرفه ای در نوشتن انواع کدهای خطرناک متبحرند. آنها از شبکه و پروتکلهای آن و همچنین از انواع سیستم های عمل آگاهی کامل دارند. معمولا این افراد ابزارهایی تولید می کنند که توسط گروه اول به کار گرفته می شوند. آنها معمولا پیش از هر حمله، آگاهی کافی درباره قربانی خود کسب می کنند.

پردازه تشخیص نفوذ - تا بحال با انواع حملات آشنا شدیم. حال باید چگونگی شناسایی حملات و جلوگیری از آنها را بشناسیم. امروزه دو روش اصلی برای تشخیص نفوذ به شبکه ها مورد استفاده قرار می گیرد:

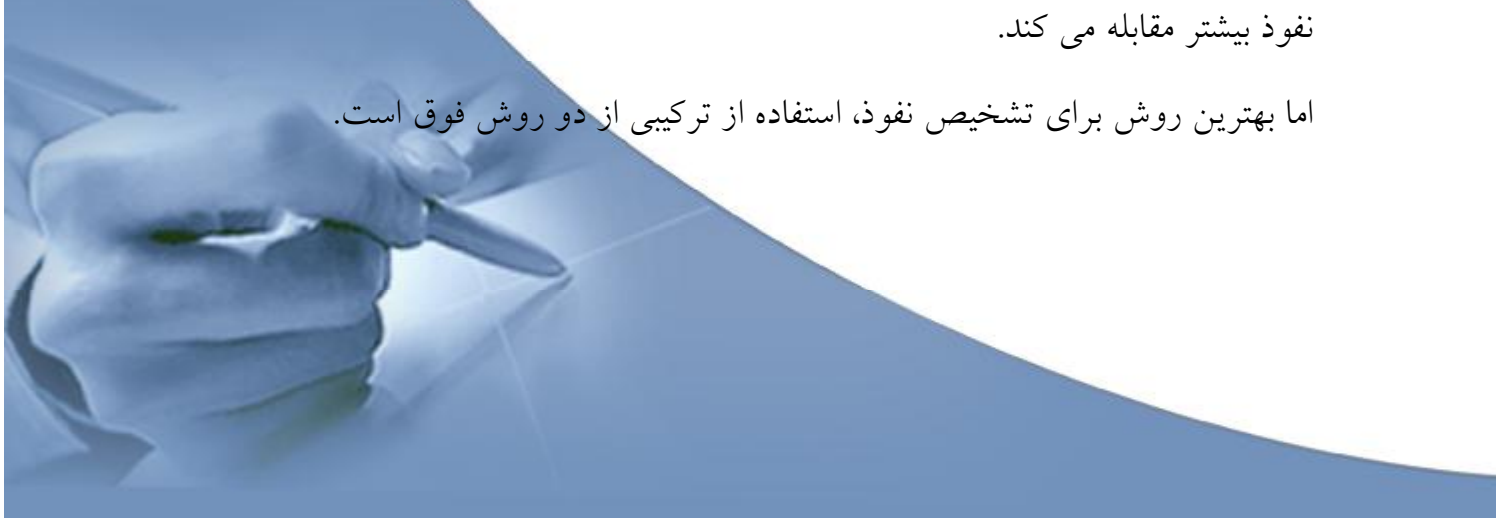
۱- IDS مبتنی بر خلاف قاعده آماری

۲- IDS مبتنی بر امضا یا تطبیق الگو

روش اول مبتنی بر تعیین آستانه انواع فعالیتها بر روی شبکه است، مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان (host) اجرا می شود.لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت خلاف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه ای هستند که نمی توان براحتی و با کمک این روش آنها را تشخیص داد.

در واقع روشی که در بیشتر سیستمهای موفق تشخیص نفوذ به کار گرفته می شود، IDS مبتنی بر امضا یا تطبیق الگو است.منظور از امضا مجموعه قواعدی است که یک حمله در حال انجام را تشخیص می دهد. دستگاهی که قرار است نفوذ را تشخیص دهد با مجموعه ای از قواعد بارگذاری می شود.هر امضا دارای اطلاعاتی است که نشان می دهد در داده های در حال عبور باید به دنبال چه فعالیتهایی گشت. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می شود و مدیر شبکه را از وقوع یک نفوذ آگاه می کند. در بسیاری از موارد IDS علاوه بر آگاه کردن مدیر شبکه، اتصال با هکر را بازآغازی می کند و یا با کمک یک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می کند.

اما بهترین روش برای تشخیص نفوذ، استفاده از ترکیبی از دو روش فوق است.



مقایسه تشخیص نفوذ و پیش گیری از نفوذ

Intrusion Prevention

ایده پیش گیری از نفوذ (Intrusion Prevention) این است که تمام حملات علیه هر بخش از محیط محافظت شده توسط روش های به کار گرفته شده ناکام بماند. این روش ها می توانند تمام بسته های شبکه را بگیرند و نیت آنها را مشخص کنند ـ آیا هرکدام یک حمله هستند یا یک استفاده قانونی ـ سپس عمل مناسب را انجام دهند.

تفاوت شکلی تشخیص با پیش گیری

در ظاهر، روش های تشخیص نفوذ و پیش گیری از نفوذ رقیب هستند. به هرحال، آنها لیست بلند بالایی از عملکردهای مشابه، مانند بررسی بسته داده، تحلیل با توجه به حفظ وضعیت، گردآوری بخش های TCP، ارزیابی پروتکل و تطبیق امضاء دارند. اما این قابلیت ها به عنوان ابزاری برای رسیدن به اهداف متفاوت در این دو روش به کار گرفته می شوند. یک IPS (Intrusion Prevention System) یا سیستم پیش گیری مانند یک محافظ امنیتی در مدخل یک اجتماع اختصاصی عمل می کند که بر پایه بعضی گواهی ها و قوانین یا سیاست های از پیش تعیین شده اجازه عبور می دهد. یک IDS (Intrusion Detection System) یا سیستم تشخیص مانند یک اتومبیل گشت زنی در میان اجتماع عمل می کند که فعالیت ها را به نمایش می گذارد و دنبال موقعیت

های غیرعادی می گردد. بدون توجه به قدرت امنیت در مدخل، گشت زن ها به کار خود در سیستم ادامه می دهند و بررسی های خود را انجام می دهند.

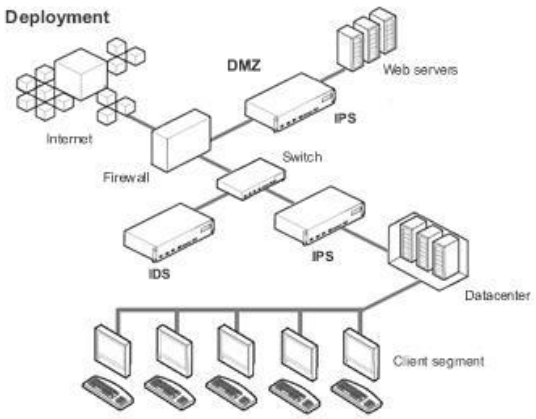
تشخیص نفوذ

هدف از تشخیص نفوذ نمایش، بررسی و ارائه گزارش از فعالیت شبکه است. این سیستم روی بسته های داده که از ابزار کنترل دسترسی عبور کرده اند، عمل می کند. به دلیل وجود محدودیت های اطمینان پذیری، تهدیدهای داخلی و وجود شک و تردید مورد نیاز، پیش گیری از نفوذ باید به بعضی از موارد مشکوک به حمله اجازه عبور دهد تا احتمال تشخیص های غلط (positive false) کاهش یابد. از طرف دیگر، روش های IDS با هوشمندی همراه هستند و از تکنیک های مختلفی برای تشخیص حملات بالقوه، نفوذها و سوء استفاده ها بهره می گیرند. یک IDS معمولاً به گونه ای از پهنای باند استفاده می کند که می تواند بدون تأثیر گذاشتن روی معماری های محاسباتی و شبکه ای به کار خود ادامه دهد. طبیعت منفعل IDS آن چیزی است که قدرت هدایت تحلیل هوشمند جریان بسته ها را ایجاد می کند. همین امر IDS را در جایگاه خوبی برای تشخیص موارد زیر قرارمی دهد:

- حملات شناخته شده از طریق امضاءها و قوانین
- تغییرات در حجم و جهت ترافیک با استفاده از قوانین پیچیده و تحلیل آماری
- تغییرات الگوی ترافیک ارتباطی با استفاده از تحلیل جریان
- تشخیص فعالیت غیرعادی با استفاده از تحلیل انحراف معیار

- تشخیص فعالیت مشکوک با استفاده از تکنیک های آماری، تحلیل جریان و تشخیص خلاف قاعده

بعضی حملات تا درجه ای از یقین بسختی قابل تشخیص هستند، و بیشتر آنها فقط می توانند توسط روش هایی که دارای طبیعت غیرقطعی هستند تشخیص داده شوند. یعنی این روش ها برای تصمیم گیری مسدودسازی براساس سیاست مناسب نیستند.



پیش گیری از نفوذ

چنانچه قبلاً هم ذکر شد، روش های پیش گیری از نفوذ به منظور محافظت از دارایی ها، منابع، داده و شبکه ها استفاده می شوند. انتظار اصلی از آنها این است که خطر حمله را با حذف ترافیک مضر شبکه کاهش دهند در حالیکه به فعالیت صحیح اجازه ادامه کار می دهند. هدف نهایی یک سیستم کامل است- یعنی نه تشخیص غلط حمله (false positive) که از بازدهی شبکه می کاهد

و نه عدم تشخیص حمله (false negative) که باعث ریسک بی مورد در محیط شبکه شود. شاید یک نقش اساسی تر نیاز به مطمئن بودن است؛ یعنی فعالیت به روش مورد انتظار تحت هر شرایطی. بمنظور حصول این منظور، روش های IPS باید طبیعت قطعی (deterministic) داشته باشند.

قابلیت های قطعی، اطمینان مورد نیاز برای تصمیم گیری های سخت را ایجاد می کند. به این معنی که روش های پیش گیری از نفوذ برای سروکار داشتن با موارد زیر ایده آل هستند:

- برنامه های ناخواسته و حملات اسب تروای فعال علیه شبکه ها و برنامه های اختصاصی، با استفاده از قوانین قطعی و لیست های کنترل دسترسی
- بسته های دیتای متعلق به حمله با استفاده از فیلترهای بسته داده ای سرعت بالا
- سوءاستفاده از پروتکل و دستکاری پروتکل شبکه با استفاده از بازسازی هوشمند
- حملات DoS/DDoS مانند طغیان SYN وICMP با استفاده از الگوریتم های فیلترینگ برپایه حد آستانه
- سوءاستفاده از برنامه ها و دستکاری های پروتکل ـ حملات شناخته شده و شناخته نشده علیه HTTP، FTP، DNS، SMTP و غیره با استفاده از قوانین پروتکل برنامه ها و امضاءها
- باراضافی برنامه ها با استفاده از ایجاد محدودیت های مصرف منابع

تمام این حملات و وضعیت آسیب پذیری که به آنها اجازه وقوع می دهد به خوبی مستندسازی شده اند. بعلاوه، انحرافات از پروتکل های ارتباطی از لایه شبکه تا لایه برنامه جایگاهی در هیچ گونه ترافیک صحیح ندارند.

نتیجه نهایی

تفاوت بین IDS و IPS به فلسفه جبرگرایی می انجامد. یعنی IDS می تواند (و باید) از روش های غیرقطعی برای استنباط هرنوع تهدید یا تهدید بالقوه از ترافیک موجود استفاده کند. این شامل انجام تحلیل آماری از حجم ترافیک، الگوهای ترافیک و فعالیت های غیرعادی می شود. IDS به درد افرادی می خورد که واقعاً می خواهند بدانند چه چیزی در شبکه شان در حال رخ دادن است.

از طرف دیگر، IPS باید در تمام تصمیماتش برای انجام وظیفه اش در پالایش ترافیک قطعیت داشته باشد. از یک ابزار IPS انتظار می رود که در تمام مدت کار کند و در مورد کنترل دسترسی تصمیم گیری کند. فایروال ها اولین رویکرد قطعی را برای کنترل دسترسی در شبکه ها با ایجاد قابلیت اولیه IPS فراهم کردند. ابزارهای IPS قابلیت نسل بعد را به این فایروال ها اضافه کردند و هنوز در این فعالیت های قطعی در تصمیم گیری برای کنترل دسترسی ها مشارکت دارند.

حملات DoS

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoS قرار گرفته است. این نوع از حملات صرفا" متوجه وب سایت ها نبوده و ممکن است شما قربانی بعدی باشید. تشخیص حملات DoS از طریق عملیات متداول شبکه امری مشکل است ولی با مشاهده برخی علائم در یک شبکه و یا کامپیوتر می توان از میزان پیشرفت این نوع از حملات آگاهی یافت.

حملات از نوع DoS (denial-of-service)

در یک تهاجم از نوع DoS ، یک مهاجم باعث ممانعت دستیابی کاربران تائید شده به اطلاعات و یا سرویس های خاصی می نماید. یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه ای آن و یا کامپیوترها و شبکه ای از سایت هائی که شما قصد استفاده از آنان را دارید، باعث سلب دستیابی شما به سایت های Email ، وب سایت ها، account های online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد.

متداولترین و مشهودترین نوع حملات DoS ، زمانی محقق می گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. زمانی که شما آدرس URL یک وب سایت خاص را از طریق مرورگر خود تایپ می نمائید، درخواست شما برای سرویس دهنده ارسال می گردد. سرویس دهنده در هر لحظه قادر به پاسخگوئی به حجم محدودی از درخواست ها می باشد، بنابراین اگر یک مهاجم با ارسال درخواست های متعدد و سیلاب گونه باعث افزایش حجم عملیات سرویس دهند گردد، قطعا" امکان پردازش درخواست شما برای سرویس دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می باشند، چراکه امکان دستیابی شما به سایت مورد نظر سلب شده است.

یک مهاجم می تواند با ارسال پیام های الکترونیکی ناخواسته که از آنان با نام Spam یاد می شود، حملات مشابهی را متوجه سرویس دهنده پست الکترونیکی نماید. هر account پست الکترونیکی (صرفنظر از منبعی که آن را در اختیار شما قرار می دهد، نظیر سازمان مربوطه و یا سرویس های رایگانی نظیر یاهو و hotmail) دارای ظرفیت محدودی می باشند. پس از تکمیل ظرفیت فوق، عملا" امکان ارسال Email دیگری به account فوق وجود نخواهد داشت. مهاجمان با ارسال نامه های الکترونیکی ناخواسته سعی می نمایند که ظرفیت account مورد نظر را تکمیل و عملا" امکان دریافت email های معتبر را از account فوق سلب نمایند.

حملات از نوع DDoS (distributed denial-of-service)

در یک تهاجم از نوع DDoS ، یک مهاجم ممکن است از کامپیوتر شما برای تهاجم بر علیه کامپیوتر دیگری استفاده نماید. مهاجمان با استفاده از نقاط آسیب پذیر و یا ضعف امنیتی موجود بر روی سیستم شما می توانند کنترل کامپیوتر شما را بدست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند. ارسال حجم بسیار بالائی داده از طریق کامپیوتر شما برای یک وب سایت و یا ارسال نامه های الکترونیکی ناخواسته برای آدرس های Email خاصی، نمونه هائی از همکاری کامپیوتر شما در بروز یک تهاجم DDOS می باشد. حملات فوق، "توزیع شده " می باشند، چراکه مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می نماید.

نحوه پیشگیری از حملات

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoS و یا DDoS وجود ندارد. علیرغم موضوع فوق، می توان با رعایت برخی نکات و انجام عملیات

پیشگیری، احتمال بروز چنین حملاتی (استفاده از کامپیوتر شما برای تهاجم بر علیه سایر کامپیوتر ها) را کاهش داد.

- نصب و نگهداری نرم افزار آنتی ویروس
- نصب و پیکربندی یک فایروال
- تبعیت از مجموعه سیاست های خاصی در خصوص توزیع و ارائه آدرس Email خود به دیگران

چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟

خرابی و یا بروز اشکال در یک سرویس شبکه، همواره بدلیل بروز یک تهاجم DoS نمی باشد. در این رابطه ممکن است دلایل متعددی فنی وجود داشته و یا مدیر شبکه به منظور انجام عملیات نگهداری موقتا" برخی سرویس ها را غیر فعال کرده باشد. وجود و یا مشاهده علائم زیر می تواند نشاندهنده بروز یک تهاجم از نوع DoS و یا DDoS باشد:

- کاهش سرعت و یا کارآئی شبکه بطرز غیر معمول (در زمان باز نمودن فایل ها و یا دستیابی به وب سایت ها).
- عدم در دسترس بودن یک سایت خاص(بدون وجود دلایل فنی)
- عدم امکان دستیابی به هر سایتی(بدون وجود دلایل فنی)
- افزایش محسوس حجم نامه های الکترونیکی ناخواسته دریافتی

در صورت بروز یک تهاجم ، چه عملیاتی را می بایست انجام داد؟

حتی در صورتی که شما قادر به شناسائی حملات از نوع DoS و یا DDoS باشید، امکان شناسائی مقصد و یا منبع واقعی تهاجم، وجود نخواهد داشت. در این رابطه لازم

است با کارشناسان فنی ماهر، تماس گرفته تا آنان موضوع را بررسی و برای آن راهکار مناسب را ارائه نمایند.

- در صورتی که برای شما مسلم شده است که نمی توانید به برخی از فایل های خود و یا هر وب سایتی خارج از شبکه خود دستیابی داشته باشید، بلافاصله با مدیران شبکه تماس گرفته و موضوع را به اطلاع آنان برسانید. وضعیت فوق می تواند نشاندهنده بروز یک تهاجم بر علیه کامپیوتر و یا سازمان شما باشد.
- در صورتی که وضعیت مشابه آنچه اشاره گردید را در خصوص کامپیوترهای موجود در منازل مشاهده می نمائید با مرکز ارائه دهنده خدمات اینترنت (ISP) تماس گرفته و موضوع را به اطلاع آنان برسانید. ISP مورد نظر می تواند توصیه های لازم به منظور انجام عملیات مناسب را در اختیار شما قرار دهد.

عدم پذیرش سرویس (۱)

قصد داریم تا طی چند قسمت با نوعی از حمله به نام DoS آشنا شویم که مخفف عبارت Denial-of-Service یا عدم پذیرش سرویس است. همانطور که در روش های معمول حمله به کامپیوترها اشاره مختصری شد، این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از اندازه کامپیوتر می شود تا حدی که غیرقابل استفاده می شود. در بیشتر موارد، حفره های امنیتی محل انجام این حملات است و لذا نصب آخرین وصله های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود. نفوذگران با ایجاد ترافیک بی مورد و بی استفاده باعث می شوند که حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی مورد شود و این تقاضا تا جایی که دستگاه سرویس دهنده را به زانو در آورد ادامه پیدا می کند. نیت اولیه و تأثیر حملات DoS جلوگیری از استفاده صحیح از منابع کامپیوتری و شبکه ای و از بین بردن این منابع است.

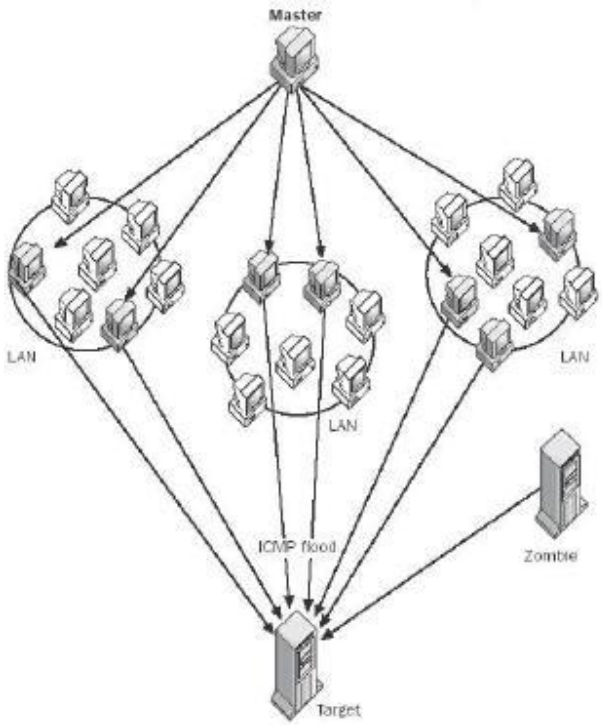
علیرغم تلاش و منابعی که برای ایمن سازی علیه نفوذ و خرابکاری مصـــروف گشته است، سیستم های متصل به اینترنت با تهـــــدیدی واقعی و مداوم به نام حملات DoS مواجه هستند. این امر بدلیل دو مشخصه اساسی اینترنت است:

- **منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند.**

زیرساختار سیستم ها و شبکه های بهم متصل که اینترنت را می سازند، کاملاً از منابع محدود تشکیل شده است. پهنای باند، قدرت پردازش و ظرفیت های ذخیره سازی، همگی محدود و هدف های معمول حملات DoS هستند. مهاجمان با انجام این حملات سعی می کنند با مصرف کردن مقدار قابل توجهی از منابع در دسترس، باعث قطع میزانی از سرویس ها شوند. وفور منابعی که بدرستی طراحی و استفاده شده اند ممکن است عاملی برای کاهش میزان تاثیر یک حمله DoS باشد، اما شیوه ها و ابزار امروزی حمله حتی در کارکرد فراوان ترین منابع نیز اختلال ایجاد می کند.

- **امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است.**

حملات DoS معمولاً از یک یا چند نقطه که از دید سیستم یا شبکه قربانی عامل بیرونی هستند، صورت می گیرند. در بسیاری موارد، نقطه آغاز حمله شامل یک یا چند سیستم است که از طریق سوءاستفاده های امنیتی در اختیار یک نفوذگر قرار گرفته اند و لذا حملات از سیستم یا سیستم های خود نفوذگر صورت نمی گیرد. بنابراین، دفاع برعلیه نفوذ نه تنها به حفاظت از اموال مرتبط با اینترنت کمک می کند، بلکه به جلوگیری از استفاده از این اموال برای حمله به سایر شبکه ها و سیستم ها نیز کمک می کند. پس بدون توجه به اینکه سیستم هایتان به چه میزان محافظت می شوند، قرار گرفتن در معرض بسیاری از انواع حمله و مشخصاً DoS ، به وضعیت امنیتی در سایر قسمت های اینترنت بستگی زیادی دارد.

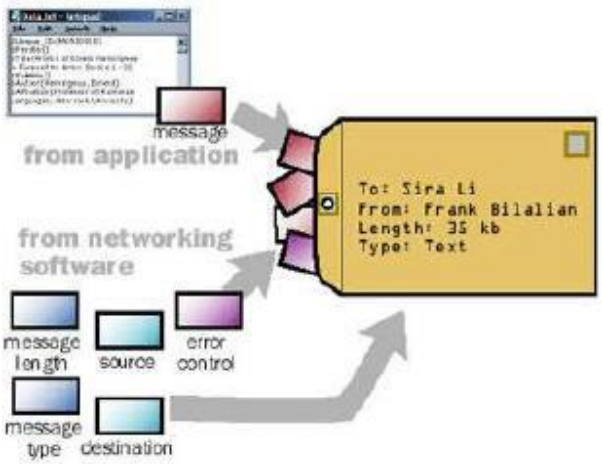


مقابله با حملات DoS تنها یک بحث عملی نیست. محدودکردن میزان تقاضا، فیلترکردن بسته ها و دستکاری پارامترهای نرم افزاری در بعضی موارد می تواند به محدودکردن اثر حملات DoS کمک کند، اما بشرطی که حمله DoS در حال مصرف کردن تمام منابع موجود نباشد. در بسیاری موارد، تنها می توان یک دفاع واکنشی داشت و این در صورتی است که منبع یا منابع حمله مشخص شوند. استفاده از جعل آدرس IP در طول حمله و ظهور روش های حمله توزیع شده و ابزارهای موجود یک چالش همیشگی را در مقابل کسانی که باید به حملات DoS پاسخ دهند، قرار داده است.

تکنولوژی حملات DoS اولیه شامل ابزار ساده ای بود که بسته ها را تولید و از «یک منبع به یک مقصد» ارسال می کرد. با گذشت زمان، ابزارها تا حد اجرای حملات از «یک

منبع به چندین هدف»، «از چندین منبع به هدف های تنها» و «چندین منبع به چندین هدف»، پیشرفت کرده اند.

امروزه بیشترین حملات گزارش شده به CERT/CC مبنی بر ارسال تعداد بسیار زیادی بسته به یک مقصد است که باعث ایجاد نقاط انتهایی بسیار زیاد و مصرف پهنای باند شبکه می شود. از چنین حملاتی معمولاً به عنوان حملات طغیان بسته (Packet flooding) یاد می شود. اما در مورد «حمله به چندین هدف» گزارش کمتری دریافت شده است.



انواع بسته ها (Packets) مورد استفاده برای حملات طغیان بسته، در طول زمان تغییر کرده است، اما چندین نوع بسته معمول وجود دارند که هنوز توسط ابزار حمله DoS استفاده می شوند.

- **طغیان های TCP**: رشته ای از بسته های TCP با پرچم های (flag) متفاوت به آدرس IP قربانی فرستاده می شوند. پرچم های SYN، ACK و RST بیشتر استفاده می شوند.
- **طغیان های تقاضا\پاسخ ICMP** (مانند طغیان های ping): رشته ای از بسته های ICMP به آدرس IP قربانی فرستاده می شود.
- **طغیان های UDP**: رشته ای از بسته های UDP به آدرس IP قربانی ارسال می شوند.

درقسمت بعدی به بررسی بیشتر حملات DoS خوهیم پرداخت.

عدم پذیرش سرویس (۲) : انواع حملات

در قسمت پیش با حمله DoS آشنا شدیم. از آنجا که حملات طغیان بسته های دیتا معمولاً تلاش می کنند منابع پهنای باند و پردازش را خلع سلاح کنند، میزان بسته ها و حجم دیتای متناظر با رشته بسته ها عوامل مهمی در تعیین درجه موفقیت حمله هستند. بعضی از ابزارهای حمله خواص بسته ها را در رشته بسته ها بدلایلی تغییر می دهند:

- **آدرس IP منبع** – در بعضی موارد، یک آدرس IP منبع ناصحیح، (روشی که جعل IP نامیده می شود) برای پنهان کردن منبع واقعی یک رشته بسته استفاده می شود. در موارد دیگر، جعل IP هنگامی استفاده می شود که رشته های بسته به یک یا تعداد بیشتری از سایت های واسطه فرستاده می شوند تا باعث شود که پاسخ ها به سمت قربانی ارسال شود. مثال بعدی در مورد حملات افزایش بسته است (مانند smurf و fraggle)
- **پورتهای منبع\مقصد**- ابزار حمله طغیان بسته بر اساس TCP و UDP ، گاهی اوقات پورت منبع و یا مقصد را تغییر می دهند تا واکنش توسط فیلتر کردن بسته را مشکل تر کنند.
- **مقادیر IP Header دیگر** - در نهایت در ابزار حمله DoS مشاهده کرده ایم که برای مقداردهی تصادفی، مقادیر Header هر بسته در رشته بسته ها طراحی شده اند که تنها آدرس IP مقصد است که بین بسته ها ثابت می ماند.

بسته ها با خواص ساختگی بسادگی در طول شبکه تولید و ارسال می شوند. پروتکل TCP/IP به آسانی مکانیزم هایی برای تضمین پیوستگی خواص بسته ها در هنگام تولید و یا ارسال نقطه به نقطه بسته ها ارائه نمی کند. معمولاً، یک نفوذگر فقط به داشتن اختیار کافی روی یک سیستم برای بکارگیری ابزار و حملاتی که قادر به تولید و ارسال بسته های با خواص تغییریافته باشند، نیاز دارد.

ژوئن ۱۹۹۹، آغاز بکارگیری ابزار DoS با چندین منبع یا DDos (Distributed DoS) بود.

روش های حمله DoS

در این قسمت به یک تقسیم بندی کلی درباره انواع حملات DoS می پردازیم:

Smurf یا Fraggle

حملات smurf یک از مخرب ترین حملات DoS هستند. (شکل زیر)

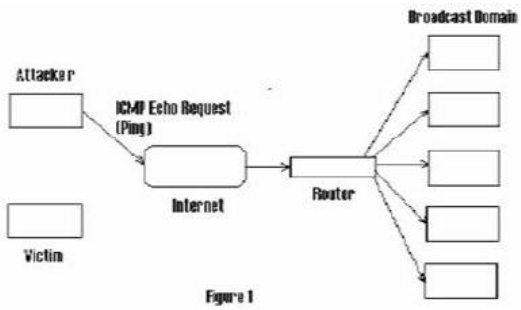


Figure 1

در حمله Smurf (حمله براساس ازدیاد بسته های ICMP)، نفوذگر یک تقاضای اکوی ICMP (ping) به یک آدرس ناحیه می فرستد.

آدرس منبع تقاضای اکو، آدرس IP قربانی است. (از آدرس IP قربانی بعنوان آدرس برگشت استفاده می شود). بعد از دریافت تقاضای اکو، تمام ماشین های ناحیه پاسخ های اکو را به آدرس IP قربانی می فرستند. در این حالت قربانی هنگام دریافت طغیان بسته های با اندازه بزرگ از تعداد زیادی ماشین، از کار خواهد افتاد.

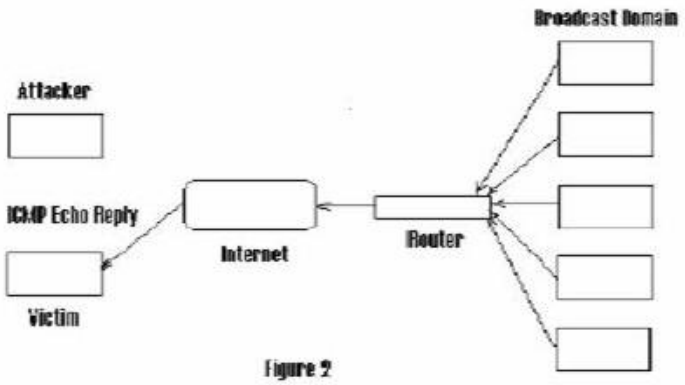


Figure 2

حمله Smurf برای ازکار انداختن منابع شبکه سیستم قربانی از روش مصرف پهنای باند استفاده می کند. این حمله این عمل را با استفاده از تقویت پهنای باند نفوذگران انجام می دهد. اگر شبکه تقویت کننده ۱۰۰ ماشین دارد، سیگنال می تواند ۱۰۰ برابر شود، و بنابراین حمله کننده با پهنای باند پایین (مانند مودم ۵۶ کیلوبیتی) می تواند سیستم قربانی را با پهنای باند بیشتری (مانند اتصال T1) از کار بیندازد.

حمله Fraggle (تقویت بسته UDP) در حقیقت شباهت هایی به حمله Smurf دارد. حمله Fraggle از بسته های اکوی UDP بر طبق همان روش بسته های اکوی ICMP در حمله Smurf استفاده می کند.

Fraggle معمولاً به ضریب تقویت کمتری نسبت به Smurf می رسد، و در بیشتر شبکه ها اکوی UDP سرویسی با اهمیت کمتر نسبت به اکوی ICMP است، بنابراین Fraggle عمومیت Smurf را ندارد.

SYN Flood

حمله طغیان SYN قبل از کشف حمله Smurf بعنوان مخرب ترین شیوه حمله DoS بشمار می رفت. این روش برای ایجاد حمله DoS بر اساس قحطی منابع عمل می کند.

در طول برقراری یک ارتباط معمولی TCP، سرویس گیرنده یک تقاضای SYN به سرویس دهنده می فرستد، سپس سرور با یک ACK/SYN به کلاینت پاسخ می دهد، در نهایت کلاینت یک ACK نهایی را به سرور ارسال می کند و به این ترتیب ارتباط برقرار می شود.

اما در حمله طغیان SYN، حمله کننده چند تقاضای SYN به سرور قربانی با آدرس های منبع جعلی بعنوان آدرس برگشت، می فرستد. آدرس های جعلی روی شبکه وجود ندارند. سرور قربانی سپس با ACK/SYN به آدرس های ناموجود پاسخ می دهد. از آنجا که هیچ آدرسی این ACK/SYN را دریافت نمی کند، سرور قربانی منتظر ACK از طرف کلاینت می ماند. ACK هرگز نمی رسد، و زمان انتظار سرور قربانی پس از مدتی به پایان می رسد. اگر حمله کننده به اندازه کافی و مرتب تقاضاهای SYN بفرستد، منابع موجود سرور قربانی برای برقراری یک اتصال و انتظار برای این ACKهای در حقیقت تقلبی

مصرف خواهد شد. این منابع معمولاً از نظر تعداد زیاد نیستند، بنابراین تقاضاهای SYN جعلی حتی با تعداد نسبتاً کم می توانند باعث وقوع یک حمله DoS شوند.

حملات DNS

در نسخه های اولیه BIND (Berkely Internet Name Domain)، حمله کنندگان می توانستند بطور مؤثری حافظه نهان یک سرور DNS را که در حال استفاده از عملیات بازگشت برای جستجوی یک ناحیه بود که توسط این سرور سرویس داده نمی شد، مسموم کنند. زمانی که حافظه نهان مسموم می شد، یک کاربر قانونی به سمت شبکه مورد نظر حمله کننده یا یک شبکه ناموجود هدایت می شد. این مشکل با نسخه های جدیدتر BIND برطرف شده است. در این روش حمله کننده اطلاعات DNS غلط که می تواند باعث تغییر مسیر درخواست ها شود، ارسال می کند.

حملات DDoS

حملات DDoS (Distributed Denial of Service) حمله گسترده ای از DoS است. در اصل DDos حمله هماهنگ شده ای برعلیه سرویس های موجود در اینترنت است. در این روش حملات DoS بطور غیرمستقیم از طریق تعداد زیادی از کامپیوترهای هک شده بر روی کامپیوتر قربانی انجام می گیرد. سرویس ها و منابع مورد حمله ، «قربانی های اولیه» و کامپیوترهای مورد استفاده در این حمله «قربانی های ثانویه» نامیده می شوند. حملات DDoS عموماً در از کار انداختن سایت های کمپانی های عظیم از حملات DoS مؤثرتر هستند.

انواع حملات DDoS

عموماً حملات DDoS به سه گروه Trinoo، TFN/TFN2K و Stecheldraht تقسیم می شوند.

Trinoo

Trinoo در اصل از برنامه های Master/Slave است که با یکدیگر برای یک حمله طغیان UDP بر علیه کامپیوتر قربانی هماهنگ می شوند. در یک روند عادی، مراحل زیر برای برقراری یک شبکه Trinoo DDoS واقع می شوند:

مرحله۱: حمله کننده، با استفاده از یک میزبان هک شده، لیستی از سیستم هایی را که می توانند هک شوند، گردآوری می کند. بیشتر این پروسه بصورت خودکار از طریق میزبان هک شده انجام می گیرد. این میزبان اطلاعاتی شامل نحوه یافتن سایر میزبان ها برای هک در خود نگهداری می کند.

مرحله۲: به محض اینکه این لیست آماده شد، اسکریپت ها برای هک کردن و تبدیل آنها به اربابان(Masters) یا شیاطین (Daemons) اجراء می شوند. یک ارباب می تواند چند شیطان را کنترل کند. شیاطین میزبانان هک شده ای هستند که طغیان UDP اصلی را روی ماشین قربانی انجام می دهند.

مرحله۳: حمله DDoS هنگامی که حمله کننده فرمانی به میزبانان Master ارسال می کند، انجام می گیرد. این اربابان به هر شیطانی دستور می دهند که حمله DoS را علیه آدرس IP مشخص شده در فرمان آغاز کنند و با انجام تعداد زیادی حمله DoS یک حمله DDoS شکل می گیرد.

TFN / TFN2K

TFN (Tribal Flood Network) یا شبکه طغیان قبیله ای، مانند Trinoo، در اصل یک حمله Master/Slave است که در آن برای طغیان SYN علیه سیستم قربانی هماهنگی صورت می گیرد. شیاطین TFN قادر به انجام حملات بسیار متنوع تری شامل طغیان ICMP، طغیان SYN و حملات Smurf هستند، بنابراین TFN از حمله Trinoo پیچیده تر است.

TFN2K نسبت به ابزار TFN اصلی چندین برتری و پیشرفت دارد. حملات TFN2K با استفاده از جعل آدرس های IP اجرا می شوند که باعث کشف مشکل تر منبع حمله می شود. حملات TFN2K فقط طغیان ساده مانند TFN نیستند. آنها همچنین شامل حملاتی می شوند که از شکاف های امنیتی سیستم عامل ها برای بسته های نامعتبر و ناقص سوءاستفاده می کنند تا به این ترتیب باعث از کار افتادن سیستم های قربانی شوند. حمله کنندگان TFN2K دیگر نیازی به اجرای فرمان ها با وارد شدن به ماشین های مخدوم (Client) (به جای Master در TFN) ندارند و می توانند این فرمان ها را از راه دور اجراء کنند. ارتباط بین Clientها و Daemonها دیگر به پاسخ های اکوی ICMP محدود نمی شود و می تواند روی واسط های مختلفی مانند TCP و UDP صورت گیرد. بنابراین TFN2K خطرناک تر و همچنین برای کشف کردن مشکل تر است.

Stacheldraht

کد Stacheldraht بسیار شبیه به Trinoo و TFN است، اما Stacheldraht اجازه می دهد که ارتباط بین حمله کننده و Masterها (که در این حمله Handler نامیده می شوند) رمزنگاری شود؛ عامل ها می توانند کد خود را بصورت خودکار ارتقاء دهند، می توانند اقدام به انواع مختلفی از حملات مانند طغیان های ICMP، طغیان های UDP و طغیان های SYN کنند.

در قسمت بعدی به روشهای مقابله با این نوع حملات خواهیم پرداخت.

عدم پذیرش سرویس (۳) : روش های مقابله

در قسمت پیش با انواع حملات DoS و DDoS آشنا شدیم. در این شماره با چند روش مقابله با حملات DoS و DDoS آشنا می شویم.

دفاع علیه حملات Smurf یا Fraggle

اگر در معرض حمله Smurf قرار گرفته باشید، کار چندانی از شما ساخته نیست. هرچند که این امکان وجود دارد که بسته های مهاجم را در روتر خارجی مسدود کنید، اما پهنای باند منشاء آن روتر مسدود خواهد شد. برای اینکه فراهم کننده شبکه بالاسری شما، حملات را در مبداء حمله مسدود کند، به هماهنگی نیاز است.

بمنظور جلوگیری از آغاز حمله از سایت خودتان، روتر خارجی را طوری پیکربندی کنید که تمام بسته های خارج شونده را که آدرس مبداء متناقض با زیرشبکه شما دارند، مسدود کند. اگر بسته جعل شده نتواند خارج شود، نمی تواند آسیب چندانی برساند.

برای جلوگیری از قرار گرفتن بعنوان یک واسطه و شرکت در حمله DoS شخص دیگر، روتر خود را طوری پیکربندی کنید که بسته هایی را که مقصدشان تمام آدرس های شبکه شماست، مسدود کند. یعنی، به بسته های ICMP منتشر شده به شبکه خود، اجازه عبور از روتر ندهید. این عمل به شما اجازه می دهد که توانایی انجام ping به تمام سیستم های موجود در شبکه خود را حفظ کنید، در حالیکه اجازه این عمل را از یک

سیستم بیرونی بگیرید. اگر واقعاً نگران هستید، می توانید سیستم های میزبان خود را طوری پیکربندی کنید که از انتشارهای ICMP کاملاً جلوگیری کنند.

دفاع علیه حملات طغیان SYN

بلاک های کوچک

بجای تخصیص یک شیء از نوع ارتباط کامل (که باعث اشغال فضای زیاد و نهایتاً اشکال در حافظه می شود)، یک رکورد کوچک (micro-record) تخصیص دهید. پیاده سازی های جدیدتر برای SYN های ورودی ، تنها ۱۶ بایت تخصیص می دهد.

کوکی های SYN

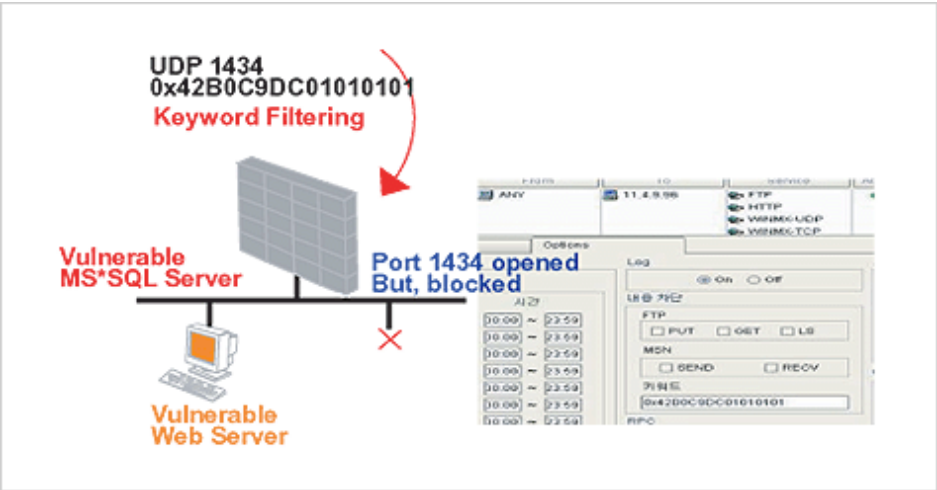
یک دفاع جدید علیه طغیان SYN «کوکی های SYN» است. در کوکی های SYN، هر طرف ارتباط، شماره توالی (Sequence Number) خودش را دارد. در پاسخ به یک SYN، سیستم مورد حمله واقع شده، یک شماره توالی مخصوص از ارتباط ایجاد می کند که یک «کوکی» است و سپس همه چیز را فراموش می کند یا بعبارتی از حافظه خارج می کند (کوکی بعنوان مشخص کننده یکتای یک تبادل یا مذاکره استفاده می شود). کوکی در مورد ارتباط اطلاعات لازم را در بردارد، بنابراین بعداً می تواند هنگامی که بسته ها از یک ارتباط سالم می آیند، مجدداً اطلاعات فراموش شده در مورد ارتباط را ایجاد کند.

کوکی های RST

جایگزینی برای کوکی های SYN است، اما ممکن است با سیستم عامل های ویندوز ۹۵ که پشت فایروال قرار دارند، مشکل ایجاد کند. روش مذکور به این ترتیب است که سرور یک ACK/SYN اشتباه به کلاینت ارسال می کند.

کلاینت باید یک بسته RST تولید کند تا به سرور بگوید که چیزی اشتباه است. در این هنگام، سرور می فهمد که کلاینت معتبر است و ارتباط ورودی از آن کلاینت را بطور طبیعی خواهد پذیرفت.

پشته های (stack) های TCP بمنظور کاستن از تأثیر طغیان های SYN می توانند دستکاری شوند. معمول ترین مثال کاستن زمان انقضاء (timeout) قبل از این است که پشته، فضای تخصیص داده شده به یک ارتباط را آزاد کند. تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.



دفاع علیه حملات DNS

دفاع از سرور اصلی (root server)

پایگاه داده سرور اصلی کوچک است و بندرت تغییر می کند. یک کپی کامل از پایگاه داده اصلی تهیه کنید، روزی یک بار آپدیت ها را چک کنید و گاه و بیگاه بارگذاری های مجدد انجام دهید. از سرورهای اصلی با استفاده از آدرس های anycast استفاده کنید

(این عمل باعث می شود که سیستم ها در شبکه های با موقعیت های مختلف بعنوان یک سرور بنظر برسند.)

دفاع از سازمان تان

اگر سازمان شما یک اینترانت دارد، باید دسترسی های جداگانه ای از DNS برای کاربران داخلی و مشتریان خارجی خود فراهم کنید. این عمل DNS داخلی را از حملات خارجی در امان نگاه می دارد. ناحیه اصلی را کپی کنید تا سازمان خود را از حملات DDoS آتی روی قسمت های اصلی محفوظ نگه دارید. همچنین به کپی کردن نواحی DNS از شرکای تجاری خود که در خارج از شبکه شما قرار دارند، توجه کنید. هنگامی که بروز رسان های DNS به روی اینترنت می روند، می توانند در هنگام انتقال مورد ربایش و دستکاری قرار گیرند. از TSIGها (transaction signature) یا امضاهای معاملاتی برای امضای آن ها یا ارسال بروز رسان ها روی VPN (شبکه های خصوصی مجازی) یا سایر کانال ها استفاده کنید.

مقابله با حملات DDoS

چگونه می توانید از سرورهای خود در مقابل یورش دیتاهای ارسالی از طرف کامپیوترهای آلوده موجود در اینترنت مراقبت کنید تا شبکه شرکت شما مختل نشود؟ در اینجا به چند روش بطور مختصر اشاره می شود:

سیاه چاله

این روش تمام ترافیک را مسدود می کند و به سمت سیاه چاله! یعنی جایی که بسته ها دور ریخته می شود هدایت می کند. اشکال در این است که تمام ترافیک – چه خوب و چه بد– دور ریخته می شود و در حقیقت شبکه مورد نظر بصورت یک سیستم off-line قابل استفاده خواهد بود. در روش های اینچنین حتی اجازه دسترسی به کاربران قانونی نیز داده نمی شود.

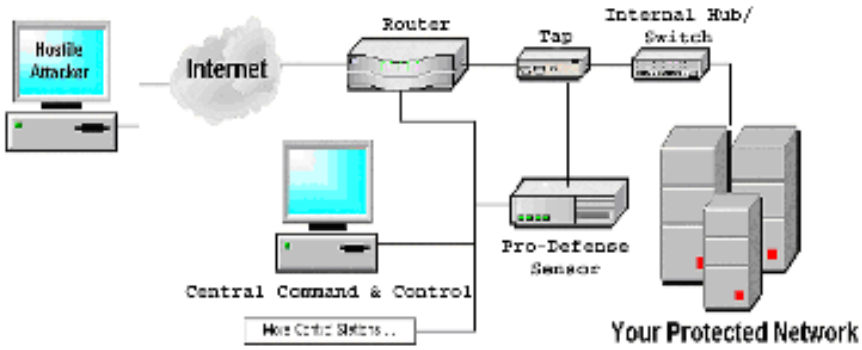
مسیریاب ها و فایروال ها

روتر ها می توانند طوری پیکربندی شوند که از حملات ساده ping با فیلترکردن پروتکل های غیرضروری جلوگیری کنند و می توانند آدرس های IP نامعتبر را نیز متوقف کنند. بهرحال، روترها معمولاً در مقابل حمله جعل شده پیچیده تر و حملات در سطح Application با استفاده از آدرس های IP معتبر، بی تأثیر هستند.

سیستم های کشف نفوذ

روش های سیستم های کشف نفوذ (intrusion detection systems) توانایی هایی ایجاد می کند که باعث تشخیص استفاده از پروتکل های معتبر بعنوان ابزار حمله می شود. این سیستمها می توانند بهمراه فایروال ها بکار روند تا بتوانند بصورت خودکار

در مواقع لزوم ترافیک را مسدود کنند. در بعضی مواقع سیستم تشخیص نفوذ نیاز به تنظیم توسط افراد خبره امنیتی دارد و البته گاهی در تشخیص نفوذ دچار اشتباه می شود.



سرورها

پیکربندی مناسب applicationهای سرویس دهنده در به حداقل رساندن تأثیر حمله DDoS تأثیر بسیار مهمی دارند. یک سرپرست شبکه می تواند بوضوح مشخص کند که یک application از چه منابعی می تواند استفاده کند و چگونه به تقاضاهای کلاینت ها پاسخ دهد. سرورهای بهینه سازی شده، در ترکیب با ابزار تخفیف دهنده، می توانند هنوز شانس ادامه ارائه سرویس را در هنگامی که مورد حمله DDoS قرار می گیرند، داشته باشند.

ابزار تخفیف DDoS

چندین شرکت ابزارهایی تولید می کنند که برای ضدعفونی ! کردن ترافیک یا تخفیف حملات DDoS استفاده می شوند که این ابزار قبلاً بیشتر برای متعادل کردن بار شبکه یا فایروالینگ استفاده می شد. این ابزارها سطوح مختلفی از میزان تأثیر دارند. هیچکدام کامل

نیستند. بعضی ترافیک قانونی را نیز متوقف می کنند و بعضی ترافیک غیرقانونی نیز اجازه ورود به سرور پیدا می کنند. زیرساخت سرور هنوز باید مقاوم تر شود تا در تشخیص ترافیک درست از نادرست بهتر عمل کند.

پهنای باند زیاد

خرید یا تهیه پهنای باند زیاد یا شبکه های افزونه برای سروکار داشتن با مواقعی که ترافیک شدت می یابد، می تواند برای مقابله با DDoS مؤثر باشد.

عموماً، شرکت ها از قبل نمی دانند که یک حمله DDoS بوقوع خواهد پیوست. طبیعت یک حمله گاهی در میان کار تغییر می کند و به این نیاز دارد که شرکت بسرعت و بطور پیوسته در طی چند ساعت یا روز، واکنش نشان دهد. از آنجا که تأثیر اولیه بیشتر حملات، مصرف کردن پهنای باند شبکه شماست، یک ارائه کننده سرویس های میزبان روی اینترنت که بدرستی مدیریت و تجهیز شده باشد، هم پهنای باند مناسب و هم ابزار لازم را در اختیار دارد تا بتواند تأثیرات یک حمله را تخفیف دهد.

روش‌های معمول حمله به کامپیوترها (۱)

روش‌هایی که مورد استفاده خرابکاران برای ورود به کامپیوتر یا از کارانداختن آن قرارمی‌گیرد، بشرح ذیل میباشد.

۱- برنامه‌های اسب تروا

۲- درهای پشتی و برنامه‌های مدیریت از راه دور

۳-عدم پذیرش سرویس

۴- وساطت برای یک حمله دیگر

۵- اشتراکهای ویندوزی حفاظت‌نشده

۶- کدهای قابل انتقال (Java ، JavaScript و ActiveX)

۷- اسکریپتهای Cross-Site

۸- ایمیلهای جعلی

۹- ویروسهای داخل ایمیل

۱۰- پسوندهای مخفی فایل

۱۱- سرویس‌گیرندگان چت

۱۲- شنود بسته‌های اطلاعات

۱- برنامه‌های اسب تروا

برنامه‌های اسب تروا روشی معمول برای گول زدن شما هستند (گاهی مهندسی اجتماعی نیز گفته می‌شود) تا برنامه‌های "درپشتی" را روی کامپیوتر شما نصب کنند. و به این ترتیب اجازه دسترسی آسان کامپیوترتان را بدون اطلاعتان به مزاحمین می‌دهند، پیکربندی سیستم شما را تغییر می‌دهند، یا کامپیوترتان را با یک ویروس آلوده می‌کنند.

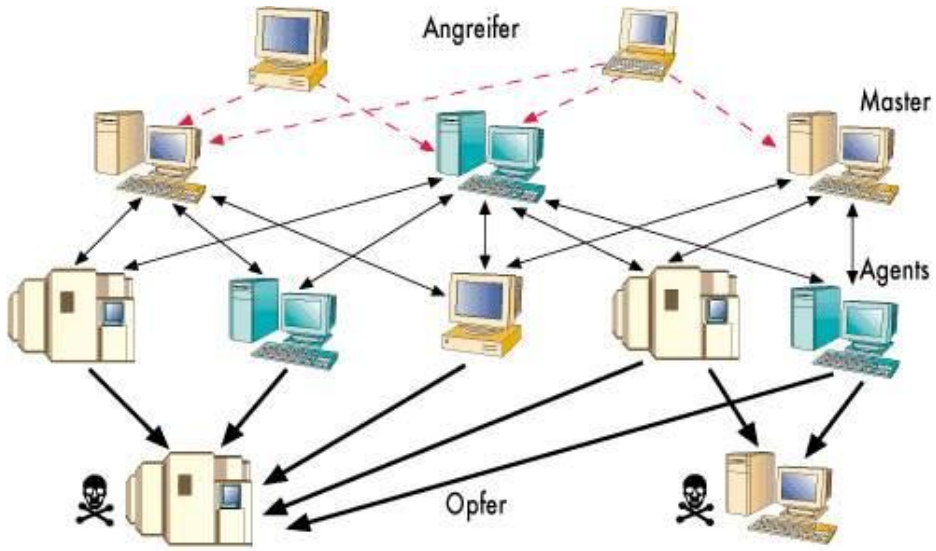
۲- درهای پشتی و برنامه‌های مدیریت از راه دور

روی کامپیوترهای ویندوزی، معمولا سه ابزار توسط مزاحمین برای دسترسی از راه دور به کامپیوترتان استفاده می‌شود. BackOrifice ، Netbus و SubSeven. این برنامه‌های درپشتی یا مدیریت از راه‌دور وقتی نصب می‌شوند، به افراد دیگر اجازه دسترسی و کنترل کامپیوترتان را می‌دهند. به شما توصیه می‌کنیم که شکاف‌های امنیتی را بخصوص در مورد BackOrifice از CERT مطالعه کنید.

۳- عدم پذیرش سرویس

نوعی دیگر از حمله، Denial-of-Service یا عدم‌پذیرش‌سرویس نام دارد. این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از حد کامپیوتر تا حد غیرقابل‌استفاده

شدن می‌شود. در بیشتر موارد، آخرین وصله‌های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می‌گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود.



۴- وساطت برای یک حمله دیگر

مزاحمین به‌کرات از کامپیوترهای مورد حمله قرارگرفته برای پایگاهی برای حمله به سیستم‌های دیگر استفاده می‌کنند. یک مثال آن چگونگی استفاده از آنها بعنوان ابزار حملات DoS توزیع‌شده است. مزاحمین یک "عامل" را (معمولا از طریق یک اسب تروا) نصب می‌کنند که روی کامپیوتر مورد حمله قرارگرفته اجرا می‌شود و منتظر دستورهای بعدی می‌ماند. سپس، هنگامی که تعدادی از عامل‌ها روی کامپیوترهای مختلف در حال اجرا هستند، به تمام آنها دستور داده می‌شود که یک حمله denial-of-service را روی یک سیستم پیاده کنند. بنابراین، هدف نهایی حمله، کامپیوتر شما

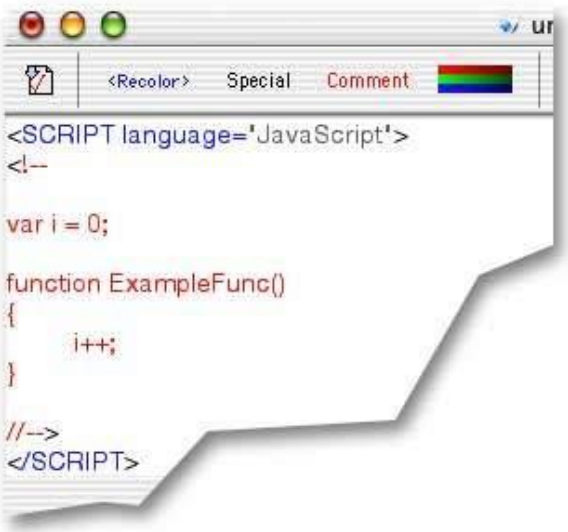
نیست، بلکه سیستم شخص دیگری است – کامپیوتر شما فقط یک ابزار مناسب برای یک حمله بزرگتر است.

۵- اشتراکهای ویندوزی حفاظت‌نشده

اشتراکهای شبکه ویندوزی محافظت‌نشده می‌توانند توسط مزاحمین تحت یک روش خودکار برای قراردادن ابزارها روی تعداد زیادی از کامپیوترهای ویندوزی متصل به اینترنت مورد سوءاستفاده قرار گیرند. از آنجا که برای امنیت سایت روی اینترنت وابستگی بین سیستمها وجود دارد، یک کامپیوتر مورد حمله قرارگرفته نه تنها مشکلاتی برای صاحبش فراهم می‌کند، بلکه تهدیدی برای سایتهای دیگر روی اینترنت محسوب می‌شود. عامل بالقوه بزرگی در گستره وسیع برای ظهور ناگهانی سایر ابزارهای مزاحمت وجود دارد که از اشتراکهای شبکه ویندوزی محافظت‌نشده استفاده می‌کند.

۶- کدهای قابل انتقال (Java ، JavaScript و ActiveX)

گزارشهایی در مورد مشکلات با " کدهای سیار" (مانند Java، JavaScript و ActiveX) وجود داشته است. اینها زبانهای برنامه‌سازی هستند که به توسعه‌دهندگان وب اجازه نوشتن کدهای قابل اجرا در مرورگر شما را می‌دهند. اگرچه کد عموما مفید است، اما می‌ؤواند توسط مزاحمان برای جمع‌آوری اطلاعات (مثلا وب‌سایتهایی که سر می‌زنید) یا اجرای کدهای آسیب‌رسان روی کامپیوتر شما مورد استفاده قرار گیرد. امکان از کار انداختن Java، JavaScript و ActiveX در مرورگر شما وجود دارد. توصیه می‌شود که اگر در حال مرور وب‌سایتهایی هستید که با آنها آشنا نیستید یا اطمینان ندارید، این کار را انجام دهید، اگرچه از خطرات احتمالی در استفاده از کدهای سیار در برنامه‌های ایمیل آگاه باشید. بسیاری از برنامه‌های ایمیل از همان کد بعنوان مرورگرهای وب برای نمایش HTML استفاده می‌کنند. بنابراین، شکافهای امنیتی که بر Java، JavaScript و ActiveX اثرگذارند، اغلب علاوه بر صفحات وب در ایمیلها هم قابل اجرا هستند.



در قسمت بعد به ادامه روشها پرداخته خواهد شد...

در قسمت قبل به ۶ روش حمله بطور مختصر پرداختیم ...

۷- اسکریپتهای Cross-Site

یک برنامه نویس وب با افکار بدخواهانه ممکن است اسکریپتی به آنچه که به یک وب سایت فرستاده می شود، مانند یک URL ، یک عنصر در شکلی خاص، یا درخواست از یک پایگاه داده، بچسباند. بعدا، وقتی وب سایت به شما پاسخ می دهد، اسکریپت زیان رسان به مرورگر شما منتقل می شود.

شما می توانید مرورگر وب تان را توسط روشهای زیر در اختیار اسکریپتهای زیان رسان قرار دهید:

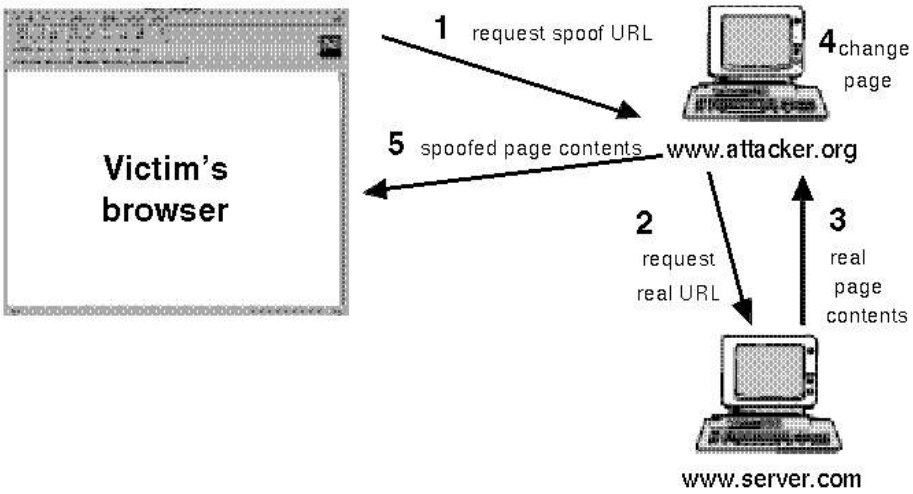
× تعقیب لینک ها در صفحات وب، ایمیلها یا پیام های گروه های خبری بدون دانستن به آنچه لینک داده شده است.

× استفاده از فرم های محاوره ای روی یک سایت غیرقابل اطمینان

× دیدن گروه های بحث آنلاین، مجمع ها یا دیگر صفحاتی که بصورت پویا تولید می شوند در جایی که کاربران می توانند متنهای شامل تگ های HTML ارسال کنند.

۸- ایمیلهای جعلی

این حالت زمانی اتفاق می افتد که یک ایمیل به ظاهر متعلق به منبعی می باشد درحالیکه در حقیقت از منبعی دیگر ارسال شده است. Email Spoofing اغلب برای گول زدن کاربر بمنظوراین که اطلاعات حساس (مانند کلمات عبور) را افشاء کند بکار می رود.



ایمیل جعل شده می تواند گستره ای از شوخی های بی ضرر تا اقدامات مربوط به مهندسی اجتماعی داشته باشد. مثالهایی از مورد دوم اینها هستند:

× ایمیل ادعا می کند که از مدیر یک سیستم است و از کاربران تقاضای تغییر کلمات عبورشان را به یک رشته مشخص دارد و آنها را در صورت عدم تابعیت به تعلیق اکانتهایشان تهدید می کند.

× ایمیل ادعا می کند از یک شخص با اختیارات لازم است و از کاربران تقاضا می کند که یک کپی از فایل کلمات عبور یا سایر اطلاعات حساس را برایش ارسال کنند.

توجه کنید وقتی سرویس دهندگان گهگاهی تقاضا می کنند که کلمه عبورتان را تغییر دهید، معمولا مشخص نمی کنند که به چه کلمه ای تغییر کند. همچنین، بیشتر سرویس دهندگان قانونی از شما هرگز تقاضای ارسال کلمات عبورتان را از طریق ایمیل نمی کنند. اگر شک دارید که یک ایمیل جعلی از شخصی با تمایلات بدخواهانه دریافت کرده اید، باید با پرسنل پشتیبانی سرویس دهنده خود سریعا تماس بگیرید.

۹- ویروسهای داخل ایمیل

ویروس ها و سایر کدهای آسیب رسان اغلب بعنوان پیوست ایمیلها گسترش می یابند. قبل از بازکردن هر پیوستی، از شناخته شده بودن منبع آن اطمینان حاصل کنید. اینکه ایمیل از آدرسی باشد که شما می شناسید، کافی نیست. ویروس ملیسا دقیقا به این علت گسترش یافت که آدرس فرستنده آن آشنا بود. همچنین، کدهای آسیب رسان ممکن است در برنامه های سرگرم کننده یا فریبنده گسترش پیدا کنند.

هرگز برنامه ای را اجرا نکنید، مگر اینکه توسط شخص یا شرکتی نوشته شده باشد که به آن اعتماد دارید. بعلاوه، برنامه هایی را که از منابع ناشناخته دریافت می کنید، صرفا بخاطر اینکه سرگرم کننده هستند، برای دوستان یا همکاران خود ارسال نکنید.

۱۰- پسوندهای مخفی فایل

سیستم عاملهای ویندوز انتخابی را در اختیار شما قرار می دهند که " پسوند فایلهایی که نوع آنها شناخته شده است را پنهان می کند". این انتخاب بصورت پیش فرض فعال است، اما ممکن است یک کاربر این قابلیت را بمنظور به نمایش درآمدن پسوند تمام فایلها توسط ویندوزغیرفعال کند. ویروسهای داخل ایمیل از پنهان ماندن پسوند فایلهای شناخته شده بهره برداری می کنند. اولین حمله عمده که از این قابلیت بهره گرفت کرم VBS/LoveLetter بود که حاوی یک پیوست به نام "LOVE-LETTER-FOR-YOU.TXT.vbx" بود. سایر برنامه های آسیب رسان چنین طرحهای نامگذاری مشابهی دارند. چندین مثال اینها هستند:

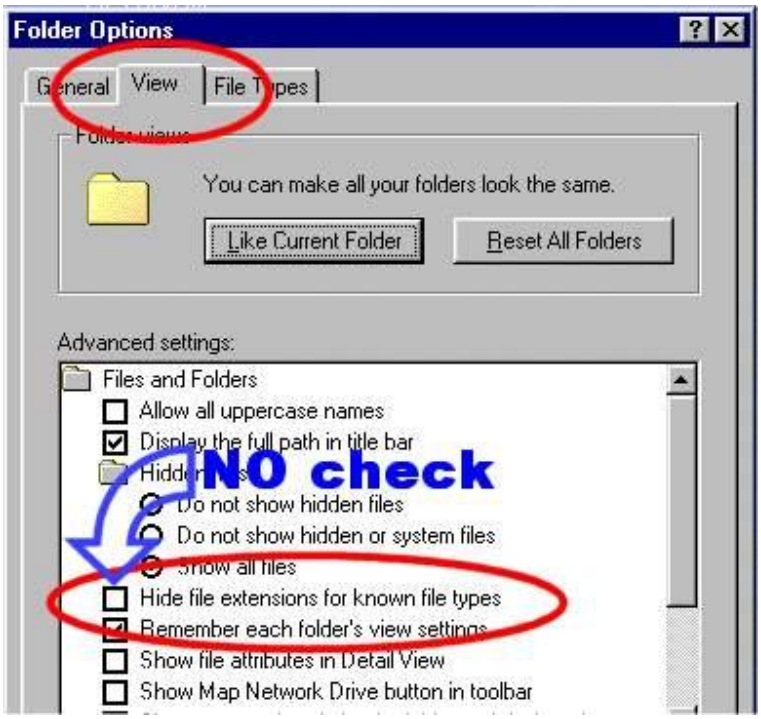
Downloader (MySis.avi.exe or QuickFlicking.mpg.exe)×

VBS/Timofonica (TIMOFONICA.TXT.vbs)×

VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)×

VBS/OnTheFly (AnnaKournikova.jpg.vbs)×

فایلهای پیوسته به ایمیلها که توسط این ویروسها فرستاده می شوند، ممکن است بی ضرر بنظر برسند، فایلهای متنی (.txt)، فایلهای تصویری (.mpg یا .avi) یا دیگر انواع فایل در حالیکه در حقیقت این فایل یک اسکریپت یا فایل اجرایی آسیب رسان است (برای مثال .vbs یا .exe)



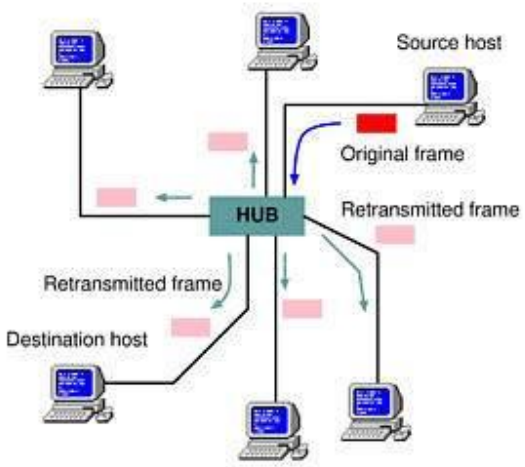
۱۱- سرویس گیرندگان چت

برنامه های چت اینترنتی، مانند برنامه های پیام رسانی سریع و شبکه های IRC، مکانیسمی را فراهم می کنند تا اطلاعات بصورت دوطرفه بین کامپیوترهای متصل به اینترنت منتقل شود. برنامه های چت برای گروههایی از افراد، امکان مکالمه، تبادل URL و در بسیاری موارد انتقال انواع فایلها را فراهم می کنند.

چون بسیاری از برنامه های چت اجازه تبادل کدهای قابل اجرا را می دهند، خطراتی مشابه برنامه های انتقال ایمیل را ایجاد می کنند. مانند برنامه های ایمیل، باید دقت کافی برای محدودکردن توانایی برنامه های چت برای اجرای فایلهای دانلود شده، بکار گرفته شود. مثل همیشه، باید مواظب تبادل فایل با طرفهای ناشناس باشید.

۱۲- شنود بسته های اطلاعات

یک برنامه شنود بسته های اطلاعاتی، برنامه ای است که دیتا را از اطلاعاتی که در حال انتقال در روی شبکه هستند، در اختیار می گیرد. این دیتا ممکن است شامل نام کاربران، کلمات عبور و هر اطلاعات اختصاصی دیگری باشد که روی شبکه و بدون اینکه رمز شده باشند، حرکت می کنند. با شاید صدها یا هزاران کلمات عبور گرفته شده توسط این برنامه، مزاحمین می توانند حملات گسترده ای را روی سیستمها پیاده کنند. نصب چنین برنامه ای لزوما به سطح دسترسی مدیر احتیاج ندارد.



نسبت به کاربران DSL و خطوط تلفن سنتی، کاربران مودمهای کابلی در معرض خطر بیشتری برای شنود قرار دارند، زیرا که تمام کاربران مودمهای کابلی همسایه بخشی از یک LAN هستند. یک برنامه شنود نصب شده روی کامپیوتر هر کاربر مودم کابلی ممکن است بتواند دیتا ارسال شده توسط هر مودم کابلی دیگر را در همان همسایگی دریافت کند.

از کوکی چه می‌دانید؟

کوکی چیست؟

«کوکی» بخش کوچکی از اطلاعات فرستاده شده توسط وب‌سرور برای ذخیره در مرورگر است تا بتواند بعدا از طریق آن مرورگر، دوباره خوانده شود. دیتای ذخیره شده برای اینکه وب‌سرور یک سایت، اطلاعات مشخصی را درباره بازدیدکننده آن وب‌سایت خاص بداند، مفید است. کوکی فرمت فایل متنی را دارد که در دایرکتوری مربوط به مرورگر ذخیره می‌شود و در هنگامی که مرورگر در حال اجراست در حافظه RAM قرار می‌گیرد. این اطلاعات می‌تواند هنگامی که کاربر از وب‌سایت خاصی خارج شد، در هارد درایو ذخیره شود. کوکی‌ها ابزار بسیار مهمی برای نگهداشتن state روی وب هستند. state به توانایی یک برنامه برای کار با کاربر بصورت محاوره‌ای اشاره دارد. برای مثال، شما برای استفاده از قطار یا اتوبوس بلیت رزرو می‌کنید. در روز سفر، هنگامی که بلیت را نشان می‌دهید، اجازه خواهید یافت که وارد قطار یا اتوبوس شوید، در غیراینصورت مسوول وسیله نقلیه نمی‌داند که آیا شما این اجازه را دارید یا خیر. در حقیقت در اینجا بلیت برای نگهداشتن state بین شما و مسوول قطار مهم است. HTTP یک پروتکل بدون قابلیت state است. به این معنی که هر بار مشاهده یک سایت توسط سرور بعنوان اولین مشاهده کاربر تلقی می‌شود. به این معنی که سرور همه چیز را بعد از هر درخواست فراموش می‌کند، مگر اینکه یک بازدیدکننده برای یادآوری آینده به سرور به طریقی مشخص گردد. کوکی‌ها این کار را انجام می‌دهند.

کوکی‌ها فقط می‌توانند به وب‌سرور بگویند که آیا شما قبلا هم از سایت دیدن کرده‌اید و اطلاعات کمی (مثلا یک شماره کاربر) در مرتبه بعد که از سایت دیدن می‌کنید از خود وب‌سرور به آن برگردانند. بیشتر کوکی‌ها هنگامی که از مرورگر خارج می‌شوید از بین می‌روند. نوع دیگری از کوکی‌ها بعنوان کوکی ماندگار وجود دارند که تاریخ انقضاء دارند و تا آن تاریخ روی هارددرایو شما باقی می‌مانند. کوکی ماندگار می‌تواند برای ردگیری عادات وبگردی یک کاربر با مشخص‌کردن وی هنگام مراجعه مجدد به یک سایت مورد استفاده قرار گیرد. اطلاعات در مورد اینکه اهل کجا هستید و به چه صفحات وبی سر می‌زنید در فایلهای لاگ یک وب‌سرور وجود دارد و می‌تواند برای ردگیری رفتار وبگردی کاربران مورد استفاده قرار گیرند، اما کوکی‌ها آن را آسانتر می‌کنند.

چگونه می‌توان از وجود کوکی‌های ماندگار روی سیستم مطلع شد؟

کوکی‌های ماندگار در مکانهای مختلفی روی سیستم شما بسته به مرورگر وب و نسخه‌ای از آن که استفاده می‌کنید، ذخیره می‌شوند. نت‌اسکیپ تمام کوکی‌های ماندگارش را در فایلی به نام cookies.txt روی کامپیوتر شما در دایرکتوری نت‌اسکیپ ذخیره می‌کند. می‌توانید این فایل را با یک ویرایشگر متن باز و ویرایش کنید و یا هر کوکی را که نمی‌خواهید نگهدارید، پاک کنید و چنانچه می‌خواهید از دست تمام کوکی‌ها خلاص شوید، فایل را پاک کنید. اینترنت‌اکسپلورر کوکی‌های ماندگار را در فایلهای جداگانه ذخیره می‌کند و توسط نام کاربر و نام دامنه سایتی که کوکی را فرستاده است، نامگذاری می‌کند. برای مثال john@wsiac.txt . این کوکی‌ها در دایرکتوری

/Windows/cookies یا /Windows/profiles/cookies ذخیره می‌شوند.

می‌توانید هرکدام از این کوکی‌ها را که نمی‌خواهید، پاک کنید. می‌توانید این فایلها را بازکنید تا ببینید از کجا آمده‌اند و چه اطلاعاتی دارند. برای مثال آنچه می‌بینید محتویات یک کوکی IE هستند.

WEBTRENDS_ID
61.1.129.58-1041789995.121030
www.bazwe.com/
1024
3872737152
30271763
3731731632
29537508

این فایل کوکی abishek@www.birt.txt (abishek شناسه فرد وارد شونده به سایت است) نامیده شده است. کوکی‌ها ممکن است اطلاعات مختلفی را دربرداشته باشند که بسته به کوکی متفاوت است. در این کوکی IP فرد نیز(61.1.129.58) ذخیره شده است. در اینجا قصد وارد شدن به جزئیات را نداریم.

Cookie:administrator@4icards	Cookie:administrator@4icards.c...	Text Document	1 KB	1/1/2005 8:30 AM
Cookie:administrator@atdmt	Cookie:administrator@atdmt.com/	Text Document	1 KB	6/28/2009 3:30 AM
Cookie:administrator@baazee	Cookie:administrator@baazee.c...	Text Document	1 KB	7/5/2005 6:38 PM
Cookie:administrator@babylon	Cookie:administrator@babylon.c...	Text Document	1 KB	1/1/2100 3:30 AM
Cookie:administrator@bonzi	Cookie:administrator@bonzi.com/	Text Document	1 KB	7/5/2004 6:07 PM
Cookie:administrator@dp.information	Cookie:administrator@dp.inform...	Text Document	1 KB	7/6/2004 1:42 PM
Cookie:administrator@fastclick	Cookie:administrator@fastclick....	Text Document	1 KB	6/24/2006 5:59 PM
Cookie:administrator@google	Cookie:administrator@google.com/	Text Document	1 KB	1/17/2038 10:44 ...
Cookie:administrator@ittoolbox	Cookie:administrator@ittoolbox....	Text Document	1 KB	7/5/2008 7:30 AM
Cookie:administrator@microsoft	Cookie:administrator@microsoft...	Text Document	1 KB	10/3/2006 10:30 ...
Cookie:administrator@passport	Cookie:administrator@passport....	Text Document	1 KB	12/30/2037 7:30 ...
Cookie:administrator@revenue	Cookie:administrator@revenue....	Text Document	1 KB	6/10/2022 8:35 AM
Cookie:administrator@search.domainsponsor	Cookie:administrator@search.d...	Text Document	1 KB	7/6/2004 1:43 PM
Cookie:administrator@search.information	Cookie:administrator@search.in...	Text Document	1 KB	7/6/2004 1:42 PM
Cookie:administrator@securitydocs	Cookie:administrator@securityd...	Text Document	1 KB	1/18/2038 3:30 AM
Cookie:administrator@securityfocus	Cookie:administrator@securityf...	Text Document	1 KB	1/1/2011 3:30 AM
Cookie:administrator@www.baazee	Cookie:administrator@www.baa...	Text Document	1 KB	7/3/2014 5:39 PM
Cookie:administrator@www.google	Cookie:administrator@www.goo...	Text Document	1 KB	6/29/2005 12:39 ...
Cookie:administrator@www.securityfocus	Cookie:administrator@www.sec...	Text Document	1 KB	7/3/2014 2:46 PM
Cookie:administrator@yahoo	Cookie:administrator@yahoo.com/	Text Document	1 KB	1/1/2038 3:30 AM
Cookie:administrator@z1.adserver	Cookie:administrator@z1.adser...	Text Document	1 KB	7/5/2005 3:29 PM

کوکی‌ها برای چه استفاده می‌شوند؟

یک استفاده از کوکی‌ها برای ذخیره کلمات عبور و شناسه‌های برای وب‌سایتهای خاص است. همچنین برای ذخیره اولویتهای کاربران در صفحات آغازین نیز استفاده می‌شوند. در این حالت مقداری از هارد کامپیوتر شما برای ذخیره این اطلاعات از مرورگرتان تقاضا می‌شود. بدین طریق، هر زمان که به آن وب‌سایت وارد می‌شوید مرورگر شما بررسی می‌کند که ببیند آیا الویتهای از پیش تعیین‌شده (کوکی) برای آن سرور مشخص دارید یا خیر. اگر اینطور باشد، مرورگر کوکی را همراه با تقاضای شما برای صفحه وب، به وب‌سرور ارسال خواهد کرد. مایکروسافت و نت‌اسکیپ از کوکی‌هایی برای ایجاد صفحات آغازین شخصی روی وب‌سایتهایشان استفاده می‌کنند. استفاده‌های معمول که

شرکتها بخاطر آنها از کوکی استفاده می‌کنند شامل سیستمهای سفارش آنلاین، شخصی‌سازی سایتها و ردگیری وب‌سایتها می‌شود. کوکی‌ها منافعی دارند. شخصی‌سازی سایت یکی از مفیدترین استفاده‌های کوکی‌ها است. برای مثال، فردی وارد سایت CNN (یا حتی MyYahoo) می‌شود اما نمی‌خواهد اخبار تجاری را ببیند. این سایت به فرد اجازه این انتخاب را می‌دهد. از این به بعد (یا تا زمانیکه کوکی منقضی می‌شود) این شخص اخبار تجاری را وقتی به سایت CNN متصل می‌شود، نمی‌بیند. حتما تا حالا دیده‌اید که در بعضی وب‌سایتها هنگامی که با استفاده از شناسه و گذرواژه وارد می‌شوید، انتخابی تحت عنوان «مرا دفعه بعد بخاطر داشته باش» وجود دارد. این امر با ذخیره شدن شناسه و کلمه عبور شما در یک کوکی روی کامپیوترتان، میسر می‌شود. بعضی بازدیدکنندگان آن را بعنوان تعرض به حریم خصوصی می‌پندارند برای وب‌سایتهایی که روند فعالیتشان روی یک سایت را ردگیری می‌کنند. این کمک می‌کند که اطلاعات و سرویس‌های مورد جستجو را بسرعت بیابید و بدون تاخیر به سر کار اصلی خودتان برگردید. آمار برای طراحی مجدد سایت بسیار مهم هستند. گاهی مدیر سایت نیاز دارد بداند آیا ۱۰۰ نفر مختلف از سایتش بازدید کرده‌اند یا فقط یک فرد (یا روبات) بطور پیوسته ۱۰۰ مرتبه دکمه reload (یا refresh) را انتخاب کرده است. کوکی‌ها کاربردهای دیگری نیز دارند و یکی از آنها امکان ردگیری فعالیت کاربران است. اجازه دهید که یک مثال را ببینیم. DoubleClickNetwork سیستمی است که توسط DoubleClickCorporation ایجاد شده است تا پروفایل افرادی را

که از وب استفاده می‌کنند ایجاد کند و آگهی‌های تجاری متناسب با علاقه‌شان را به آنها ارائه کند. مشتری‌های DoubleClick وب‌سایتهایی هستند که قصد تبلیغ خدماتشان را دارند. هر عضو این شبکه میزبانی برای تبلیغ سایر اعضاء می‌شود. هر وب‌سایت که عضو می‌شود تبلیغ خود را ایجاد و در اختیار سرور DoubleClick قرار می‌دهد. هنگامی که یک کاربر به یکی از این سایتها می‌رود، یک آگهی از سایر سایتها نیز در HTML ارائه شده به کاربر وجود دارد. با هربار بارگذاری مجدد صفحه، آگهی متفاتی به کاربر ارائه می‌شود. از نظر کاربران این تبلیغات با سایر تبلیغات تفاوتی ندارند، در حالیکه اینطور نیست. هنگامی که کاربری برای اولین بار به سرور DoubleClick متصل می‌شود، سرور یک کوکی برای آن مرورگر ایجاد می‌کند که یک شماره مشخصه یکتا در بردارد. از آن به بعد هر زمان که کاربر به یکی از وب‌سایتهای عضو DoubleClick متصل می‌شود، شماره مذکور به سرور ارسال می‌شود و کاربر تشخیص داده می‌شود. با گذشت زمان و داشتن اطلاع از سایتهایی که کاربر بازدید کرده است، پروفایلی از علائق کاربر در اختیار سرور قرار می‌گیرد. با داشتن این پروفایل، سرور DoubleClick می‌تواند تبلیغاتی را که بیشتر مورد نظر کاربر است انتخاب کند. بعلاوه می‌تواند از این اطلاعات برای دادن بازخورد مناسب به اعضا مانند پروفایل کاربران و میزان تاثیر تبلیغاتشان استفاده کند. برای اینکه بفهمید آیا توسط DoubleClick ردگیری شده‌اید یا نه، کوکی‌های مرورگر خود را امتحان کنید و ببینید آیا چیزی شبیه به این: ad.doubleclick.net FALSE / FALSE 942195440 IAA d2bbd5 در کوکی‌ها وجود دارد یا خیر.

کوکی‌ها و مسائل امنیتی

بررسی انواع کوکی

علاوه بر کوکی‌های **موقت** و **ماندگار** که در مقاله قبل در مورد آن صحبت شد، کوکی‌ها دسته‌بندی دیگری نیز دارند:

کوکی‌های **شخص‌اول!** در مقابل کوکی‌های **شخص‌ثالث**: یک کوکی شخص‌اول از وب‌سایتی نشات می‌گیرد یا به آن فرستاده می‌شود که در آن زمان در حال مشاهده آن هستید. این کوکی‌ها معمولا برای ذخیره اطلاعات مانند اولویتهای شما استفاده می‌شوند. یک کوکی شخص ثالث از وب‌سایت متفاوت با آنچه در حال مشاهده آن هستید نشات می‌گیرد یا به آن فرستاده می‌شود. وب‌سایتهای شخص‌ثالث معمولا محتویاتی روی وب‌سایتی که در حال مشاهده هستید، ارائه می‌کنند. برای مثال، بسیاری سایتها از تبلیغات وب‌سایتهای شخص‌ثالث استفاده می‌کنند و آن وب‌سایتها ممکن است از کوکی استفاده کنند. یک استفاده معمول برای این نوع از کوکی ردیابی استفاده از صفحه‌وب شما برای تبلیغات یا سایر مقاصد بازاریابی است. این نوع کوکی‌ها می‌توانند موقت یا ماندگار باشند.

نوعی از کوکی‌ها هستند که بعنوان کوکی‌های **ناخوشایند** نامیده می‌شوند. کوکی‌هایی هستند که ممکن است اجازه دسترسی به اطلاعات شخصا قابل‌شناسایی شما را برای اهداف ثانویه بدون اجازه شما، فراهم کنند.

مزایا و معایب کوکی‌ها از دید کاربران اینترنت

اگرچه خیلی‌ها از کوکی‌ها تصورات بدی دارند، اما اکنون می‌دانید که کابردهای خوبی نیز دارند. بسیاری از افراد کوکی‌ها را دوست ندارند زیرا آنها را ابزار "بردار بزرگ" (کسی که همواره ناظر بر اعمال و رفتار آنهاست) می‌دانند. بعبارتی بعلت ردیابی شدن توسط کوکی‌ها، به آنها سوءظن دارند. این افراد باید بدانند که این نوع ردگیری می‌تواند توسط تکنیک‌های دیگر نیز انجام گیرد، اما از کوکی‌ها بدلیل ثبات بیشتر آنها نسبت به سایر روش‌ها استفاده می‌شود. برای آنان که دوست ندارند دیگران بدانند در اینترنت چه می‌کنند یا به کدام سایتها سر می‌زنند، این امر مساله ساز است.

مردم همچنان کوکی‌ها دوست ندارند، زیرا آنها را موجوداتی "آب‌زیرکاه" می‌دانند. مگر اینکه نسخه‌های جدید مرورگرها را داشته باشید تا بتوانید با تنظیماتی که انجام می‌دهید از

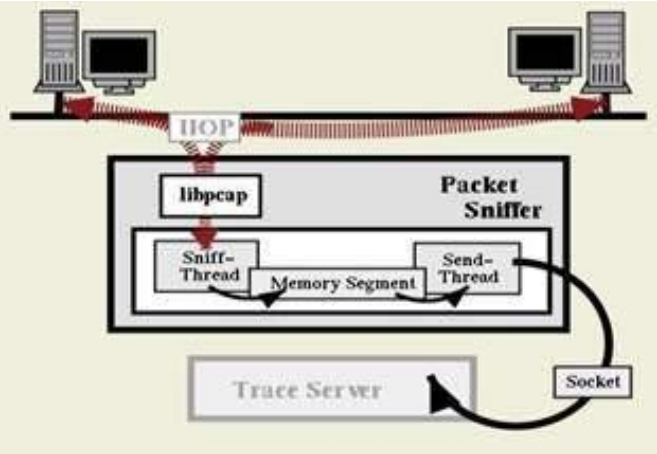
ورود آنها مطلع شوید، در غیر اینصورت آنها بدون هیچ نشانی وارد هارد شما می‌شوند. سیس می‌توانند بدون اطلاع کاربر کارهای خاصی انجام دهند (شاید هدف قرار دادنتان برای اعمال تبلیغاتی).

بهرحال فکر کردن به این موضوع خوشایند نیست که در آینده نزدیک علائق خصوصی ما ممکن است برای کسانی که دوست نداریم، فاش شود. این نگرانی و عیب اصلی کوکی‌هاست. تقریبا قرار دادن ویروس از طریق کوکی فعلا ممکن نیست و جای نگرانی

ندارد. همچنین کوکی‌ها نمی‌توانند به هارد شما صدمه وارد کنند، یا از آنچه روی هارد خود دارید، تصویری تهیه کنند یا هر کار دیگری شبیه اینها. **کوکی‌ها فقط آنچه را شما به آنها می‌گویید، میدانند**. بهرحال اگر شما اطلاعاتی را در وب‌سایتی وارد کنید، مطمئنا در جایی در یک کوکی قرار خواهد گرفت. جایگزینهای آینده بجای کوکی‌ها باید با آغوش باز پذیرفته شود و اگرچه ممکن است همه چیز را حل نکنند، اما بعضی از نگرانیها را از بین خواهند برد.

مسائل امنیتی مربوط به کوکی‌ها

کوکی‌ها باعث بعضی خطرات امنیتی می‌شوند. می‌توانند توسط افرادی که بسته‌های اطلاعاتی را شنود می‌کنند برای اهداف غیراخلاقی استفاده شوند و باعث دسترسی غیرمجاز به وب‌سایت‌ها یا تراکنش‌های غیرمجاز شوند. (یک سیستم شنود، کامپیوتری است که نرم‌افزارهایی را اجرا می‌کند تا تمام بسته‌های TCP/IP وارد و خارج‌شونده را بررسی کند)



ایجادکنندگان وب‌سایتها کوکی‌ها را می‌سازند تا امکان دسترسی بهتر به سایتشان را فراهم کنند، یا در انواع دیگر تراکنش با سرورشان استفاده می‌شوند. آنها باید از امکان وقوع این امر مطلع باشند و سیستم را طوری طراحی کنند تا خطر را به حداقل ممکن برسانند.

چند مورد وجود دارد که ایجادکننده وب‌سایت می‌تواند انجام دهد:

- مطمئن شود که کوکی‌ها کمترین اطلاعات خصوصی را دربردارند.
- مطمئن شود که اطلاعات حساس قرارگرفته در کوکی‌ها همیشه رمزنگاری می‌شود. (هرگز و هرگز شناسه‌ها و کلمات عبور نباید بصورت متن رمزنشده استفاده و ذخیره شوند)• کل کوکی را رمز کند.

کوکی‌ها باید اطلاعات کافی را برای تایید اینکه فرد استفاده کننده از کوکی، مجاز به استفاده از آن است، دارا باشند. بیشتر سایتهای استفاده‌کننده از کوکی، اطلاعات زیر را نیز لحاظ می‌کنند:

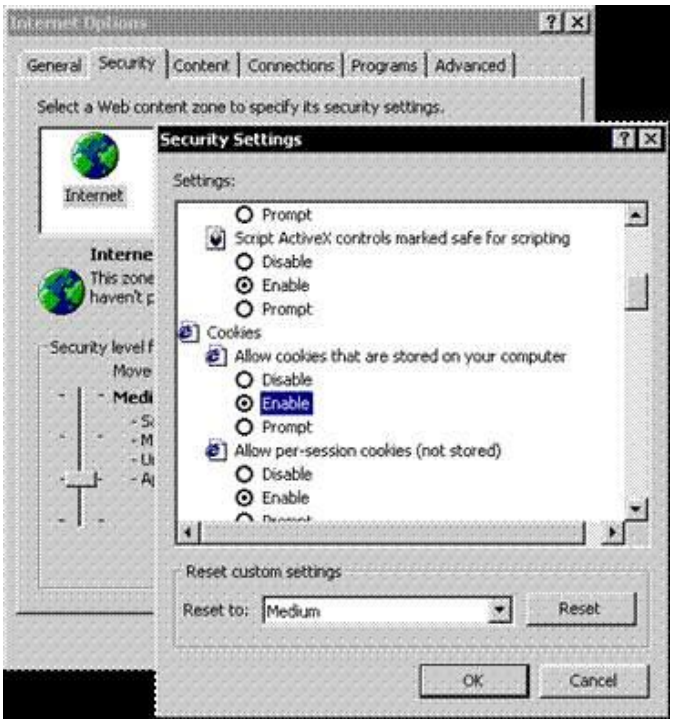
- اطلاعات لازم برای دادن اجازه به فرد
- ساعت و تاریخ
- آدرس IP استفاده کننده وب
- تاریخ انقضاء
- کد MAC (Message Authenticity Check)

قراردادن آدرس IP به این منظور است که کوکی تنها در صورتی تایید شود که آدرس IP ذخیره‌شده در سرور با آدرس IP مرورگر فرستنده کوکی یکسان باشد. تاریخ انقضاء مدت زمان استفاده از یک کوکی را محدود می‌کند و MAC تضمین می‌کند که کوکی دچار تغییر نشده است.

کد MAC شامل یک رشته ادغامی از فیلدهای داده در کوکی و یک رشته مخفی است که به آن اضافه می‌شود. اطلاعات کد می‌شود سپس مجددا ادغام می‌شود و دوباره کد می‌شود. نتیجه نهایی در داده کوکی قرار می‌گیرد. هنگامی که کوکی به سرور برمی‌گردد، سرور خود، MAC را تولید می‌کند و با MAC موجود در کوکی مقایسه می‌کند. در صورت یکسان بودن، نشانه عدم تغییر کوکی است.

کار با کوکی‌ها

مرورگرهای جدید اجازه نحوه کار با کوکی‌ها را به شما می‌دهند؛ می‌توانید تنظیمات مرورگر خود را طوری انجام دهید که به شما قبل از قراردادن کوکی روی کامپیوترتان خبر داده شود. (این کار به شما این امکان را می‌دهد که اجازه قراردادن کوکی را بدهید یا خیر)؛ همچنین می‌توانید توسط مرورگر خود جلوی ورود تمام کوکی‌ها را بگیرید.



بعنوان مثال در اینترنت اکسپلورر امکان تنظیم نحوه برخورد با کوکی‌ها از سایتهای مشخص گرفته تا کل سایتها وجود دارد. برای اطلاع یافتن بیشتر از نحوه کار با کوکی‌ها راهنمای مرورگر خود را مطالعه کنید.

محتویات فعال و کوکی

هر یک از ما در مدت زمان اتصال به اینترنت از وب سایت ها و یا وبلاگ های متعددی دیدن می نمائیم. طراحان و پیاده کنندگان وب سایت ها و وبلاگ ها به منظور ارائه خدمات مورد نظر خود از امکانات و یا بهتر بگوئیم تکنولوژی های متفاوتی استفاده می نمایند . اغلب ملاقات کننده گان، احساس خاصی نسبت به این تکنولوژی ها نداشته و صرفا" برای آنان نوع سرویس ها و خدمات ارائه شده دارای اهمیت است.

برخی از تکنولوژی های استفاده شده علیرغم داشتن جنبه های مثبت و مهم به ابزارهائی برای برنامه ریزی برخی حملات تبدیل شده و حریـــم خصوصی کاربران را به مخاطره می اندازد. محتویات فعال (Active contents) و کوکی ها (Cookies) از جمله موارد فوق، می باشند.

محتویات فعال چیست ؟

در اغلب وب سایت ها به منظور افزایش پتانسیل های قابل ارائه به کاربران و یا تزئین سایت از اسکریپت هائی که باعث اجرای برنامه ها بر روی مرورگر وب می شود، استفاده می گردد. ایجاد منوهای Drop-down و یا انجام افکت های گرافیکی متفاوت در یک صفحه وب، نمونه هائی در این زمینه می باشند. این نوع اسکریپت ها که به "محتویات فعال"معروف شده اند، اغلب به روشی برای انواع حملات نظیر سرقت اطلاعات و یا اجرای کدهای مخرب بر روی کامپیوتر کاربران، تبدیل شده اند.

- **جاوا اسکریپت** : جاوا اسکریپت یکی از متداولترین زبان های اسکریپت نویسی در وب است که در اکثر وب سایت ها از آن استفاده می گردد.

- (VBscript,ECMAScript و Jscript نمونه هائی دیگر در این زمینه می باشند). تامین طیف وسیعی از خواسته ها، عملکرد مناسب، سادگی در استفاده و ترکیب آسان با سایر نرم افزارها از جمله دلایل گسترش استفاده از زبان های اسکریپت نویسی در وب می باشد.مهاجمان نیز از پتانسیل های ارائه شده توسط زبان های اسکریپت نویسی به منظور نیل به اهداف مخرب خود استفاده می نمایند . مثلا" یکی از حملات متداول که با محوریت جاوا اسکریپت صورت می پذیرد، هدایت کاربران از یک وب سایت مطمئن به یک وب سایت مخرب است که در آن اقدام به download ویروس ها و یا جمع آوری اطلاعات شخصی کاربران می گردد.
- **اپلت های جاوا و کنترل های اکتیوایکس**: اپلت های جاوا و کنترل های اکتیوایکس برنامه هائی می باشند که بر روی کامپیوتر شما مستقر شده و یا از طریق شبکه بر روی مرورگر شما download می گردند. در صورتی که اینگونه برنامه ها (خصوصا" کنترل های اکتیوایکس) توسط مهاجمان مدیریت و هدایت گردند، امکان انجام هر گونه عملیاتی بر روی کامپیوتر شما وجود خواهد داشت. اپلت های جاوا معمولا" دریک محیط محدودتر اجراء می گردند. این نوع از برنامه ها در صورت عدم ایمنی مناسب محیط ایجاد شده، فرصت های مناسبی به منظور انواع حملات را برای مهاجمان فراهم می نمایند.

استفاده از جاوا اسکریپت، اپلت های جاوا و کنترل های اکتیوایکس، همواره خطرناک نمی باشد. ولی می بایست به این موضوع دقت شود که امکانات فوق به ابزارهائی برای انواع حملات توسط مهاجمان، تبدیل شده اند. به منظور پیشگیری در خصوص محتویات فعال ، امکانات متعددی در اکثر مرورگرها پیش بینی شده است که با استفاده از آنان و تنظیم بهینه پارامترهای موجود می توان یک سطح ایمنی مناسب را ایجاد نمود. بموازات افزایش ضریب ایمنی مرورگر خود به منظور برخوردبا محتویات فعال، ممکن است محدودیت های خاصی در خصوص برخی ویژگی های ارائه شده توسط برخی

سایت ها، ایجاد گردد. در صورتی که از یک وب سایت دیدن می نمائید که نسبت به آن شناخت کافی وجود ندارد، می بایست پیشگیری لازم در خصوص غیر فعال نمودن محتویات فعال را انجام داد. تهدیدات مشابهی نیز می تواند متوجه برنامه های پست الکترونیکی باشد. تعداد زیادی از برنامه های پست الکترونیکی از برنامه های مشابه مرورگرها به منظور نمایش HTML استفاده می نمایند . بنابراین امکان تهدید محتویات فعال در خصوص نامه های الکترونیکی نیز می تواند وجود داشته باشد. به منظور پیشگیری لازم در خصوص این نوع تهدیدات می توان پیام ها را به صورت متن معمولی، مشاهده نمود.

در زمان استفاده از اینترنت، امکان جمع آوری و ذخیره اطلاعات شما وجود خواهد داشت . اطلاعات فوق ممکن است اطلاعاتی عمومی در خصوص کامپیوتر شما نظیر آدرس IP ، نام Domain استفاده شده به منظور ارتباط با اینترنت، نوع مرورگر و سیستم عامل، باشد. اطلاعات جمع آوری شده می تواند شامل موارد خاصی نظیر آخرین مرتبه ای که یک وب سایت را ملاقات نموده اید و یا اطلاعات شخصی شما در زمان استفاده از یک وب سایت خاص نظیر آدرس پست الکترونیکی باشد.

- **Session cookie** . این نوع کوکی ها صرفا" و تا زمانی که از مرورگر استفاده می گردد، اطلاعاتی را ذخیره نموده و پس از بستن مرورگر اطلاعات از بین می رود. هدف از بکارگیری این نوع کوکی ها، ارائه تسهیلات لازم در خصوص حرکت بین صفحات متعدد است. مثلا" تشخیص مشاهده یک صفحه خاص و یا نگهداری اطلاعاتی در خصوص داده های مرتبط با یک صفحه.
- **cookie Presistent** : این نوع کوکی ها اطلاعاتی را بر روی کامپیوتر شما ذخیره می نمایند. بدین ترتیب امکان نگهداری اطلاعات شخصی مرتبط با شما فراهم می گردد . در اکثر مرورگرها برای این نوع از کوکی ها می توان یک مدت

- زمان خاص را مشخص نمود(عمر مفید). در صورتی که یک مهاجم امکان دستیابی به کامپیوتر شما را پیدا نماید، می تواند با مشاهده محتویات فایل های فوق به اطلاعات شخصی شما دسترسی نماید.

به منظور افزایش سطح ایمنی خود، می بایست تنظیمات امنیتی لازم در خصوص اعمال محدودیت و یا بلاک نمودن کوکی ها را در جهت حفظ حریم خصوصی، انجام داد. در صورتی که از یک کامپیوتر عمومی استفاده می نمائید، می بایست کوکی ها را غیر فعال نموده تا پیشگیری لازم در خصوص دستیابی سایرین به اطلاعات شخصی شما ، صورت پذیرد .

داده های حساس

فرض کنید هارددیسک کامپیوتر شما در اختیار فرد و یا افرادی دیگر قرار بگیرد، آیا آنان می توانند با بررسی آن اطلاعات خاصی در خصوص شما و نوع فعالیت هائی که انجام می دهید را کسب نمایند؟ در پاسخ می بایست با صراحت گفت که چنین امری میسر است و شاید بیش از آنچیزی که احتمال آن را می دهید. در این مطلب قصد داریم به بررسی این موضوع بپردازیم که چگونه یک کارشناس کالبد شکافی اطلاعات کامپیوتر قادر است داده هائی را که به نظر شما مدت ها است از روی کامپیوتر حذف و ظاهرا" اثری از آنان مشاهده نمی گردد را جان دوباره داده و از آنان استفاده نماید. بررسی این موضوع از دو زاویه می تواند مفید باشد: اول برای افرادی که قصد بازیافت اطلاعات(recovery) خود را دارند و دوم برای افرادی که می خواهند مقاومت سیستم خود را در مقابل بازبینی های غیرمجاز، افزایش دهند.

به منظور ایمن سازی کامپیوتر خود و حفاظت از اطلاعات حساس موجود بر روی آن لازم نیست که حتما" یک کارشناس حرفه ای کامپیوتر باشیم، با اندک دانشی نسبت به نحوه عملکرد سیستم عامل نصب شده بر روی کامپیوتر نظیر ویندوز، می توان اقدامات لازم در این خصوص را انجام داد. افشای اطلاعات حساس موجود بر روی هارددیسک، آگاهی از وب سایت های مشاهده شده و فایل هائی که از طریق اینترنت download شده اند و بازیابی فایل های حذف شده، از جمله مواردی می باشند که می تواند توسط هر فردی که به سیستم شما دستیابی پیدا می نماید و دارای دانش مختصری در رابطه با نحوه بازیافت اطلاعات است، مورد سوء استفاده قرار گیرد. افراد فوق با در اختیار گرفتن مجموعه ای از ابزارهای موجود که بدین منظور و گاها" با اهداف خیرخواهانه طراحی شده اند، می توانند حتی اقدام به بازیابی داده هائی نمایند که شما قبلا" آنان را حذف نموده اید.

آنان در این رابطه اقدام به بازیابی مجموعه ای از بیت ها و بایت ها نموده و در ادامه با قرار دادن آنان در کنار یکدیگر، قادر به دستیابی و مشاهده اطلاعات حذف شده خواهند بود.

داده های مخفی و نحوه یافتن آنان

کامپیوترهای موجود در منازل و یا سازمان ها مملو از داده هائی است که کاربران از وجود آنان بر روی سیستم خود بی اطلاع می باشند. حتی تعداد زیادی از کارشناسان حرفه ای فن آوری اطلاعات نیز در این رابطه اطلاعات و یا شناخت مناسبی را ندارند. بر روی کامپیوتر مکان های دنج و خلوتی وجود دارد که داده ها در آنجا مخفی شده و با شناخت مناسب نسبت به محل اختفای آنان، احتمال بازیابی و سوء استفاده از آنان وجود خواهد داشت. با بازرسی مکان های فوق و بررسی ردپای داده های به جا مانده بر روی سیستم، می توان اطلاعات زیادی در خصوص استفاده کننده کامپیوتر و نوع فعالیت های وی را کسب نمود و حتی متوجه شد که وی با چه سرویس دهندگانی ارتباط داشته است. در ادامه به بررسی متداولترین موارد در این خصوص خواهیم پرداخت.

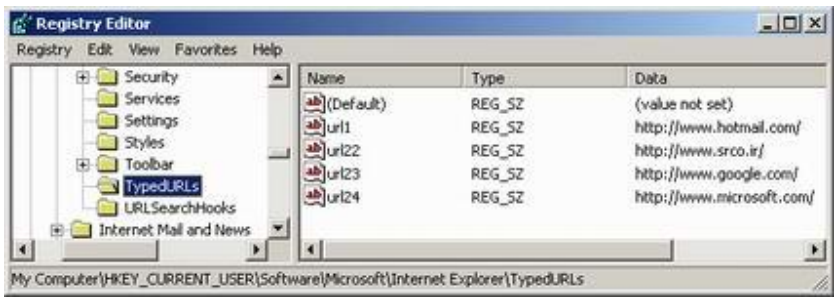
آگاهی از وب سایت های مشاهده شده

جملگی می دانیم که با بررسی history مرورگر و فایل های موقت اینترنت (Cache)، می توان آگاهی لازم در خصوص وب سایت های مشاهده شده توسط کاربر یک کامپیوتر را پیدا نمود. در صورتی که نمی خواهیم ردپای استفاده از وب بر روی سیستم برجای بماند، می بایست این نوع فایل ها را حذف نمود.(فرآیندی ساده در اکثر مرورگرها). کلیک بر روی یک دکمه به منظور حذف یک فولدر به تنهائی کافی نبوده و همچنان احتمال بازیابی آنان وجود خواهد داشت. حتی در مواردی که اقدام به پاک نمودن history مرورگر می شود، تمامی فایل ها حذف نخواهند شد!

سرنخ وب سایت های مشاهده شده در مکان هائی دیگر مخفی شده و همچنان باقی خواهند ماند. با بررسی فولدرهای Favorites و یا Bookmarks نیز می توان اطلاعات زیادی در خصوص سایت هائی که توسط یک کاربر به تناوب استفاده می گردد

را پیدا نمود. بررسی فولدر کوکی (Cookies) نیز می تواند نشان دهنده سایت های مشاهده شده توسط یک کاربر باشد. نظر شما در رابطه با آدرس هائی که در بخش آدرس مرورگر تایپ می گردد و ادامه آن به صورت اتوماتیک توسط برنامه مرورگر درج می گردد، چیست؟ یک فرد آشنا به کامپیوتر می تواند با تایپ تصادفی حروف، متوجه شود که شما قبلاً" چه آدرس هائی را در این بخش مستقیما" تایپ نموده اید. آدرس وب سایت هائی را که شما مستقیما" در بخش آدرس یک مرورگر تایپ می نمائید(منظور کلیک بر روی لینک های pop up نمی باشد) در کلید ریجستری زیر ذخیره می گردند:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



حذف history در مرورگر IE باعث حذف URLs تایپ شده می گردد. در صورت تمایل، می توان این عملیات را مستقیما" و با اجرای برنامه regedit انجام داد. در چنین مواردی می توان یک و یا چندین URLs را مستقیما" حذف نمود(یافتن کلید ریجستری اشاره شده، انتخاب یک و یا چندین URLs، کلیک سمت راست و فعال نمودن دکمه Delete). بررسی فولدرهای Download My و دایرکتوری های temp نیز می تواند مشخص کننده فایل های Downlaod شده توسط شما باشد. با استفاده از نرم افزارهائی که بدین منظور طراحی شده است، می توان به سادگی تمامی "نشانه های وب " را از روی سیستم پاک نمود. Web Cache Illuminator ، یک نمونه در این رابطه است.

در صورتی که شما از طریق یک فایروال از اینترنت استفاده می نمائید، در اغلب موارد فایروال مربوطه و یا سرویس دهنده پروکسی لیستی از وب سایت های مشاهده شده توسط کاربران و یا کامپیوترهای موجود در شبکه را ثبت می نماید.

سایر مکان های داده های مخفی

علاوه بر موارد اشاره شده در خصوص محل اختفای داده ها خصوصا" وب سایت های مشاهده شده، مکان های دیگری نیز وجود دارد که احتمال ذخیره سازی داده ها و بالطبع بازیابی(بازیافت) آنان توسط افراد غیر مجاز وجود خواهد داشت :

- **برنامه های واژه پرداز و سایر برنامه هائی که فایل های موقتی را ایجاد می نمایند**. این فایل ها معمولا" به صورت اتوماتیک و پس از خروج از برنامه و یا حتی راه اندازی کامپیوتر، حذف نمی گردند. فایل های فوق ممکن است در فولدری مشابه با محل نصب برنامه و یا فولدرهای موقتی که بدین منظور توسط برنامه ایجاد می گردد، ذخیره شوند.

- **Clipboard مربوط به ویندوز و یا آفیس**، می تواند داده هائی را که اخیرا" توسط سند مربوطه Cut و Copy شده اند، افشاء نماید. (حتی در صورتی که سند مورد نظر حذف گردد). Clipboard آفیس، می تواند شامل چندین آیتمی باشد که در طی مراحل قبل Cut و Copy شده اند (صرفا" شامل آخرین آیتم نمی باشد).

- **برنامه های IM یا Instant Messenger** ممکن است بگونه ای پیکربندی شده باشند که ماحصل مکالمه و یا محاوره انجام شده را در یک فایل و بر روی هارد دیسک ذخیره نمایند.

- سیستم های IM سرویس گیرنده – سرویس دهنده که از طریق یک سرویس دهنده IM مرکزی امکان ارتباط را فراهم می نمایند، ممکن است ماحصل مکالمه و یا گفتگوی انجام شده را بر روی سرویس دهنده ذخیره نمایند. لیست تماس و یا buddy موجود در این نوع نرم افزارها نیز نشاندهنده افرادی است که شما عموما" با آنان ارتباط برقرار می نمائید (مثلا" چت).
- **نرم افزار پست الکترونیکی و یا برنامه مربوط به نگهداری لیست تماس شما،** ممکن است باعث افشای اطلاعات موجود در آن نظیر آدرس پست الکترونیکی، آدرس فیزیکی و شماره تلفن افرادی گردد که شما با آنان در ارتباط هستید. همچنین تقویم و لیست فعالیت های روزمره نیز می تواند برخی اطلاعات شما را افشاء نماید.
- **فولدرMy Documents نیزمیتواند اسنادی را که اخیرا" با آنان کار نموده اید را مشخص نماید.** playlist مربوط به نرم افزارهای Media Player و بخش history آنان نیز می تواند نشان دهنده فایل های تصویری و صوتی باشد که آنان را مشاهده و یا گوش داده اید.
- **درایوهای مربوط به tape، سی دی، فلاپی و حافظه های فلش** نیز ممکن است همچنان دارای نسخه هائی از اسناد و فایل هائی باشند که شما آنان را از روی کامپیوتر حذف نموده اید.
- **اطلاعاتی که اخیرا" شما اقدام به حذف آنان نموده اید،** ممکن است همچنان و تا زمان Shut down نمودن کامپیوتر در حافظه و یا حافظه مجازی (فایل های swap) موجود باشند.

فایل های حذف شده

با حذف یک فایل آن فایل از روی کامپیوتر شما پاک نمی گردد. مثلا" زمانی که شما یک نامه الکترونیکی را حذف می نمائید، پیام حذف شده صرفا" به یک فولدر دیگر

(Deleted Items)، منتقل می گردد. زمانی که فولدر فوق خالی می گردد (دستی و یا بر اساس برنامه زمانبندی پست الکترونیکی)، تمامی آیتم های موجود به صورت پیش فرض به Recycle Bin منتقل می گردند. حتی در صورت تخلیه Recycle Bin ماجرا خاتمه نیافته و فایل های حذف شده توسط سیستم عامل از روی دیسک حذف نخواهند شد. در حقیقت پس از حذف یک فایل و یا مجموعه ای از فایل ها، صرفا" اشاره گرهائی که به فایل های فوق اشاره می کنند از جدول سیستم فایل حذف شده و فضای استفاده شده توسط فایل های حذف شده بر روی دیسک، علامت " قابل استفاده مجدد " درج می شود. صفرها و یک هائی که داده های موجود در یک فایل را تشکیل می دهند، همچنان در مکان های مورد نظر خود موجود بوده و احتمال بازیابی تمام و یا بخش هائی از آنان وجود خواهد داشت. حتی با فرمت کردن هارد دیسک، فایل های حذف شده موجود بر روی آن، دور انداخته نخواهند شد. حتما" این سوال برای شما مطرح شده است که وجود این نوع اطلاعات حذف شده بر روی کامپیوتر چه تهدیدات امنیتی را ایجاد خواهد کرد و یا چگونه و با استفاده از چه روش و یا روش هائی امکان بازیافت مجدد آنان وجود خواهد داشت؟

مهاجمان و یا بهتر بگوئیم افراد غیر مجاز با استفاده از نرم افزارهای خاصی قادر به برگرداندن داده هائی می باشند که عملا" و از دید کاربر حذف شده ولی همچنان بر روی محیط ذخیره سازی نظیر هارددیسک موجود می باشند. معمولا" فرآیند بازیافت و ریکاوری اطلاعات عملیاتی پیچیده و در عین حال طولانی است. بدیهی است نرم افزارهائی که قادر به انجام اینچنین عملیاتی می باشند، بسیار گرانقیمت باشند:

- File Scavenger
- GetDataBack
- Back2Life

به منظور بازیابی اطلاعات حذف شده می توان از برخی نرم افزارهای ارزان قیمت و یا رایگان موجود نیز استفاده نمود. برخی از نرم افزارهای فوق را می توان با مراجعه به آدرس:http://free-backup-software.net/data-recovery.htm دریافت نمود.

اکثر نرم افزارهای فوق با این هدف طراحی شده اند که اگر شما به صورت تصادفی فایل و یا فایل هائی را حذف کرده باشید، امکان بازیابی مجدد آنان را در اختیار شما قرار دهند. متاسفانه مهاجمان و سایر افراد غیرمجاز نیز می توانند با استفاده از نرم افزارهای فوق به برخی از اطلاعات موجود بر روی سیستم شما دستیابی پیدا نمایند.

مهاجمان و افراد غیر مجاز دارای آگاهی لازم در خصوص مکان هائی که ممکن است داده ها در آنجا مخفی شده اند نیز می باشند. برخی از کاربران به منظور مخفی نمودن فایل های مورد نظر خود، آنان را در یک مکان غیرمتداول و در یک دایرکتوری خاص نظیر دایرکتوری های سیستم ذخیره می نمایند. یک جستجوی ساده برای نوع های خاصی از فایل (نظیرjpeg و یا gif) و یا فایل هائی با ظرفیت بالا که تعمدا" مخفی شده اند، باعث افشای آنان می گردد. مهاجمان و افراد غیرمجازی که اقدام به کنکاش در یک سیستم می نمایند، سعی می نمایند که پس از اتمام عملیات خود وضعیت هارددیسک را به حالت اولیه برگردانند. با توجه به این که هر گونه تلاش در جهت بازیافت اطلاعات ممکن است تغییر داده و ساختار اطلاعاتی موجود بر روی یک هارد دیسک را بدنبال داشته باشد،

مهاجمان در ابتدا اقدام به ایجاد نسخه های ثانویه از اطلاعات موجود بر روی یک هارددیسک نموده و در ادامه عملیات مورد نظر خود را بر روی آنان انجام می دهند (نسخه های ثانویه در سطح بیت ایجاد می گردد). در برخی موارد مهاجمان و افراد غیر

مجاز اقدام به نصب Spyware (برنامه های جاسوسی) و یا سخت افزار خاصی بر روی سیستم نموده تا به سادگی اقدام به جمع آوری و ارسال اطلاعات به یک آدرس مشخص شده را بنمایند. در اینجا لازم است به نقش خطرناک نرم افزارهای موسوم به لاگرها(loggers) نیز اشاره گردد که به صورت سخت افزاری و یا نرم افزاری ارائه می شوند. لاگرها، قادر به انجام عملیات متفاوت و در ابعاد گسترده ای می باشند. ثبت تمامی اطلاعات تایپ شده توسط صفحه کلید، مانیتور نمودن صفحه نمایشگر و گرفتن تصاویر لازم از اطلاعات موجود بر روی نمایشگر، تکثیر پیام های پست الکترونیکی و ذخیره آنان در یک فولدر خاص و یا حتی ارسال آنان به افراد و یا مراکزی خاص بر روی اینترنت بدون آگاهی کاربران، نمونه هائی از عملکرد مخرب لاگرها می باشد.

نحوه حفاظت و ایمن سازی سیستم

در این رابطه می توان اقدامات زیر را انجام داد:

- حصول اطمینان از خالی بودن فولدر Deleted Items برنامه پست الکترونیکی، حذف history مرورگر و Cache مربوط به نگهداری موقت فایل های اینترنت و تمامی فایل های temp در زمان Sign on
- حساسیت لازم در خصوص فایل های موجود در فولدر Downloads ، لاگ مربوط به برنامه ها(نظیر برنامه IM)، و history lists برنامه های متفاوت
- پیکربندی سیستم به منظور عدم نگهداری لیستی از اسنادی که اخیرا" با آنان کار شده است
- رمزنگاری اسناد و فایل های حاوی اطلاعات حساس
- استفاده از رمزهای عبور مناسب در رابطه با account مربوط به Email و سایر نرم افزارهای حفاظت شده
- خاموش نمودن کامپیوتر به منظور پاک نمودن حافظه اصلی

- حذف فایل های page و یا swap مربوط به حافظه مجازی قبل از خاموش نمودن سیستم (فایل های فوق پس از راه اندازی مجدد کامپیوتر ایجاد خواهند شد). در صورتی که قصد فروش و یا ارتقای سیستم خود را دارید و نگران اطلاعات موجود بر روی هارد دیسک آن می باشید، فرمت کردن آن به تنهائی کفایت نخواهد کرد. در چنین مواردی لازم است از یک برنامه overwriting به منظور بازنویسی اطلاعات بر روی دیسک و آنهم چندین مرتبه، استفاده گردد. برنامه های زیر نمونه هائی در این زمینه می باشند.

- Cyber scrub
- Wipe Drive
- Data Gone

داده ها و یا اطلاعات دارای نقشی اساسی در عصر حاضر می باشند. اهمیت این موضوع به حدی است که عصر حاضر را عصر اطلاعات نامیده اند. کامپیوتر نیز در این هنگامه توانسته است با توجه به توان بالای پردازش، سرعت مطلوب در امر ذخیره و بازیابی اطلاعات نقشی محوری و تعیین کننده را برعهده بگیرد. صیانت از اطلاعات حساس موجود بر روی هر کامپیوتر وظیفه ای مهم برای هر کاربر کامپیوتر است. برخی از داده های حساس در مکان های خاصی بر روی کامپیوتر ذخیره و بنوعی مخفی نگاه داشته می شوند. مهاجمان و یا افراد غیر مجاز که تمایل و علاقه به وارسی و کنکاش در سیستم های کامپیوتری را دارند، می توانند با مراجعه به محل اختفای داده ها و بازیابی آنان، اطلاعات زیادی را در خصوص استفاده کننده کامپیوتر کسب نمایند. با کمی صبر و حوصله و دانش اندکی نسبت به کامپیوتر می توان تمهیدات امنیتی لازم در این خصوص را اندیشید و پیشگیری لازم را انجام داد. دستیابی و استفاده از داده های حساس توسط افراد غیرمجاز مهمترین تهدید امنیتی در حال حاضر است که می بایست همواره نسبت به آن حساسیت خاصی را داشت.

Spam

Spam یکی از متداولترین و در عین حال منفی ترین جنبه های دارا بودن یک آدرس Email است. با این که در حال حاضر و با توجه به تکنولوژی های موجود امکان حذف کامل این نوع از نامه های الکترونیکی ناخواسته وجود ندارد، ولی می توان با استفاده از برخی روش های موجود تعداد آنان را کاهش داد.

Spam چیست ؟

Spam ، نسخه الکترونیکی از " نامه های بدرد نخور " است. واژه Spam به پیام های الکترونیکی ناخواسته، اطلاق می گردد. این نوع از نامه های الکترونیکی ارتباط مستقیمی با ویروس نداشته و حتی ممکن است پیام هائی که از منابع معتبر ارسال شده اند نیز در زمره این گروه قرار گیرند.

چگونه می توان میزان Spam را کاهش داد ؟

با رعایت برخی نکات، می توان میزان Spam دریافتی را بطرز محسوسی کاهش داد:

- **آدرس Email خود را بدون دلیل در اختیار دیگران قرار ندهید** . آدرس های پست الکترونیکی به اندازه ای متداول شده اند که شما می توانید بر روی هر فرمی که به منظور کسب اطلاعات شما در نظر گرفته می شود، وجود فیلد خاصی به منظور دریافت آدرس Email را مشاهد نمائید. تعدادی زیادی از مردم بدون درنظر گرفتن مسائل جانبی، آدرس Email خود را در هر محلی و یا هر فرمی درج می نمایند. مثلا" شرکت ها، اغلب آدرس ها را در یک بانک اطلاعاتی ثبت تا بتوانند وضعیت مشتریان خود را در آینده دنبال نمایند. برخی اوقات، اطلاعات فوق به سایر شرکت ها فروخته شده و یا امکان استفاده مشترک برای آنان، فراهم می گردد. بدیهی است در چنین مواردی ممکن است برای شما یک Email و از طرف شرکتی ارسال شود که نه توقع آن را داشته اید و نه از آنان درخواستی مبنی بر ارائه اطلاعات خاصی را داشته اید.

- **بررسی سیاست های محرمانگی**. قبل از ارسال آدرس Email خود به صورت online، بدنبال Privacy سایت مورد نظر بگردید. تعداد بسیار زیادی از سایت های شناخته شده و خوشنام دارای یک لینک خاص بر روی سایت خود به منظور آشنائی کاربران با سیاست های آن سایت در خصوص نحوه برخورد با اطلاعات ارسالی شما می باشند. (همواره این پرسش را برای خود مطرح نمائید که آیا ما آدرسEmail خود را در سایت هائی درج می نمائیم که نسبت به آنان شناخت کافی داریم ؟). شما می بایست قبل از ارسال آدرس Email خود و یا سایر اطلاعات شخصی، سیاست های اعلام شده توسط سایت مورد نظر را مطالعه نموده و از این موضوع آگاه شوید که مالکین و یا مسئولین سایت قصد انجام چه کاری را با اطلاعات ارسالی شما دارند.
- **دقت لازم در خصوص گزینه هائی که به صورت پیش فرض فعال شده اند.** زمانی که شما برای دریافت خدمات و یا Account جدید عملیات sign in را انجام می دهید، ممکن است بخشی وجود داشته باشد که به شما مجموعه ای از گزینه ها را در خصوص دریافت email در خصوص محصولات و یا سرویس های جدید، ارائه نماید. در برخی مواقع، گزینه ها به صورت پیش فرض انتخاب شده اند، بنابراین در صورتی که شما آنان را به همان وضعیت باقی بگذارید، در آینده نه چندان دور برای شما حجم زیادی از نامه های الکترونیکی که شاید انتظار آنان را نداشته باشد، ارسال گردد.
- **استفاده از فیلترها**: تعدادی زیادی از برنامه های پست الکترونیکی امکان فیلترینگ را ارائه می نمایند. پتانسیل فوق به شما این اجازه را خواهد داد که آدرس های خاصی را بلاک نموده و یا امکان دریافت نامه را صرفا" از طریق لیست تماس موجود بر روی کامپیوتر خود، داشته باشید. برخی مراکز ارائه دهنده خدمات اینترنت(ISP) نیز سرویس فیلترینگ و علامت گذاری مربوط به مقابله با Spam

- را ارائه می نمایند. در چنین مواردی ممکن است پیام های معتبری که بدرستی طبقه بندی نشده باشند به عنوان spam درنظر گرفته شده و هرگز به صندوق پستی شما ارسال نگردند.
- **هرگز برروی لینک های موجود در یک Spam ، کلیک ننمائید** . برخی از منابع ارسال کننده Spam با ارسال آدرس هـــــای Email متغیـــر در یک Domain خاص، سعی در تشخیص معتبر بودن یک آدرس Email می نمایند. (مثلا" تشخیص آدرس های Email معتبر موجود بر روی hotmail و یا yahoo). در صورتی که شما بر روی یک لینک ارسالی توسط یک Spam کلیک نمائید، صرفا" معتبر بودن آدرس Email خود را به اطلاع آنان رسانده اید. پیام های ناخواسته ای که یک گزینه "عدم عضویت " وسوسه انگیز را در اختیار شما قرارمی دهند، اغلب به عنوان روشی به منظور جمع آوری آدرس های Email معتبر مورد استفاده قرار گرفته که در آینده از آنان به منظور ارسال Spam استفاده گردد.
- **غیرفعال نمودن گزینه دریافت اتوماتیک گرافیک در نامه های الکترونیکی با فرمت HTML** . تعداد زیادی از شرکت ها، نامه های الکترونیکی را با فرمت HTML و همراه با یک فایل گرافیکی لینک شده ارسال نموده که در ادامه از آن به منظور ردیابی فردی که پیام الکترونیکی را باز نموده است، استفاده می نمایند. زمانی که برنامه سرویس گیرنده پست الکترونیکی شما، اقدام به download گرافیک از سرویس دهنده آنان می نماید، آنان می دانند که شما پیام الکترونیکی را باز نموده اید. با غیر فعال نمودن HTML mail و مشاهده پیام ها با فرمت صرفا" متن، می توان پیشگیری لازم در خصوص این مسئله را انجام داد.
- **ایجاد و یا باز نمودن Account های جدید اضافی**: تعداد زیادی از سایت ها، اقدام به عرضه آدرس پست الکترونیکی به صورت رایگان می نمایند.

- در صورتی که شما بطور مداوم اقدام به ارسال آدرس Email خود می نمائید (برای خرید online ، دریافت سرویس و ...)، ممکن است مجبور به ایجاد یک account دیگر به منظور حفاظت آدرس account اولیه خود در مقابل spam شوید. شما همچنین می بایست از یک account دیگر در زمانی که اطلاعاتی را بر روی بولتن های خبری online، اطاق های چت، لیست های عمومی Mailing و یا USENET ارسال می نمائید، استفاده نمائید. بدین ترتیب می توان یک سطح حفاظتی مناسب در خصوص دریافت spam به آدرس Email اولیه خود را ایجاد کرد.
- **برای سایرین Spam ارسال ننمائید.** یک کاربر متعهد و دلسوز باشید. در خصوص پیام هائی که قصد فوروارد نمودن آنان را دارید، سختگیرانه عمل کنید. هرگز هرگونه پیامی را برای هر شخص موجود در لیست دفترچه آدرس خود فوروارد نکرده و اگر فردی از شما بخواهد که پیامی را برای وی فوروارد ننمائید، به درخواست وی احترام بگذارید.

Spyware

اینترنت با سرعتی باورنکردنی همچنان به رشد خود ادامه می دهد و این پدیده نسبتا" جدید بشریت مورد توجه تمامی افراد و سازمان ها با اهداف مثبت و منفی قرار گرفته است. استفاده از اینترنت برای آگهی های تجاری و بازرگانی از جمله موارد فوق است. در صورتی که فرآیند پخش آگهی های تجاری با آگاهی و رضایت استفاده کننده اینترنت باشد، نمی توان چندان بر آن خرده گرفت ولی در صورتی که فرآیند فوق بدون آگاهی و یا کسب مجوز کاربران انجام شده و با نصب یک برنامه ناخواسته از سیستم های آنان برای ارسال آگهی های تجاری استفاده شود، حریم خصوصی کاربران در معرض تهدید قرار گرفته و این موضوع می تواند پیامدهای بمراتب خطرناکتری را بدنبال داشته باشد و آن زمانی است که اینگونه نرم افزارها از محدوده وظایف خود تعدی نموده و اقدام به جمع آوری و ارسال اطلاعات شخصی کاربران، بدون آگاهی و رضایت آنان می نمایند. ما امروزه شاهد تولد نسل جدیدی از نرم افزارهای جاسوسی می باشیم که از آنان با نام Spyware یاد می گردد. نصب اینگونه نرم افزارهای ناخواسته، مسائل متعددی را برای کاربران بدنبال خواهد داشت.

SpyWare چیست ؟

Spyware ، نرم افزاری است که اقدام به جمع آوری اطلاعات شخصی بدون آگاهی و یا اجازه کاربران می نماید. اطلاعات جمع آوری شده می تواند شامل لیست سایت های مشاهده شده توسط کاربر و یا اطلاعات بمراتب حساس تری نظیر نام و رمز عبور باشد. به این نوع برنامه ها adware نیز گفته می شود. نرم افزارهای فوق پس از نصب بر روی کامپیوتر، قادر به ارسال آگهی های تجاری pop-up ، هدایت مرورگر به

وب سایت هائی خاص، ارسال لیست سایت های مشاهده شده توسط کاربر و یا مانیتورینگ عملکرد کاربران در زمان اتصال به اینترنت می باشند. برخی از برنامه های Spyware ، قادر به ردیابی و تشخیص اطلاعات تایپ شده از طریق صفحه کلید نیز می باشند. با توجه به انجام پردازش های اضافی توسط اینگونه نرم افزارها، سیستم های کاربران کند و کارآئی آنان بطرز محسوسی کاهش خواهد یافت. در صورت دریافت موزیک از طریق برنامه های اشتراک فایل، بازی های رایگان از سایت های ناامن و یا سایر نرم افزارها از منابع ناشناخته، شرایط لازم به منظور نصب اینگونه نرم افزارها و در نهایت آلودگی سیستم فراهم می گردد.

نحوه تشخیص Spyware

علائم زیر می تواند نشاندهنده نصب Spyware بر روی یک کامپیوتر باشد:

- نمایش مستمر پنجره های pop-up آگهی
- هدایت ناخواسته کاربران به وب سایت هائی که هرگز نام آنان در مرورگر تایپ نشده است.
- نصب Toolbars جدید و ناخواسته در مرورگر وب
- تغییر ناگهانی و غیرمنتظره صفحه اصلی مرورگر(home page)
- تغییر موتور جستجوی مرتبط با مرورگر پس از کلیک بر روی دکمه Search همراه مرورگر
- عدم عملکرد صحیح برخی کلیدها در مرورگر (نظیر کلید Tab زمانی که بر روی فیلدهای یک فرم حرکت می شود)
- نمایش تصادفی پیام های خطاء
- کاهش ملموس سرعت کامپیوتر در زمان فعال نمودن برنامه ها و یا انجام عملیاتی خاص (ذخیره فایل ها و ...)

- فعال شدن مرورگر و بدنبال آن وب سایت های آگهی بدون انجام عملیاتی خاص توسط کاربر
- عدم کارکرد صحیح لینک های همراه یک برنامه
- توقف ناگهانی و غیرمنتظره مرورگر وب
- عدم عملکرد صحیح برخی از عناصر سیستم عامل و یا سایر برنامه ها

نحوه پیشگیری از نصب Spyware

- **عدم کلیک بر روی لینک های موجود در پنجره های pop-up** . با توجه به این که پنجره های pop-up اغلب محصول و یا نوع خاصی از Spyware می باشند، کلیک بر روی آنان می تواند باعث نصب یک نرم افزار Spyware گردد. برای بستن این نوع پنجره ها از آیکون "X" در titlebar استفاده گردد(در مقابل لینک close همراه پنجره).
- **پاسخ منفی به سوالات ناخواسته**: در صورت برخورد با جعبه های محاوره ای که درخواست اجرای یک برنامه را نموده و یا قصد انجام عملیات خاص دیگری را دارند، همواره گزینه NO و یا Cancel انتخاب گردد. در موارد خاص می توان از آیکون "X" موجود در titlebar استفاده نمود.
- **دقت لازم در خصوص دریافت نرم افزارهای رایگان از اینترنت**: سایت های زیادی اقدام به ارائه Toolbar های سفارشی و یا ویژگی های خاص دیگری می نمایند. تا زمانی که نسبت به ایمن بودن این نوع سایت ها اطمینان حاصل نشده است، نمی بایست فایل و یا برنامه ای را از طریق آنان Download نمود.
- **عدم کلیک بر روی لینک های موجود در Email که ادعای ارائه یک نرم افزار Anti-Spyware را دارند**. نظیر ویروس های کامپیوتری،

لینک های موجود در نامه های الکترونیکی ممکن است اهداف سودمندی را دنبال ننموده و نصب Spyware بر روی سیستم شما را بدنبال داشته باشند.

علاوه بر موارد فوق و خصوصا" در مواردی که احساس می شود بر روی کامپیوتر Spyware نصب شده است و قصد داشته باشیم عملکرد آن را به حداقل مقدار خود برسانیم می توان عملیات زیر را انجام داد:

- **اعمال محدودیت در رابطه با پنجره های Pop-up و کوکی ازطریق تنظیمات برنامه مرورگر**: پنجره های pop-up توسط نوع خاصی از اسکریپت ها و یا محتویات فعال(اپلت های جاوا، کنترل های اکتیوایکس) ایجاد می گردند. با تنظیم مناسب پارامترهای برنامه مرورگر، می توان محدودیت لازم در اجرای اسکریپت ها، اپلت های جاوا، کنترل های اکتیو ایکس و تعداد پنجره های pop-up را اعمال نمود. عملکرد برخی از کوکی ها مشابه Spyware می باشند، چراکه از طریق آنان مشخص خواهد شد که شما چه وب سایت هائی را مشاهده نموده اید. با تنظیم پارامترهای برنامه مرورگر می توان محدودیت لازم در خصوص ایجاد کوکی ها را اعمال نمود.

نحوه حذف Spyware

- **اجرای یک برنامه ضد ویروس و پویش کامل کامپیوتر**: برخی از نرم افزارهای آنتی ویروس قادر به یافتن و حذف برنامه های Spyware می باشند.
- **اجرای یک برنامه معتبر که مختص حذف Spyware طراحی شده است.** تعداد زیادی از تولیدکنندگان محصولاتی را به منظور شناسائی وحذف برنامه های Spyware ، ارائه داده اند.

Adaware, Webroot's SpySweeper, PestPatrol, LavaSoft's Spybot Search and Destroy ، نمونه هائی در این زمینه می باشند.

نرم‌افزار جاسوسی چیست؟

حتما تاحالا برایتان پیش آمده است که در حال کار با اینترنت ناگهان پنجره‌های مختلف زیادی بدون میل شما باز می‌شوند که اصطلاحا popup windows نام دارند و وقت زیادی را باید برای بستن آنها صرف کنید. اگر در آن موقع کم‌حوصله باشید سریعا از کوره در میروید! این مطلب به شما کمک می‌کند که متوجه شوید این پنجره‌های مزاحم از کجا می‌آیند.

نرم‌افزار جاسوسی هر نوع فناوری یا برنامه روی کامپیوتر شماست که اطلاعات را بطور پنهانی جمع‌آوری می‌کند. این دیتا سپس به تبلیغ‌کنندگان یا به سایر گروه‌های علاقه‌مند

فروخته می‌شود. نوع اطلاعاتی که از کامپیوتر شما جمع‌آوری می‌شود متفاوت است. بعضی نرم‌افزارهای جاسوسی فقط اطلاعات سیستمی شما را ردیابی می‌کنند – مانند نوع اتصال شما به اینترنت و سیستم‌عامل کامپیوترتان. بقیه نرم‌افزارهای جاسوسی اطلاعات فردی را جمع‌آوری می‌کنند ـ مانند ردگیری عادات و علائق شما در هنگام کار با اینترنت و یا گاهی بدتر، با فایلهای شخصی شما سروکار دارند. نرم‌افزار جاسوسی بدون رضایت و اجازه کاربر نصب می‌گردد. (چنانچه به یک شرکت اجازه جمع‌آوری دیتا را بدهید، دیگر نام این عمل جاسوسی نیست، بنابراین همیشه قبل از اجازه دادن، موارد افشای دیتا بصورت آنلاین را با دقت بخوانید). بعضی افراد به جاسوسی عمومی که گرایشات اینترنتی و نرم‌افزاری را ردگیری می‌کند تا جاییکه اطلاعات مشخصه فردی را شامل نشود، اعتراضی ندارند. اما بقیه به هر نوع دیتایی که بدون اجازه از کامپیوترشان برداشته می‌شود، معترض هستند. بهرحال، نرم‌افزار یا ابزاری که این اطلاعات را جمع‌آوری می‌کند، نرم‌افزار جاسوسی نامیده می‌شود.

نصب نرم‌افزار جاسوسی روی کامپیوتر شما می‌تواند با مشاهده یک وب‌سایت، دیدن یک ایمیل به فرمت HTML یا با کلیک‌کردن یک پنجره بازشونده (pop-up) آغاز شود. روند دانلود به شما اطلاع داده نمی‌شود، بنابراین شما از اینکه کامپیوترتان پذیرای یک نرم‌افزار جاسوسی شده است، بی‌اطلاع خواهید ماند.

تولد نرم‌افزارهای جاسوسی

قبل از ظهور نرم‌افزارهای جاسوسی تبلیغ اینترنتی از طریق قرار دادن bannerهایی بود که در صفحات وب قابل مشاهده بود (البته هنوز هم وجود دارند)، و کاربران با کلیک

کردن روی آنها از اطلاعات یا خدمات ارائه‌شده به دلخواه آگاهی می‌یافتند. اما بتدریج کاربران از این نحو تبلیغ خسته شده‌بودند و به این ترتیب تبلیغ‌کنندگان در حال ورشکستگی بودند، زیرا میزان درآمد آنها متناسب با میزان کلیک از طرف بازدیدکنندگان بر روی تبلیغاتی بود که بر روی وب‌سایت خود قرار می‌دادند.

تبلیغ‌کنندگان دریافتند که اگر همچنان می‌خواهند از طریق اینترنت درآمد داشته باشند، مجبور به تغییر تاکتیکهایشان هستند. بسیاری از آنها دریافت خود را بر اساس میزان واقعی فروش قرار دادند. بقیه به راههای جدید تبلیغ فکر کردند. آنها به روشی تازه رسیدند که به آنها اجازه تبلیغ محصولات را بدون داشتن وب‌سایت یا سرویس‌دهنده می‌داد و به این ترتیب نرم‌افزارهای جاسوسی پدید آمدند.

در ابتدا نرم‌افزار جاسوسی در دل برنامه‌های رایگان قرار می‌گرفت، اما بعده‌ها به حقه‌های کثیف‌تری! رو آوردند و آن استفاده از سوءاستفاده‌های هکری برای نصب نرم‌افزار جاسوسی روی کامپیوترهاست. اگر از سیستم‌های عامل رایج استفاده می‌کنید شانس شما برای داشتن نرم‌افزار جاسوسی روی سیستم‌تان بیشتر است. براحتی می‌توان ادعا کرد که بسیاری از کاربران خانگی بر روی کامپیوتر خود جاسوس! دارند.

انواع نرم افزارهای جاسوسی

همانطور که گفته شد، نرم افزار جاسوسی هر نوع نرم افزاری است که اطلاعات را از یک کامپیوتر بدون آگاهی کاربر بدست میاورد. انواع زیادی از این نوع نرم افزارها در اینترنت فعال هستند اما میتوان آنها را به دو گروه عمده تقسیم کرد:

نرم‌افزار جاسوسی خانگی (Domestic Spyware)

نرم‌افزاری است که معمولا توسط صاحبان کامپیوترها بمنظور آگاهی یافتن از تاثیرات اینترنت برروی شبکه های کامپیوتری خودشان، خریداری و نصب می گردد. مدیران از این نرم افزار برای آگاهی از فعالیتهای آنلاین کارمندان استفاده می کنند. بعضی افراد نیز برای اطلاع از فعالیتهای سایر اعضاء خانواده استفاده می کنند (مانند مشاهده محتویات اتاقهای گفتگو توسط والدینی که کودکانشان در آنها شرکت می کنند)

یک شخص ثالث نیز می تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب کامپیوتر نصب کند. مجریان قانون از نرم افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی

استفاده میکنند که این مجرمان خود از همین نرم افزارهای جاسوسی برای حصول اطلاعات از کامپیوترهای شخصی به قصد دزدی دارایی‌ها استفاده کرده‌اند.

نرم افزار جاسوسی تجاری (Commercial Spyware)

این نرم‌افزار که بعنوان adware نیز شناخته می‌شود، نرم‌افزاری است که شرکتها برای تعقیب فعالیتهای وبگردی کاربران اینترنت استفاده می کنند. این شرکتها اغلب اطلاعات حاصل را به بازاریابان می فروشند و آنها کاربران را با تبلیغات خاص مورد هدف قرار می‌دهند – منظور تبلیغاتی است که با علائق کاربر مطابقت دارد و به احتمال زیاد برای وی جذاب است.

بدست آوردن اطلاعات به این سادگی موجب خوشحالی تبلیغ‌کنندگان می‌شود. سابقا، بازاریابان برای فهمیدن علائق افراد باید آنها را از طریق برگزاری مسابقات یا موارد مشابه تطمیع می کردند. آن روشهای کسب اطلاعات شخصی هنوز وجود دارد، اما در آن روشها قدرت خواندن و اطلاع از سرنوشت اطلاعات شخصی و پذیرفتن یا نپذیرفتن آنها توسط افراد وجود دارد. بهرحال، اطلاع از سلیقه‌های شما بصورت پنهانی با استفاده از نرم افزارهای جاسوسی بسیار آسانتر است و تصویر بسیار کاملتری به صنعت بازایابی ارائه می کند. در کل می توان ادعا کرد که نرم افزارهای جاسوسی همه جا هستند.

نرم‌افزارهای جاسوسی و مقابله با آنها (۲)

انواع و اهداف نرم‌افزارهای جاسوسی مختلف

نرم‌افزارجاسوسی هرچه نباشد، حداقل یک عامل آزاردهنده است که سرعت کامپیوتر را کم می‌کند، هارددیسک سیستم را بی‌جهت پر می‌کند و کامپیوتر شما را به هدفی برای تبلیغ‌کنندگان تبدیل می‌کند. فراتر از آگاهی از اطلاعات خصوصی شما، نرم‌افزار جاسوسی می‌تواند بعنوان ابزاری برای جرائمی مانند تقلب در شناسایی مورد استفاده قرار گیرد. در ادامه لیستی از انواع مختلف نرم‌افزارهای جاسوسی و هدفشان ارائه می‌شود.

ثبت‌کنندگان نشانی‌های وب و صفحات نمایش

ثبت‌کنندگان نشانی‌های وب، وب‌سایتها و صفحات دیده‌شده را ردیابی می‌کنند. ثبت‌کنندگان صفحه‌نمایش می‌توانند یک تصویر سیاه‌وسفید کوچک (برای کم‌کردن حجم تصویر) از صفحه پیش‌روی شما در هر زمان بگیرند و این تصاویر را بدون اطلاع شما ذخیره یا ارسال کنند. این روشها برای جاسوسی‌های خانگی متداول هستند.

ثبت‌کنندگان چت و ایمیل

این ثبت‌کنندگان یک کپی متنی از تمام ایمیلهای واردشونده و خارج‌شونده و چتها تهیه می‌کنند. یک جاسوس خانگی به کرات از این روش استفاده می‌کند.

ثبت‌کنندگان کلید و کلمات عبور

هنگامی که شما مشغول کار با کامپیوتر هستید، یک نفر بالای سر شما ایستاده است و اعمال شما را نظارت می‌کند! ثبت‌کننده کلمه عبور این کار را می‌کند یعنی کلمات عبور تایپ‌شده را ردگیری می‌کند. اما ثبت‌کننده کلید تمام آنچه را که تایپ می‌شود، ثبت می‌کند.

حشرات وبی!

حشرات وبی بعنوان جاسوسان تبلیغ‌کننده یا نرم‌افزارهای تبلیغ شناخته می‌شوند. هنگامی که شما چنین نرم‌افزاری روی کامپیوتر خود دارید، بعد از انجام بعضی کارها، مانند تایپ کردن عباراتی در یک موتور جستجو، پنجره‌های بازشونده تبلیغاتی خاصی را مرتبط با عناوین مورد جستجو دریافت می‌کنید. این تبلیغات حتی گاهی می‌توانند زمانی که به اینترنت متصل نیستید، بر روی صفحه شما ظاهر شوند. اگر بطور پیوسته زیربار

صفحات تبلیغاتی قراردارید، احتمالا یک حشره وبی بر روی کامپیوتر شما نصب شده است.

مرورگر ربایان!

بعضی‌ها کامپیوتر شما را برای استفاده خودشان بخدمت می‌گیرند ـ کاربران نرم‌افزارهای جاسوسی می‌توانند اتصال شما را برای ارسال اسپم‌هایشان از طریق سرویس‌دهنده‌اینترنت شما، بربایند!!! به این معنی که یک اسپم‌ساز انگل می‌تواند هزاران ایمیل اسپمی را از طریق اتصال کامپیوترتان به اینترنت و آدرس ISP شما، ارسال کند. دسترسیهای با سرعت و حجم بالا به اینترنت معمولا هدف این نوع کاربران قرار می‌گیرند. اغلب قربانیان متوجه نمی‌شوند که از اعتبار آنها سوءاستفاده شده است، تا اینکه به خاطر شکایت علیه اسپم‌ها، سرویس‌دهنده‌اینترنت اتصالشان را قطع کند.

مودم ربایان!

اگر برای اتصال به اینترنت از یک مودم و خط تلفن استفاده می‌کنید، یک فرد بی‌مرام! ممکن است قادر باشد یک شماره‌گیر آنلاین برای برقراری یک اتصال جدید اینترنت بر روی کامپیوتر شما نصب کند. این اتصال ممکن است یک اتصال راه دور با هزینه بالا باشد. هنگامی که قبض تلفن بدستان میرسد، به شما شک وارد خواهد شد. این نرم‌افزارهای جاسوسی اغلب داخل اسپم و ایمیلهای مربوط به امور جنسی قرار دارند. بازکردن ایمیل میتواند بصورت سهوی باعث آغاز نصب شماره‌گیر شود. این افراد بدذات! که پی‌گیریشان کار آسانی نیست، روی این حقیقت حساب می‌کنند که شما قبض تلفن را قبل از اینکه فرصت پیگیری داشته باشید، پرداخت می‌کنید.

PC ربایان!

PCربایان میانبرهای(shortcuts) اینترنتی را در فولدر Favorites شما بدون خبردادن به خودتان قرار میدهند. این میانبرها باعث می‌شوند که بسیاری بطور اتفاقی از وب‌سایتشان دیدن کنید و به این ترتیب بصورت تصنعی آمار ترافیک سایت خود را بالا می‌برند. این اتفاق به آنها اجازه دریافت مبالغ بیشتری را بابت تبلیغات در سایتشان می‌دهد که هزینه پرداخت‌شده آن در واقع زمان و پهنای باندی است که از شما گرفته می‌شود. ممکن است بتوانید با تغییر انتخابهای اینترنت خود از دست این Fovorites کاذب رها شوید، اما گاهی تنها راه خلاص شدن از شر این لینکهای مزاحم پاک کردن آنها از داخل رجیستری است. بهرحال، ممکن است این نرم‌افزار جاسوسی طوری طراحی شده باشد که با هر بار راه‌اندازی مجدد کامپیوتر خودش را در داخل رجیستری قرار دهد. تنها راه حل پیش پای شما برای کشتن این نوع جاسوس متجاوز! فرمت کردن هارد کامپیوتر یا استفاده از یک برنامه ضدجاسوس بسیار قدرتمند است.

تروا‌ها و ویروس‌ها

مانند اسب چوبی تروا که یونانیان برای ورود به شهر تروا استفاده کردند، این نرم‌افزار برای سوءاستفاده از کامپیوتر شما، خود را به شکلی بی‌ضرر درمیاورد. دیتای شما ممکن است کپی، توزیع یا تخریب شود. ویروس نیز مشابه تروا است با این تفاوت که قدرت ایجاد شبیه خود را دارد تا باعث خسارت به کامپیوترهای بیشتری شود. بهرحال، هردوی این قطعات آسیب‌رسان می‌توانند تحت تعریف نرم‌افزار جاسوسی قرار بگیرند، زیرا کاربر از وجودشان بی‌اطلاع است و هدف واقعی آنان را نمی‌داند.

نرم‌افزارهای جاسوسی و مقابله با آنها (۳)

چگونگی قرارگرفتن نرم‌افزار جاسوسی روی کامپیوتر و روش مقابله به آن

تنها مساله در مورد نرم‌افزار جاسوسی این نیست که چه مدت روی کامپیوتر شما قرار داشته و چه قصدی دارد، بلکه فهمیدن اینکه چگونه و از کجا این برنامه وارد کامپیوتر شما شده است، در درجه اول قرار دارد.

در شماره‌های (۱) و (۲) با نرم‌افزارهای جاسوسی و انواع و عملکرد آنها آشنا شدیم. درست مانند علفهای هرز که بدون سروصدا هنگام قدم زدن در جنگل به جوراب شما می‌چسبند، هنگامی که مشغول گشت و گذار در اینترنت هستید، نرم‌افزار جاسوسی خودش را مانند یک مسافر قاچاقی به کامپیوتر شما می‌چسباند! اما قبل از اینکه هرچیزی بتواند روی کامپیوتر شما نصب گردد، معمولا باید روی چیزی کلیک یا برنامه‌ای را باز کنید. در زیر چند تا از معمولترین روشهای مورد استفاده برای فریب‌دادن کاربران برای نصب نرم‌افزارهای جاسوسی بیان شده است:

- بازکردن ایمیل اسپمی
- کلیک کردن روی پنجره‌های بازشونده فریبنده
- دانلود کردن رایگان برنامه‌ها، بازیها، ابزارها و غیره
- برنامه‌های اشتراک فایل

- مشاهده وب‌سایتهای ناجور!
- نرم‌افزارهای اجرای فایلهای صوتی و تصویری آنلاین

درحالیکه حجم فراوانی از محتوا روی اینترنت قرار دارد که برای تماشای اعمال شما بصورت پنهانی طراحی نشده است، بسیاری از نرم‌افزارهای رایگان یا از رده خارج وجود دارد که بی‌سروصدا همراه با نرم‌افزار جاسوسی وارد کامپیوتر شما می‌شود. نرم‌افزار جاسوسی نه تنها علائق شما را برای تبلیغ‌کنندگان آشکار می‌سازد، بلکه می‌تواند منجر به افشای اطلاعات شخصی نیز شود. ببینیم نرم‌افزار جاسوسی چگونه روی هارددیسک شما قرار میگیرد و شما برای جلوگیری از آن چه می‌توانید بکنید.

اولا، یکی از بزرگترین اشتباهاتی که کاربران انجام میدهند این است که قبل از شروع گشت و گذار در وب تنظیمات سطح امنیتی خود را بسیار پایین انتخاب می‌کنند. سطح امنیتی پایین به تمام کوکی‌ها و برنامه‌های جاسوسی به سادگی اجازه ذخیره شدن در حافظه کامپیوتر را میدهد. کارهایی که شما می‌توانید برای دور نگهداشتن نرم‌افزارهای جاسوسی از سیستم خود انجام دهید شامل موارد زیر است:

- تنظیم سطح امنیتی به سطح پیش‌گزیده یا بالاتر
- نظارت دقیق بر آنچه دانلود می‌کنید
- به روز نگهداشتن سیستم‌عامل کامپیوتر

- نصب یک برنامه ضدجاسوسی که جلوی آنچه را که از دست می‌دهید، بگیرد!

برنامه ضدجاسوسی محل برنامه‌های جاسوسی را که بدون اطلاع شما وارد شده‌اند، تعیین می‌کند، آنها را قرنطینه و سپس پاک می‌کند.

در مرحله بعدی، به احساس و غریزه خود رجوع کنید! اگر منبعی آشنا یا قابل اعتماد بنظر نمی‌رسد، ایمیل را باز نکنید، popup را کلیک نکنید و وب‌سایت را نبینید. برنامه‌های مورد نیاز خود را از منبع قابل اعتماد دریافت کنید. گاهی‌اوقات برنامه‌های مجانی ارزش دردسر بعدی را ندارند! هنگامی که به یک پیشنهاد فریبنده برخورد می‌کنید به انگیزه آن دقت کنید. چرا یک نفر می‌خواهد به شما به‌روزرسانیهای مرتب مجانی ارائه دهد؟! دنبالش نروید.

از تجربیات دیگران برای فهمیدن اینکه کدام نرم‌افزارها درون خود به برنامه‌های جاسوسی پناه داده‌اند، استفاده کنید. در عرض چند ثانیه می‌توانید جستجویی انجام دهید تا بفهمید دیگران در مورد نرم‌افزارهای توام با جاسوس، شامل برنامه‌های به اشتراک‌گذاری

فایلها (مانند Kazza و BearShare) و نرم‌افزارهای اجرای فایلهای صوتی‌تصویری آنلاین چه می‌گویند. در مورد دوم صداهای اعتراض! علیه نرم‌افزارهای جاسوسی تاثیرگذار خواهد بود. برای مثال، یک برنامه محاسبه مالیات معروف اخیرا یک برنامه جاسوسی را بمنظور جلوگیری از هر گونه کپی‌برداری از فایلهایش ـ حتی برای مقاصد قانونی مانند تهیه پشتیبان یا استفاده سایر اعضای همان خانواده ـ داخل محصول خود قرار داد. اما مشتریان از این مساله ناراضی بودند که این نرم‌افزار توانایی نظارت بر رفتارشان را دارد، و بهمین دلیل برعلیه سازنده با صدای بلند! اعتراض کردند. شرکت نرم‌افزاری به حرف آنها گوش کرد و سال بعد نرم‌افزار را بدون برنامه جاسوسی فضول! به فروش رساند.

از آنجا که شما به نرم‌افزارهای جاسوسی "نه" می‌گویید، نصب‌کنندگان برای دریافت اجازه مزاحمتان نمی‌شوند! ـ بسیاری اعتقادی به انجام بازی جوانمردانه ندارند!!! بعضی بازاریابان از حقه‌های عادی برای نصب جاسوس‌شان روی کامپیوتر شما استفاده می‌کنند. برای مثال، بخشی از یک نرم‌افزار به نام Gator وجود دارد که تلاش می‌کند شما را برای نصب محصولش از طریق یک popup تبلیغاتی فریب دهد. هنگامی که شما به پیشنهاد دانلود "نه" بگویید (پنجره را ببندید)، popup دوم ظاهر می‌شود و می‌پرسد که "آیا مطمئن هستید؟" این سوال آری/خیر مبهم باعث می‌شود که افراد با کلیک جواب دهند، که به این ترتیب بدون آگاهی کاربر، دانلود آغاز می‌شود.

روش دیگری که باعث پیاده‌شدن نرم‌افزار جاسوسی روی کامپیوتر شما می‌شود، drive-by download نامیده می‌شود. وقتی شما یک وب‌سایت معلوم‌الحال! را مشاهده می‌کنید، به یک popup برمی‌خورید که از شما اجازه برای دانلود می‌خواهد. لحن! پیام باعث می‌شود که شما باور کنید که برای دیدن صفحه وب بازشده به دانلود نیاز است، حتی اگر نیازی نباشد. اگر "بله" بگویید، برنامه جاسوس در کامپیوتر شما دانلود می‌شود. اما اگر پاسخ منفی بدهید، popupها در صفحات بعدی ظاهر می‌شوند تا بالاخره شما به کلیک کردن روی یکی از آنها فریفته شوید و به این ترتیب برنامه جاسوسی به صورت خاموش کار خود را آغاز می‌کند!

بعضی شرکتها از نرم‌افزارهای جاسوسی تبلیغاتی استفاده می‌کنند. وقتی این adwareها روی سیستم شما نصب شدند، شروع به بازکردن popupهای تبلیغاتی می‌کنند. به این ترتیب شما سیلقه‌های شخصی شما و منابع کامپیوتریتان (پهنای باند، اتصال اینترنت و زمان پردازش کامپیوتر) از اختیار شما خارج خواهد شد، اما در عوض هیچ‌چیز بدست نخواهید آورد بجز بمباران تبلیغاتی و اگر نرم‌افزار جاسوسی آدرس ایمیل شما را بدست آورد انبوهی از اسپم‌ها.

چون همواره روش‌های جدید آلوده کردن کامپیوتر شما توسط نرم‌افزارهای جاسوسی در حال ایجاد است، یک نرم‌افزار ضدجاسوسی نصب کنید. این نرم‌افزار به منظور کشف و بیرون‌کردن جاسوس‌ها قبل از اینکه شما را به‌زحمت بیندازند، طراحی شده است. اگر شما از برنامه ضدجاسوسی خود بعنوان سگ محافظ! استفاده کنید، شما را از دانلودهای بدون اجازه و بی‌خبر، آگاه خواهد کرد. نرم‌افزار جاسوسی مزاحمت ایجاد می‌کند و منجر به دردسرهای جدی می‌شود. اگر شما مراتب احتیاط را رعایت کنید، می‌توانید از دردسر احتمالی پرهیز کنید و کامپیوترتان را تمیز نگه دارید.

حملات مبتنی بر مهندسی اجتماعی

آیا شما از جمله افرادی می باشید که به ظاهر افراد و نحوه برخورد آنان بسیار اهمیت داده و با طرح صرفا" یک سوال از جانب آنان، هر آنچه را که در ارتباط با یک موضوع خاص می دانید در اختیار آنان قرار می دهید؟ رفتار فوق گرچه می تواند در موارد زیادی دستاوردهای مثبتی را برای شما بدنبال داشته باشد، ولی در برخی حالات نیز ممکن است چالش ها و یا مسائل خاصی را برای شما و یا سازمان شما، ایجاد نماید. آیا وجود اینگونه افراد در یک سازمان مدرن اطلاعاتی(خصوصا" سازمانی که با داده های حساس و مهم سروکار دارد) نمی تواند تهدیدی در مقابل امنیت آن سازمان محسوب گردد؟ به منظور ارائه اطلاعات حساس خود و یا سازمان خود از چه سیاست ها و رویه هائی استفاده می نمائید؟ آیا در چنین مواردی تابع مجموعه مقررات و سیاست های خاصی می باشید؟ صرفنظر از پاسخی که شما به هر یک از سوالات فوق خواهید داد، یک اصل مهم در این راستا وجود دارد که می بایست همواره به آن اعتقاد داشت: "هرگز اطلاعات حساس خود و یا سازمان خود را در اختیار دیگران قرار نداده مگر این که مطمئن شوید که آن فرد همان شخصی است که ادعا می نماید و می بایست به آن اطلاعات نیز دستیابی داشته باشد."

یک حمله مهندسی اجتماعی چیست ؟

به منظور تدارک و یا برنامه ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص(روابط عمومی مناسب، ظاهری آراسته و ...)، سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند. یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد.

مثلا" وانمود نماید که یک کارمند جدید است، یک تعمیر کار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید. یک مهاجم، با طرح سؤالات متعدد و برقراری یک ارتباط منطقی بین آنان، می تواند به بخش هائی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا نماید. در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نگردد، وی ممکن است با شخص دیگری از همان سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول، توانمندی خود را افزایش دهد.(یک قربانی دیگر!).

یک حمله Phishing چیست ؟

این نوع از حملات شکل خاصی از حملات مهندسی اجتماعی بوده که با هدف کلاهبرداری و شیادی سازماندهی می شوند. در حملات فوق از آدرس های Email و یا وب سایت های مخرب به منظور جلب نظر کاربران و دریافت اطلاعات شخصی آنان نظیر اطلاعات مالی استفاده می گردد. مهاجمان ممکن است با ارسال یک Email با ظاهری قابل قبول و از یک شرکت معتبر کارت اعتباری و یا موسسات مالی، از شما درخواست اطلاعات مالی را نموده و اغلب عنوان نمایند که یک مشکل خاص ایجاد شده است و ما در صدد رفع آن می باشیم. پس از پاسخ کاربران به اطلاعات درخواستی، مهاجمان از اطلاعات اخذ شده به منظور دستیابی به سایر اطلاعات مالی و بانکی استفاده می نمایند.

نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

- به تلفن ها، نامه های الکترونیکی و ملاقات هائی که عموما" ناخواسته بوده و در آنان از شما درخواست اطلاعاتی خاص در مورد کارکنان و یا سایر اطلاعات شخصی می گردد، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید. در صورتی که یک فرد ناشناس ادعا می نماید که از یک سازمان معتبر است، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب تکلیف کنید.

- هرگز اطلاعات شخصی و یا اطلاعات مربوط به سازمان خود را (مثلا" ساختار و یا شبکه ها) در اختیار دیگران قرار ندهید، مگر این که اطمینان حاصل گردد که فرد متقاضی مجور لازم به منظور دستیابی به اطلاعات درخواستی را دارا می باشد.
- هرگز اطلاعات شخصی و یا مالی خود را در یک email افشاء نکرده و به نامه های الکترونیکی ناخواسته ای که درخواست این نوع اطلاعات را از شما می نمایند، پاسخ ندهید (به لینک های موجود در اینگونه نامه های الکترونیکی ناخواسته نیز توجهی نداشته باشید).
- هرگز اطلاعات حساس و مهم شخصی خود و یا سازمان خود را بر روی اینترنت ارسال ننمائید. قبل از ارسال اینگونه اطلاعات حساس، می بایست Privacy وب سایت مورد نظر به دقت مطالعه شده تا مشخص گردد که اهداف آنان از جمع آوری اطلاعات شخصی شما چیست و نحوه برخورد آنان با اطلاعات به چه صورت است؟
- دقت لازم در خصوص آدرس URL یک وب سایت را داشته باشید. وب سایت های مخرب ممکن است خود را مشابه یک وب سایت معتبر ارائه نموده که آدرس URL آنان دارای تفاوت اندکی با وب سایت های شناخته شده باشد. وجود تفاوت اندک در حروف استفاده شده برای نام سایت و یا تفاوت در domain ، نمونه هائی در این زمینه می باشند (مثلا" com در مقابل net).
- در صورت عدم اطمینان از معتبر بودن یک Email دریافتی، سعی نمائید با برقراری تماس مستقیم با شرکت مربوطه نسبت به هویت آن اطمینان حاصل نمائید. از اطلاعات موجود بر روی یک سایت مخرب به منظور تماس با آنان استفاده نمائید چراکه این اطلاعات می تواند شما را به مسیری دیگر هدایت نماید

که صرفا" اهداف مهاجمان را تامین نماید. به منظور آگاهی از این نوع حملات که تاکنون بوقوع پیوسته است، می توانید به آدرس

http://www.antiphishing.org/phishing_archive.html

مراجعه نمائید.

- با نصب و نگهداری نرم افزارهای آنتی ویروس، فایروال ها و فیلترینگ نامه های الکترونیکی ناخواسته(spam)، سعی نمائید یک سطح حفاظتی مناسب به منظور کاهش این نوع حملات را ایجاد نمائید.

اقدامات لازم در صورت بروز تهاجم

- در صورتی که فکر می کنید به هر دلیلی اطلاعات حساس سازمان خود را در اختیار دیگران (افراد غیر مجاز) قرار داده اید، بلافاصله موضوع را به اطلاع افراد ذیربط شاغل در سازمان خود (مثلا" مدیران شبکه) برسانید. آنان می توانند در خصوص هرگونه فعالیت های غیرمعمول ویا مشکوک، هشدارهای لازم را در اسرع وقت در اختیار دیگران قرار دهند.
- در صورتی که فکر می کنید اطلاعات مالی شما ممکن است در معرض تهدید قرار گرفته شده باشد، بلافاصله با موسسه مالی خود تماس حاصل نموده و تمامی حساب های مالی در معرض تهدید را مسدود نمائید. در این رابطه لازم است دقت، حساسیت و کنترل لازم در خصوص هر گونه برداشت از حساب های بانکی خود را داشته باشید.
- گزارشی در خصوص نوع تهاجم را تهیه نموده و آن را در اختیار سازمان های ذیربط قانونی قرار دهید.

شناسایی مزاحم کامپیوتری

اگر کامپیوتر شما به اینترنت وصل است همواره در معرض انواع تهدیدات هستید. به عنوان رایج‌ترین مورد می‌توان به امکان آلودگی دستگاه به انواع ویروس‌ها و کرم‌هایی که از طریق اینترنت توزیع می‌شوند اشاره نمود. نرم‌افزارهای جاسوس نمونه دیگری از این دست برنامه‌ها هستند که بر روی دستگاه قرار گرفته، فعالیت‌های کاربر و همینطور اطلاعات شخصی مانند گذر واژه‌ها، اطلاعات مربوط به کارت‌های اعتباری و... را ثبت کرده و به منتشر کنندگان خود گزارش می‌دهند. نفوذ در سیستم‌های کاربران و انجام اعمال نامطلوب آنان از جمله موارد دیگری است که کامپیوترهای متصل به اینترنت را تهدید می‌نماید. نفوذ به روش‌های مختلفی انجام می‌شود و در بسیاری از مواقع کاربر متوجه این مسئله نمی‌شود. حتی بعضی از نفوذگران ردپای خود را هم پاک می‌کنند به نحوی که حمله به سیستم قابل آشکارسازی نیست.

با این وجود نفوذکنندگان به سیستم به صورت معمول ردپاهایی از خود باقی می‌گذارند. با وجودی که تشخیص بعضی از ردپاها دشوار است ولی با استفاده از گام‌هایی که در ادامه بیان می‌شوند می‌توان بسیاری از نفوذها را تشخیص داد.

به عنوان اولین گام باید سیستم‌عامل و نرم‌افزارهای موجود در محیطی آزمایشی (مشابه شرایط عملیاتی) توصیف شوند. توصیف به این معناست که عملکرد برنامه‌ها در حال اجرا بررسی شده و موارد مختلفی مانند سرعت، زمان پاسخ، نحوه عمل و غیره به صورت دقیق شناسایی شوند. بنابراین باید برنامه‌ها را اجرا نموده و آنها را در شرایطی مشابه حالت عملیاتی قرار داد، سپس رفتار آنها را به دقت بررسی نمود.

در گام بعدی، باید از نرم‌افزارهای توصیف استفاده نمود. یکی از رایج‌ترین ابزارها برای این کار نرم‌افزار TripWire محصول tripwiresecurity.com است. این نرم‌افزار نسخه‌هایی برای سیستم‌عامل‌های مختلف دارد و متن برنامه بعضی نسخه‌های آن به کاربران عرضه می‌شود. غیر از این نرم‌افزار ابزارهای دیگری نیز وجود دارند که همین عملکرد را نشان می‌دهند. این دسته نرم‌افزارها در رده ابزارهای تشخیص نفوذ host-based قرار می‌گیرند. با جستجو بر روی اینترنت می‌توان برنامه‌های دیگری نیز با عملکرد مشابه یافت.

در نهایت باید همه فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی سیستم شناسایی شده و تغییرات آنها در زمان مورد بررسی قرار گیرند. در محیط آزمایشی کنترل شده، شرایط طبیعی شناسایی می‌شود. به خاطر داشته باشید هرگاه سیستم وارد فاز عملیاتی شود،

شرایط طبیعی بهتر شناسایی می‌شوند، زیرا هرچقدر که سیستم‌های تست خوب و قوی طراحی شوند تنها نشان دهنده تخمینی از محیط عملیاتی هستند. باید مجموعه تغییرات جدید را درک کرده و آنها را در توصیف سیستم وارد نمود.

فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی تنها بخشی از توصیف کامل سیستم کامپیوتری هستند. سایر مواردی که باید بررسی شوند به شرح زیر می‌باشند:

- **برنامه‌های در حال اجرا**

منابعی که این برنامه‌ها مورد استفاده قرار می‌دهند و زمان اجرای آنها. به عنوان مثال اگر برنامه تهیه کننده نسخه‌های پشتیبان هر روزه در زمان مقرری اجرا می‌شود، آیا این فعالیت طبیعی قلمداد می‌شود؟ در مورد برنامه واژه‌پردازی که مدت زمان زیادی از وقت CPU را اشغال نموده است چطور؟

- **ترافیک شبکه**

آیا ایجاد ناگهانی تعداد زیادی اتصال HTTP توسط سرور email طبیعی است؟ افزایش ناگهانی بار سرور وب چگونه ارزیابی می‌شود؟

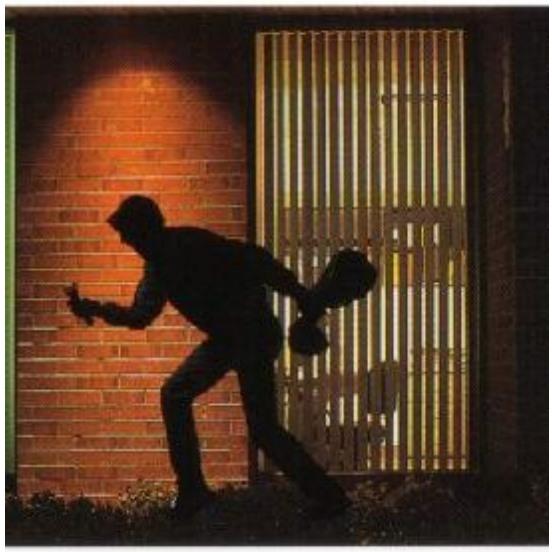
- **کارایی**

آیا سرعت وب سرور کاهش یافته است؟ سرور تراکنش، توان مدیریت چه تعداد تراکنش را دارد؟

- **سیستم عامل**

نفوذگذان در سیستم می‌توانند عملکرد سیستم عامل را به گونه‌ای عوض کنند که برنامه‌های کاربردی بدون اینکه تغییر کنند رفتاری متفاوت نشان دهند. تصور کنید

یک فراخوانی سیستم عامل که باید منجر به اجرای یک برنامه شود، برنامه دیگری را اجرا نماید.



متأسفانه ابزارهایی که برای بررسی این پارامترها وجود دارند به اندازه نرم‌افزارهایی که فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی را بررسی می‌کنند، رشد نداشته‌اند. با این وجود برای مدیریت هوشیارانه سیستم‌ها باید این پارامترها هم به صورت دقیق در توصیف سیستم قید شوند.

تنها در صورت انجام دقیق موارد فوق و نظارت بر تغییر مشخصات سیستم می‌توان به امن بودن کامپیوتر خود امیدوار بود.

ضمائم نامه های الکترونیکی

ارسال فایل و سایر مستندات به عنوان فایل ضمیمه همراه یک نامه الکترونیکی به امری متداول تبدیل شده است. علیرغم تمامی مزایای و پتانسل های ویژگی فوق، ضمائم نامه های الکترونیکی به یکی از منابع اصلی به منظور توزیع ویروس، تبدیل شده اند. استفاده کنندگان نامه های الکترونیکی، می بایست در زمان باز نمودن فایل های ضمیمه، دقت لازم را داشته باشند.(ولو اینکه این نوع ضمائم و نامه های الکترونیکی توسط افرادی ارسال می گردد که شما آنان را می شناسید).

چرا ضمائم نامه های الکترونیکی می توانند خطرناک باشند :

شاید این سوال برای شما مطرح شده باشد که چرا ضمائم نامه های الکترونیکی می توانند خطرناک بوده و تهدیدی در مقابل ایمن سازی اطلاعات باشند؟. در این رابطه به موارد زیر اشاره می گردد:

- چرخش آسان نامه های الکترونیکی: چرخش و حرکت نامه های الکترونیکی بسیار ساده بوده و ویروس ها می توانند در مدت زمان کوتاهی تعداد زیادی از ماشین ها را آلوده نمایند. اکثر ویروس ها حتی به این موضوع نیاز نخواهند داشت که کاربران نامه های الکترونیکی را فوروارد نمایند. ویروس ها، کامپیوتر کاربر را به منظور آگاهی از لیست آدرس نامه های الکترونیکی پویش نموده و به صورت اتوماتیک اقدام به ارسال پیام های آلوده برای هر یک از آدرس های موجود در دفترچه آدرس نامه های الکترونیکی، می نمایند. مهاجمان از این واقعیت ناگوار استفاده می نمایند که اکثر کاربران به نامه های ارسالی بهمراه ضمائم مربوطه از جانب هر شخص اعتماد می نمایند(سوء استفاده از حسن اعتماد کاربران).
- برنامه های پست الکترونیکی، سعی در تامین تمامی نیازهای کاربران می نمایند. تقریبا" هر نوع فایل می تواند به عنوان یک فایل ضمیمه در نظر گرفته شود.

- بنابراین مهاجمان دارای آزادی عمل زیادی در خصوص نوع ویروس ها، می باشند.
- برنامه های پست الکترونیکی دارای امکانات گسترده و متعددی در سطح لایه رابط کاربر می باشند. برخی از این نوع برنامه ها، امکان دریافت اتوماتیک ضمائم نامه های الکترونیکی را فراهم می نمایند. بدین ترتیب، امکان آلودگی سیستم بدلیل دریافت یک فایل ضمیمه آلوده افزایش خواهد یافت.

مراحل لازم به منظور حفاظت خود و سایر افراد موجود در لیست دفترچه آدرس

- **دقت لازم در خصوص ضمائم ناخواسته حتی در مواردی که از هویت فرد ارسال کننده، آگاهی لازم وجود داشته باشد.** صرف این که یک نامه الکترونیکی از طرف برادر، دوستان و یا همکاران ارسال شده باشد، به منزله ایمن بودن آنان نمی باشد. تعداد زیادی از ویروس ها قادر به "جعل" آدرس و نمایش آن به صورت یک پیام ارسالی توسط اشخاص دیگر می باشند. در صورت امکان و قبل از باز نمودن فایل ضمیمه، بررسی لازم در خصوص هویت فرد ارسال کننده فایل ضمیمه را انجام دهید. در برخی موارد این نوع نامه های الکترونیکی در ظاهری خیرخواهانه و اطلاع رسانی در خصوص ارائه یک محصول و یا Patch جدید، مخاطبان خود را شکار می نمایند. فراموش نکنیم که تولیدکنندگان نرم افزار، هرگز patch و یا محصول جدید خود را از طریق نامه الکترونیکی، ارسال نمی نمایند.

- **ذخیره و بررسی ضمائم قبل از باز نمودن آنان** : در صورتی که شما مجبور به باز نمودن یک فایل ضمیمه قبل از بررسی منبع ارسال کننده آن می باشید، پیشنهاد می گردد، مراحل زیر دنبال شود:

□ از بهنگام بودن نرم افزار آنتی ویروس خود مطمئن شوید.

□ فایل ضمیمه ارسال شده را بر روی کامپیوتر خود ذخیره نمائید.

□ با استفاده از نرم افزار آنتی ویروس، بررسی لازم در خصوص آلودگی فایل ذخیره شده را انجام دهید.

□ پس از انجام مراحل فوق و اطمینان از عدم آلودگی فایل ضمیمه، می توان آن را فعال نمود.

- **غیر فعال نمودن ویژگی دریافت اتوماتیک فایل های ضمیمه**. به منظور تسهیل در امر دریافت و مشاهده نامه های الکترونیکی، تعداد زیادی از برنامه های پست الکترونیکی، امکان دریافت اتوماتیک ضمائم نامه های الکترونیکی را در برنامه خود پیش بینی نموده اند. پیشنهاد می گردد بررسی لازم در خصوص تنظیمات موجود نرم افزار استفاده شده به منظور دریافت نامه های الکترونیکی انجام و در صورت وجود ویژگی فوق، آن را غیرفعال نمائید.

برنامه های IM و Chat

با این که برنامه های IM و Chat ، روشی مناسب به منظور ارتباط با سایر افراد می باشند، ابزارهای استفاده شده برای این نوع از مبادلات اطلاعاتی online می تواند خطرناک بوده و نتایج مخربی را به دنبال داشته باشد.

تفاوت ابزارهای استفاده شده برای مبادلات online

به منظور مبادله اطلاعاتی online بر روی اینترنت، از ابزارهای متعددی استفاده می گردد. بررسی ویژگی هر یک از این ابزارهای موجود بهمراه تمهیدات مربوطه، امکان استفاده ایمن و مطمئن از این نوع ابزارها را فراهم می نماید.

- **برنامه های IM (Instant messaging)** : از این نوع برنامه ها به منظور تفریح، سرگرمی، ارسال پیام، ارتباط صوتی و یا تصویری با سایر افراد استفاده می گردد. از برنامه های فوق در سازمان ها به منظور ارتباط بین کارکنان نیز استفاده می گردد. صرفنظر از نوع برنامه انتخابی IM ، این نوع برنامه ها بستر مناسبی به منظور ارتباط یک به یک را ایجاد می نماید.
- **اطاق های چت**: اطاق های چت صرفنظر از عمومی بودن و یا خصوصی بودن، تالارهائی برای گروههای خاص از مردم و به منظور ارتباط با یکدیگر می باشند. اکثر اطاق های چت مبتنی بر خصایص مشترکی می باشند: مثلاً" اطلاق هائی مختص افرادی با سن خاص و یا علائق مشترک. با اینکه اکثر برنامه های سرویس گیرنده IM از چت، حمایت می کنند، برنامه های IM همچنان و بر اساس روش سنتی خود ابزاری برای ارتباطات یک به یک می باشند. در حالی که چت به صورت سنتی ابزاری برای ارتباط چند نفر به چند نفر می باشد. به منظور طراحی و پیاده سازی برنامه های فوق از فن آوری های متعددی نظیر: IM ، IRC و یا

Jabber استفاده می گردد. برخی از نرم افزارهای ارائه شده با ترکیب چندین قابلیت توانسته اند پاسخگوی خواسته های متنوع کاربران باشند.

تهدیدات این نوع برنامه ها چیست ؟

- **وجود ابهام در خصوص هویت مخاطب**. در برخی موارد نه تنها شناسائی مخاطب و شخصی که در حال ارتباط با وی هستید مشکل می باشد بلکه ماهیت انسانی و رفتاری وی نیز قابل پیش بینی نخواهد بود. مردم ممکن است در رابطه با هویت خودشان، گزاف گفته، account ها ممکن است در معرض سوء ظن باشند و یا ممکن است کاربران عملیات logout را فراموش نمایند. در برخی موارد ممکن است یک account توسط چندین نفر و به صورت مشترک استفاده می گردد. تمامی موارد فوق، دلیلی است بر این ادعا که نمی توان بطور واقعی و حقیقی در رابطه با ماهیت شخصی که در حال گفتگو با وی هستید، قضاوت کرده و به یک سطح مطلوب از اطمینان دست پیدا کرد.
- **کاربران، مستعد انواع حملات می باشند**. سعی کنید به شخصی بقبولانید که برنامه ای را اجراء و یا بر روی یک لینک، کلیک نماید. اجرای یک برنامه به توصیه دیگران و یا کلیک بر روی یک لینک پیشنهادی توسط سایرین، یکی از روش های متداول به منظور انجام برخی تهاجمات می باشد. این موضوع در اطاق های چت و یا برنامه های IM امری متداول و مرسوم است. در محیطی که یک کاربر در این اندیشه است که در یک جو مطمئن و اعتمادپذیر در حال گفتگو با اشخاص است، یک کد مخرب و یا یک مهاجم می تواند شانس بیشتری برای رسیدن به اهداف خود و به دام انداختن سایر افراد را داشته باشد.
- **عدم وجود آگاهی لازم در خصوص سایر افراد درگیر و یا ناظر گفتگو**: مبادلات online بسادگی ذخیره می گردند و در صورتی که شما از یک سرویس اقتصادی رایگان استفاده می نمائید، ماحصل گفتگوی انجام شده می تواند بر روی

یک سرویس دهنده ذخیره شده (logs) و شما هیچگونه کنترلی در خصوص این logs نخواهید داشت. شما نمی دانید که آیا اشخاص و افراد دیگر نظاره گر این گفتگو می باشند یا خیر؟ یک مهاجم می تواند بسادگی اقدام به شنود اطلاعات و ره گیری آنان از طریق مبادلات اطلاعاتی انجام شده در اطاق های چت نماید.

- **نرم افزاری که شما بدین منظور استفاده می نمائید ممکن است دارای نقاط آسیب پذیر خاص خود باشد.** همانند سایر نرم افزارها، نرم افزارهای چت، ممکن است دارای نقاط آسیب پذیری باشند که مهاجمان با استفاده از آنان می توانند به اهداف خود نائل گردند.
- **تنظیمات امنیتی پیش فرض انجام شده، ممکن است به درستی مقداردهی نشده باشند.** تنظیمات امنیتی در نرم افزارهای چت، با نگرشی خیرخواهانه و ساده در نظر گرفته شده تا بدینوسیله و به زعم خود پتانسیل های بیشتری را در اختیار متقاضیان قرار دهند. رویکرد فوق، کاربران و استفاده کنندگان از این نوع برنامه ها را مستعد انواع حملات توسط مهاجمان می نماید.

چگونه می توان از این ابزارها به صورت ایمن استفاده نمود ؟

- **بررسی و ارزیابی تنظیمات امنیتی**: در این رابطه لازم است تنظیمات پیش فرض در نرم افزار به منظور بهینه سازی امنیتی آنان بررسی گردد. مطمئن شوید که ویژگی دریافت اتوماتیک فایل (Download)، غیر فعال شده باشد. برخی از نرم افزارهای چت، امکان ارتباط محدود با افراد را ارائه می نماید. در صورتی که از این نوع برنامه ها استفاده می نمائید، پیشنهاد می گردد ویژگی فوق فعال گردد.
- **هشیاری و دقت لازم در خصوص افشای اطلاعات.** تا زمانی که نسبت به هویت طرف درگیر در ارتباط اطمینان لازم را کسب نکرده اید، از افشای اطلاعات شخصی و مهم خود جدا" اجتناب کنید. مبادله اطلاعات در اطاق های چت

می بایست با دقت و حساسیت بالا، انجام شود. هرگز اطلاعات تجاری و حساس مربوط به سازمان خود را در اطاق های چت و یا برنامه های عمومی IM افشاء و برملاء ننمائید.

- **شناسائی هویت افرادیکه در حال گفتگو با آنان هستید(حتی المقدور)**. در برخی موارد تشخیص هویت فردی که در حال گفتگو با وی می باشید، چندان حائز اهمیت نمی باشد. در صورتی که شما نیازمند سطح خاصی از اطمینان در خصوص شخص مورد نظر می باشید و یا قصد اشتراک اطلاعاتی خاص با وی را دارید، شناسائی هویت مخاطب بسیار حائز اهمیت است(مطمئن شوید شخصی که در حال گفتگو با وی هستید، همان شخص مورد نظر شما است).
- **عدم اعتماد و باور هر چیز**: اطلاعات و یا توصیه هائی که شما از طریق یک اطاق چت و یا برنامه های IM دریافت می نماید، ممکن است نادرست، غلط و حتی مخرب باشند. در اینگونه موارد می بایست در ابتدا بررسی لازم در خصوص صحت اطلاعات و یا دستورالعمل های ارائه شده، انجام و در ادامه از آنان استفاده گردد.
- **بهنگام نگه داشتن نرم افزارها**: فرآیند بهنگام سازی نرم افزارها شامل نرم افزار چت، مرورگر وب، سیستم عامل، برنامه سرویس گیرنده پست الکترونیکی و برنامه آنتی ویروس است. عدم بهنگام بودن هر یک از برنامه های فوق می تواند زمینه بروز تهاجمات توسط مهاجمان را فراهم نماید.

انتخاب و محافظت از کلمات عبور

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از اکانت کاربران قرار می گیرند. یک کلمه عبور نامناسب ممکن است منجر به سوءاستفاده از کل شبکه شود. بهمین دلیل تمام کارمندان شامل پیمانکاران و فروشندگان که به سیستم شرکت دسترسی دارند مسوول انتخاب کلمه عبور مناسب و محافظت از آن هستند.

در این قسمت به نکاتی در مورد ایجاد کلمات عبور قوی و محافظت از آنها و زمان انقضاء و تغییر آنها اشاره می شود. در حقیقت مخاطب این مقاله تمام افرادی هستند که مسوول اکانت یا هر سیستمی هستند که از طریق آن به شبکه یا اطلاعات غیرعمومی دسترسی دارند.

سیاست کلی

- تمام کلمات عبور در سطح سیســـتم باید حداقل سه ماه یکبار عوض شونـــد.
- تمام کلمات عبور سطح کاربر(مانند ایمیل یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می شود.
- اکانتهای کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانتهای آن کاربر متفاوت باشد.
- کلمات عبور نباید در ایمیلها یا سایر شکلهای ارتباطات الکترونیکی درج شوند.
- باید رهنمونهای زیر در تمام کلمات عبور سطح سیستم و سطح کاربر رعایت شود.

راهنماییها

راهنمایی کلی ساخت کلمه عبور

کلمات عبور برای اهداف گوناگونی در شرکتها استفاده می شوند. تعدادی از استفاده های معمول اینها هستند:

- اکانتهای سطح کاربر
- اکانتهای دسترسی به وب
- اکانتهای ایمیل
- حفاظت از مونیتور
- کلمه عبور صندوق پستی

. ورود به روتر محلی

چون سیستمهای بسیار کمی از نشانه های یکبارمصرف استفاده می کنند (مانند کلمات عبور دینامیک که فقط یکبار استفاده می شوند)، هرکسی باید از نحوه انتخاب کلمات عبور مناسب آگاه باشد.

کلمات عبور ضعیف معمولا مشخصات زیر را دارند:

- کلمه عبور شامل کمتر از هشت حرف است.
- کلمه عبور کلمه ای است که در یک فرهنگ لغت یافت می شود.
- کلمه عبور کلمه ای است که کاربردعمومی دارد مانند: نام خانوادگی، حیوانات اهلی، دوستان، همکاران، شخصیت های خیالی وغیره نامها و اصطلاحات کامپیوتری، فرمانها، سایتها، شرکتها، سخت افزار و نرم افزار.

نام شرکت یا کلمات مشتق شده از این نام.

. تاریخ های تولد و سایر اطلاعات شخصی مانند آدرس ها و شماره های تلفن.

. الگوهای کلمات یا شماره ها مانند aaabbb، qwerty، zyxwvuts، 123321 و غیره.

. هرکدام از عبارات فوق بطور برعکس.

. هرکدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم می شود.

کلمات عبور مناسب مشخصات زیر را دارند:

- شامل هم حروف کوچک و هم بزرگ هستند (a-z و A-Z)
- علاوه بر حروف از ارقام و نشانه ها هم در آنها استفاده می شود مانند 0-9 و !@#$%^&*()_+|~='{}[];<>?./
- حداقل هشت حرف دارند.
- کلمه ای در هیچ زبان، گویش یا صنف خاص نیستند.
- برپایه اطلاعات شخصی، اسم یا فامیل نیستند.
- کلمات عبور هرگز نباید نوشته یا جایی ذخیره شوند. سعی کنید کلمات عبوری انتخاب کنید که بتوانید براحتی در ذهن داشته باشید. یک روش انجام این کار، ایجاد کلمه عبور بر پایه یک ترانه یا عبارت است.

برای مثال عبارت "This May Be One Way To Remember" و کلمه عبور می تواند "TmB1w2R!" یا "Tmb1W>r~" یا انواع دیگری از همین الگو باشد.

توجه: این مثالها را بعنوان کلمه عبور استفاده نکنید.

استانداردهای حفاظت از کلمه عبور

از کلمات عبور مشترک برای اکانتهای شرکت و دسترسی های شخصی استفاده نکنید. تا جایی ممکن است، از کلمه عبور مشترک برای نیازهای مختلف شرکت استفاده نکنید. برای مثال، برای سیستمهای مهندسی یک کلمه عبور انتخاب کنید و یک کلمه عبور دیگر برای سیستمهای IT . همچنین برای استفاده از اکانتهای NT و UNIX کلمات عبور متفاوت انتخاب کنید.

کلمات عبور شرکت با هیچ کس از جمله دستیاران و منشی ها در میان نگذارید. باید با تمام کلمات عبور بصورت اطلاعات حساس و محرمانه برخورد شوند.

در اینجا به لیستی از "انجام ندهید" ها اشاره می شود.

- کلمه عبور را از طریق تلفن به هیچ کس نگویید.
- کلمه عبور را از طریق ایمیل فاش نکنید.
- کلمه عبور را به رئیس نگویید.
- در مورد کلمه عبور در جلوی دیگران صحبت نکنید.
- به قالب کلمه عبور اشاره نکنید. (مثلا نام خانوادگی)
- کلمه عبور را روی فهرست سوالات یا فرمهای امنیتی درج نکنید.
- کلمه عبور را با اعضای خانواده در میان نگذارید.
- کلمه عبور را هنگامی که در مرخصی هستید به همکاران نگویید.

اگر کسی از شما کلمه عبور را پرسید، از ایشان بخواهید که این مطلب را مطالعه کند یا اینکه با کسی در قسمت امنیت اطلاعات تماس بگیرد.

از ویژگی "Remember Password" یا حفظ کلمه عبور در کامپیوتر استفاده نکنید.

مجدداً، کلمات عبور را در هیچ جای محل کار خود ننویسید و در فایل یا هر سیستم کامپیوتری ذخیره نکنید(شامل کامپیوترهای دستی) مگر با رمزکردن.

کلمات عبور را حداقل هر شش ماه عوض کنید(بجز کلمات عبور سطح سیستم که باید هر سه ماه تغییر کنند).

اگر هر اکانت یا کلمه عبور احتمال فاش و سوء استفاده از آن میرود، به بخش امنیت اطلاعات، اطلاع دهید و تمام کلمات عبور را تغییر دهید.

شکستن یا حدس زدن کلمه عبور ممکن است در یک زمان متناوب یا اتفاقی توسط بخش امنیت اطلاعات یا نمانیدگی های آن رخ دهد. اگر کلمه عبور در طول یکی از این پیمایش ها حدس زده یا شکسته شود، از کاربر خواسته خواهد شد که آن را تغییر دهد.

رعایت موارد مذکور، به حفاظت بیشتر از اطلاعات و قسمتهای شخصی افراد کمک خواهد کرد.

سیاست های امنیتی

در دنیایی که وجه مشخصه آن فناوری سطح بالا و ارتباطات گسترده می باشد، هر سازمانی نیاز به سیاست های امنیتی که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط هکرها، رقبا و یا کشورهای خارجی منافع سازمان را تهدید می کند. هدف سیاست های امنیتی تعریف روال ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می نماید. با اجرای دقیق سیاست های امنیتی، سازمان ها می توانند تهدیدات را کاهش دهند.

مفاهیم

سیاست امنیتی یک سازمان سندی است که برنامه های سازمان برای محافظت سرمایه های فیزیکی و مرتبط با فناوری ارتباطات را بیان می نماید. به سیاست امنیتی به عنوان یک سند زنده نگریسته می شود، بدین معنا که فرایند تکمیل و اصلاح آن هیچ گاه متوقف نشده، متناسب با تغییر فناوری و نیازهای کاربران به روز می شود. چنین سندی شامل شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست های امنیتی و راه کار به روز رسانی آنها می باشد.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است ولی در مورد راه کارهای مهندسی و پیاده سازی این اهداف بحثی نمی کند. سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر، از نظر عملی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن سطح حافظتی قابل قبولی را ارائه نماید.

تدوین سیاست

بهترین روش برای دستیابی به امنیت اطلاعات، فرموله نموده سیاست امنیتی است. مشخص نمودن سرمایه های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر اینکه چه افرادی به چه سرمایه هایی دسترسی دارند) در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند و از سوی دیگر مدیران سیستم و سازمان را در تصمیم گیری برای پیکربندی و استفاده از سیستم ها یاری رساند.

برای تدوین سیاست امنیتی پس از تحلیل ریسک های سازمان، می توان به روش هایی که دیگران برگزیده اند متوسل شد. معمولا تجارب مفیدی که قبلا در صنایع مشابه انجام شده و نتایج خوبی از آنها نتیجه شده است به صورت عمومی گزارش شده و در قالب مقالات تخصصی ارائه می گردند. استانداردهای شناخته شده ای نیز برای این کار وجود دارد که می توان از آنها هم بهره گرفت.

سازمان های بزرگ و متوسط برای تعریف سیاست امنیتی خود ناچار به پیروی روش بالا به پایین می باشند. ولی برای سازمان های کوچک انجام این کار به روش پایین به بالا نیز امکان پذیر است. در این حالت از قابلیت های ابزارهای موجود بهره گرفته می شود.

همانگونه که هرم سیاست فوق نشان می دهد، بهترین سیاست امنیتی در شرایطی تدوین می گردد که مدیریت سازمان سیاست کلی را ارائه نموده و یا دستور پیاده سازی اصول امنیتی را در سازمان صادر کند. تدوین کنندگان سیاست سازمان باید فعالیت خود را بر پایه اصول و استانداردهای صنعتی مانند ISO17799 و یا HIPAA انجام دهند. رویه ها، راهنماها و تجربیات پایه ای برای ایجاد و توسعه فناوری امنیتی در سازمان های مختلف هستند. محصولاتی مانند ESM سازگاری و انعطاف سیاست را با سیاست ها و روال های امنیتی سیستم عامل ها، پایگاه داده ها و برنامه های کاربردی ارزیابی می نمایند. این ابزارها ممکن است با محیط کامپیوتری و شبکه سازمان در تعامل باشند.

استانداردها و روال های امنیتی

سیاست های امنیتی دربردارنده کلیه انتظارات، برنامه ها و اهداف عملیاتی مدیریت سازمان می باشد. برای عملیاتی و قابل اجرا بودن، سیاست امنیتی باید با استفاده از استانداردها، راهنماها و رویه های شناخته شده تعریف شود که اطمینان از سازگاری کلیه عملیات اجرایی با سیاست های امنیتی حاصل گردد.

استاندارها، راهنما ها و روال ها تفسیر خاصی از سیاست را ارائه می کنند و کاربران، مشتریان و مدیران سازمان را برای پیاده سازی سیاست آماده می نمایند.

ساختار سیاست امنیتی

ساختار سیاست امنیتی مرکب از اجزاء زیر می باشد:

- عبارتی در رابطه با موضوع سیاست
- چگونگی اجرای سیاست در محیط سازمان
- نقش و مسئولیت افراد مختلف تاثیر گذار در سیاست
- سیاست به چه میزان انعطاف پذیر است؟
- اعمال، فعالیت ها و فرایندهای مجاز و غیر مجاز
- موارد سخت گیری و عدم انعطاف سیاست

سه محور اصلی در کنترل دسترسی در شبکه

AAA (Authentication, Authorization and Accounting)

AAA که مخفف Authentication, Authorization and Accounting است سه محور اصلی در کنترل دسترسی در شبکه هستند که در این بخش در مورد هریک از آنها به طور مجزا و مختصر صحبت می‌شود. ابتدا تعریفی از هریک از این مفاهیم ارائه می‌دهیم.

۱ – Authentication

۱-۱ – مفهوم Authentication

به معنای وارسی عناصر شناسایی ارائه شده از سوی کاربر، تجهیزات یا نرم‌افزارهایی است که تقاضای استفاده و دسترسی به منابع شبکه را دارند. عناصر شناسایی در ابتدایی‌ترین و معمول‌ترین حالت شامل نام کاربری و کلمه عبور می‌باشند. در صورت نیاز به بالاتر بودن پیچیدگی فرایند کنترل و وارسی هویت، می‌توان با اضافه نمودن عناصر شناسایی به این مهم دست یافت. بدیهی است که با اضافه نمودن فاکتورها و عناصر شناسایی، نوع خادم مورد استفاده، پایگاه‌های داده‌ای مورد نظر و در بسیاری از موارد پروتکل‌ها و استانداردها نیز باید مطابق با تغییرات اعمال شده در نظر گرفته شوند تا یکسانی در ارائه خدمات در کل شبکه حفظ شود.

پس از ارائه عناصر شناسایی از سوی متقاضی، سیستم کد کاربری و کلمه عبور را با بانک اطلاعاتی مختص کدهای شناسایی کاربری مقایسه کرده و پذیرش یا عدم پذیرش دسترسی به منابع را صادر می‌کند.

عمل Authentication، در طراحی شبکه‌هایی با حجم کم و متوسط عموماً توسط تجهیزات مسیریابی و یا دیوارهای آتش انجام می‌گیرد. علت استفاده از این روش مجتمع سازی و ساده سازی پیاده‌سازی عمل Authentication است. با استفاده از امکانات موجود نیاز به استقرار یک خادم مجزا برای صدور پذیرش هویت متقاضیان دسترسی مرتفع می‌گردد.

از سوی دیگر در شبکه‌های با حجم و پیچیدگی نسبتاً بالا، عموماً با توجه به پردازش بالای مختص عمل Authentication، خادمی بصورت مستقل و مجزا به این امر اختصاص می‌یابد. در این روش از استانداردها و پروتکل‌های مختلفی همچون TACACS+ و RADIUS استفاده می‌گردد.

۲-۱ - فعال نمودن Authentication

فعال نمودن Authentication بر روی تجهیزات مورد استفاده در شبکه عملی است که عموماً در چهار مرحله انجام می‌شود :

الف - فعال نمودن AAA بر روی سخت‌افزارهای مورد نظر

ب - ایجاد پایگاه داده‌ای از کدهای کاربری کاربران یا تجهیزات شبکه به همراه کلمه‌های عبور. همانگونه که ذکر شد، این پایگاه می‌تواند در داخل تجهیزات مورد استفاده در شبکه‌های با حجم کم پیاده‌سازی شود. در شبکه‌های با حجم نسبتاً بالا که در آنها نیاز به

استفاده از خادمی مختص عمل Authentication احساس می‌شود، تجهیزات فعال شبکه به گونه‌ای پیکربندی می‌شوند که عمل Authentication را با استفاده از پایگاه‌های داده‌ای مستقر بر روی خادم‌های مختص این فرایند، انجام دهند.

ج – ایجاد فهرست(های) روش انجام عمل Authentication. این فهرست‌ها به تعیین روش مورد نظر برای عمل Authentication اختصاص دارند.

د – اعمال فهرست(های) روش ساخته شده ار مرحله قبل.

در هر شبکه، در صورت نیاز به عمل Authentication، این چهار مرحله بر روی تمامی تجهیزاتی که در عمل AAA نقش دارند اجرا می‌شوند.

۲ – Authorization

۲-۱ – مفهوم Authorization

Authorization فرایندی است که طی آن به کاربران و یا تجهیزات متقاضی دسترسی به منابع، امکان استفاده از منبع یا منابع مستقر بر روی شبکه داده می‌شود. به بیان دیگر این عمل برای مدیران شبکه امکان تعیین نوع دسترسی به هریک از منابع شبکه، برای تک تک متقاضیان دسترسی و یا گروهی از آنها، را فراهم می‌کند.

از سوی دیگر، عمل امکان اختصاص آدرس‌های شناخته شده و از پیش تعیین شده به کاربران یا تجهیزات، همچون متقاضیانی که با استفاده از پروتکل PPP به شبکه متصل می‌شوند، را می‌دهد. این عمل متقاضی را ملزم به استفاده از نوع خاصی ار استانداردها یا پیکربندی‌های ارتباطی مورد نظر مدیر شبکه می‌کند.

زمانی که Authorization بر روی شبکه فعال شده باشد، خادم شبکه‌ای که مسئولیت Authorization را بر عهده دارد اطلاعات کاربر را از روی پایگاه داده کاربرها استخراج می‌کند. این پایگاه داده می‌تواند بر روی خادم محلی بوده و یا بر روی پایگاهی مجزا قرار داشته باشد.

پس از استخراج این اطلاعات، وضعیت دسترسی مورد قبول مدیریت با تقاضای کاربر قیاس گردیده و تایید یا عدم تایید اجازه استفاده از سرویس یا منبع مورد نظر متقاضی صادر می‌شود.

۲-۲ – برقراری Authorization

برقراری و فعال نمودن Authorization عملی مشابه فعال نمودن Authentication است. برای برقراری و فعال نمودن Authorization، Authentication باید فعال شده باشد. به عبارت دیگر کلیه مراحل را می‌توان به شکل زیرخلاصه نمود:

الف – فعال نمودن Authentication بر روی سخت‌افزارهای مورد نظر. همانگونه که ذکر شد اولین مرحله از چهار مرحله فعال‌سازی این فرایند، فعال سازی AAA بر روی تجهیزات است.

ب – ایجاد فهرست(های) روش انجام عمل Authorization. این فهرست‌ها علاوه بر تعیین روش مورد نظر برای عمل Authorization، مبین سرویس مورد نظر برای عمل Authorization نیز می‌باشند.

ج – اعمال فهرست(های) روش ساخته شده ار مرحله قبل.

۳ – Accounting

۳-۱ – مفهوم Accounting

Accounting آخرین بخش از فرایند جمعی AAA است. طی این فرایند، گزارشی از عملکرد کاربران یا سخت‌افزارهایی که هویت آنها طی اعمال Authentication و Authorization تایید شده است، توسط خادم AAA تهیه می‌شود. این عمل می‌تواند با استفاده از خادم های خارجی که اس پروتکل‌ها و استانداردهایی چون TACACS+ و RADIUS استفاده می‌کنند انجام گیرد.

به بیان دیگر، این عمل قدمی فراتر از دو مرحله پیشین برداشته، و پیگیری بعدی، پس از احراز هویت را انجام می‌دهد. پیام‌های Accounting به شکل رکورد، میان تجهیزاتی که از طریق آنها دسترسی متقاضی درخواست شده و پایگاه‌های داده‌ای از قبیل TACACS+ یا RADIUS، تبادل می‌گردد.

۳-۲ – فعال سازی Accounting

فرایند فعال سازی Accounting مشابه Authorization است که مهم‌ترین مراحل شامل ایجاد فهرست‌های روش Accounting و اعمال آنهاست

روشهای پنهان سازی سرورهای وب برای افزایای ایمنی

پوشش دادن یا پنهان کردن یک وب سرور شامل از بین بردن جزئیات هویتی ای است که هکرها می توانند برای کشف سیستم عامل و وب سرور نصب شده روی آن مورد استفاده قرار دهند. این اطلاعات در حالی که هیچ استفاده ای برای بهره برداران مشروع ندارد، اغلب نقطه شروعی برای هکرها می باشد.

دراین مقاله به بررسی برخی راهکارهایی که می توانیم با به کارگیری آنها خطر شناسایی را به حداقل برسانیم، می پردازد. بیشتر مثالها مربوط به IIS میکروسافت می باشد. زیرا بخاطر آسیب پذیری زیادش به طور وسیعی مورد توجه نفوذگران قرار گرفته است. همچنین یک سری از اقدامات پیشگیرانه شناسایی برای آپاچی سرور نیز ذکر خواهد شد. غیر قابل شناسایی کردن سرور وظیفه همه کسانی است که مسئولیت اجرایی وب سرور را بر عهده دارند.

نفوذگران از اینجا شروع می کنند ، چرا شما از این نقطه شروع نمی کنید ؟

بگذارید از نقطه نظر مهاجمین نگاه کنیم. آسیب پذیریهای امنیتی متکی بر نسخه (Version) و نوع نرم افزار دارند.

یک نفوذگر برای نفوذ به یک وب سرور باید بداند وب سرور از چه نوعی و دارای چه ورژنی می باشد. دانستن جزئیات یک وب سرور کارآمدی هرگونه تهاجمی را به مقدار زیاد افزایش می دهد.

Server Header ها همه چیز را می گویند:

بسیاری از وب سرورها خودشان و سیستم عاملی را که بر روی آن نصب هستند به هر کسی که بخواهد معرفی می نمایند.

با استفاده از ابزارهای بررسی شبکه مانند Sam Spade یا Header Check می توانید http هدرهای سرور را تشخیص دهید. تنها کافیست Home Page وب سایت را درخواست نموده و http هدرهای حاصله یا بنرهایی که توسط سرور ارسال گردیده را مورد بررسی قرار دهید. در میان آنها احتمالا چیزی شبیه به : Server Microsoft – IIS/5.0 پیدا خواهید کرد.

آپاچی سرور نیز به صورت پیش فرض همه مشخصات را اعلام می کند.

Server : Apache/2.0.41-dev(unix)

کاربران آپاچی سرور 2.x دارای مدول Mod Header هستند . این کاربران می توانند به سادگی فایل httpd.conf را به صورت زیر ادیت نمایند:

Header Set Server "New Server Name"

متاسفانه در نسخه های پیشین آپاچی سرور نمی توان سرور هدرها را تغییر داد.

کاربران IIS نیز می توانند Lock Down را نصب نموده و برای برداشتن وجایگزین کردن هدرها از فایل پیکره بندی URLScans استفاده نمایند. در صورتی که از سرور Cold Fusion استفاده می نمایید و می خواهید URLScans را به کار برید بسیار محتاط باشید. زیرا روشی که در حال حاضر هدرها را جایگزین می نماید باعث خسارات سنگینی به صفحات CFM می گردد. در این حالت تنها راه ممکن برداشتن هدرهاست.

پسوند فایلها :

نمایش پسوند فایلها مانند .ASP یا .ASPX به طور مشخص نشان دهنده آن است که شما از یک سرور مایکروسافت استفاده می کنید. به طور کلی پنهان کردن پسوند فایلها

کار مفیدی است. در طراحی سایتها سعی کنید از HTML و Java استفاده کنید. پسوند فایلهای طراحی شده توسط این زبانها نشان دهنده نوع وب سرور نمی باشد.

در مورد آپاچی سرور به مدول mod negotiation توجه خاصی داشته باشید. بوسیله این مدول می توانید پسوند فایلها را مخفی کنید. همچنین توسط mod header می توان پسوند فایلها را تعویض نمود.

کاربران IIS نیز می توانند از برنامه PageXChanger برای پنهان ساختن پسوند فایلها استفاده نمایند.

ASP Session ID Cookie

این کوکی ها وظیفه حفظ وضعیت سرویس گیرنده را بر عهده دارند و به سادگی سیستم عامل و وب سرور نصب شده بر روی آن را مشخص می کنند.

```
Set –
Cookie:ASPESSIONIDQGQGGWFC=MGMLNKMDENPEOPIJHPO
PEPPB;
```

شما می توانید ASP Session State را از کار بیندازید. همچنین می توانید برای تغییر اسامی کوکی ها از یک فیلتر ISAPI استفاده نمایید. از طرفی ASP Session ها باعث محدود شدن منابع سیستم می گردند. از کار انداختن آن به بهبود اجرایی ASP کمک می کند و باعث گمنام ماندن سرور شما نیز می گردد.

WebDAV

راه دیگر شناسایی سرورهای ویندوزی WebDAV می باشد. WebDAV منحصر به مایکروسافت یا IIS نمی باشد ، بلکه یک استاندارد پیشنهادی (RFC 2518) با گروه کاری IETF است. سرور ویندوزی در حالت پشتیبانی WebDAV اطلاعات زیادی را

به هدر می افزاید که می تواند مورد استفاده هکرها قرارگیرد. در صورتیکه از WebDAV برای پشتیبانی Outlook Web Access , Web Folders یا... استفاده نمی نمایید، می توانید با استفاده ازIISLockDown یا تغییر در رجیستری آن را از کار بیندازید.

هدرهای دیگر

برخی از سرورهای وب به وسیله نمایش هدرهای خاص در پاسخهای HTTP هویت خود را فاش می سازند. هدرهای X-Powered-By و X-ASPNET-Version علائم بارزی هستند که نشان دهنده استفاده از ASP.NET و بنابراین میزبانی IIS می باشند. همچنین به یاد داشته هدرهای Microsoft Office Web Server را باید مخفی کنید.

Windows Authentication

کاربران IIS نباید Windows Authentication را به عنوان راهی برای پنهان نمودن اطلاعات بر روی سرور مورد استفاده قرار دهند. زیرا این شیوه اطلاعات زیادی را در مورد سرور بر ملا می سازد. یک هکر می تواند با توجه به هدرهای WW- Authentication نوع وب سرور را مشخص نماید. زمانی که یک فایل یا فولدر توسط پروسه Authentication ویندوز محافظت می شود، درهدرهای فرستاده شده از طرف سرور String NTLM وجود دارد که می تواند مورد بهره برداری هکر قرار گیرد.

پیام های پیش فرض

پیامها ، صفحات و اسکریپتهای پیش فرض نیز باعث شناسایی وب سرور می گردد. اغلب نرم افزارهای پشتیبانی کننده وب سرور دارای پیغامهای پیش فرض هستند که باید به گونه ای مناسب تغییر پیدا کند. همچنین تمام Administration Pages ، اسکریپتها و Document هایی که همراه با وب سرور نصب می شوند باید مخفی یا پاک شوند.

دیگر سرویسها

بسیاری از کامپیوترهایی که با عنوان وب سرور استفاده می شوند، جدا از خدمات HTTP خدمات دیگری مانند SMTP و FTP را ارائه می دهند. به عنوان یک قانون امنیتی سعی کنید چنین سرویسهایی را در وب سرور خود راه اندازی نکنید. به ویژه از سرویسهای پیش فرض FTP و SMTP در مایکروسافت IIS اجتناب کنید. زمانی که یک ارتباط با سرویس SMTP برقرار می گردد. یک پیغام خوش آمدگویی برای Client فرستاده می شود. این پیغام هیچ تاثیری در سرویس ایمیل ندارد. اما مشابه هدرهای HTTP اطلاعاتی را در مورد وب سرور بر ملا می سازند. سرویس پیش فرض SMTP ویندوز چنین اطلاعاتی را نمایان می سازد. همچنین سرور پیش فرض IIS، FTP یک بنر شناخته شده را ارائه می دهد. از آنجایی که اصلاح این بنر از اصلاح بنر SMTP پروسه پیچیده تری است بهترین راه جایگزینی آن با یک FTP سرور دیگر مانند RhinoSoft"s Serv-U FTP Server است. که بتوان هرگونه پیغامی را در بنر FTP نمایش داد. همچنین این FTP سرور دارای امتیازات دیگری نیز از نظر ایمنی می باشد.

ورودهای غیر مجاز

بسیاری از Exploits ها از یک URL پیچیده برای گرفتن شل (Shell) یا کنترل یک CGI Program استفاده میکنند که هکر بوسیله آنها می تواند لیستی از فایلها سیستم عامل را بدست آورد. بهترین روش برای مقابله با اینگونه حملات استفاده از یک فیلتر داده می باشد که کاراکترهای غیر قابل قبول مثل متا کاراکترها را از اطلاعاتی که توسط کاربر وارد می شود حذف نماید.

برای IIS استاندارد جاری IISLockDown/URL Scan است. نسل جدیدی از Firewall ها نیز قابلیت پشتیبانی از لایه های کاربردی Web Server را دارا هستند.

پشته ها

حتی زمانیکه علائم افشاگرانه از روی لایه کاربردی وب سرور حذف شد، بر روی لایه های پایین تر شبکه نقاط ضعف آشکارسازی باقی می ماند. هر سروری با یک اتصال شبکه دارای یک Network Protocol است که قابل اسکن و شناسایی می باشد، بهترین اسکنرهای پشته مانند NMAP می تواند با استفاده از تکنیکهای مختلف سیستم عامل را شناسایی کند. همچنین پشته IP مربوط به هر سیستم عامل نیز در مقابل شناسایی از طریق پروتوکل ICMP آسیپ پذیر است. اولین راه مقابله با این نوع آسیب پذیری ها استفاده از یک فایروال می باشد. به این نکته توجه داشته باشید که با وجود فایروال ، یک تحلیل شبکه ای دقیق هنوز هم می تواند نوع وب سرور را مشخص سازد.

Netcraft

در سایت Netcraft با وارد نمودن URL هر وب سایت می توان به اطلاعاتی در مورد سیستم عامل و وب سرور آن سایت بدست آورد. با تغییر دادن HTTP هدرها می توان کاری کرد که گزارش Netcraft اشتباه شود. همچنین با حذف HTTP هدرها، Netcraftگزارش ناشناس بودن وب سرور را ارائه خواهد کرد.

پیش فرضهای TCP/IP

احتمالاً هنوز سیستم عامل شما حتی از پشت یک دیوار آهنین نیز مورد شناسائی قرار خواهد گرفت. برای آنکه بتوان یک سیستم عامل را به طور کامل ناشناس کرد باید برخی از پیش فرض های محیط TCP/IP مانند (Receive Window size) RWIN، (Maximum Transmission Units) MTU ، MSS (Maximums Segment Size)، (Time-to-Live) TTL دستکاری شود . در زمان تغییر دادن این پیش فرض ها بسیار محتاط باشید زیرا می تواند تاثیر معکوس بر روی وب سرور داشته و یا سیستم عامل را به طور کامل فلج سازد.

به خاطر داشته باشید :

برای آنکه وب سرور شما کاملاً ناشناخته بماند باید تمام مواردی که در بالا ذکر شده است را بصورت ترکیبی به کار برید. همیشه به یاد داشته باشید این اقدامات پیشگیرانه تنها می تواند باعث شکست اکثر نفوذ گران گردد نه همه آنها. یک نفوذگر ماهر و مصمم می تواند از تمامی این سدها عبور کند...

بستن درگاه ها بدون استفاده از حفاظ

مقدمه

درگاه های باز همواره راه نفوذی عالی برای حمله کنندگان به سیستم های کامپیوتری هستند. درعین حال که ارتباطات سیستم های کامپیوتری بر روی شبکه از طریق درگاه ها انجام می شود، در صورت عدم پیکربندی مناسب آن ها راه نفوذ برای هکر ها ایجاد می شود. به عنوان مثال اسب های تروا می توانند با استفاده از درگاه های باز برای حمله کنندگان اطلاعات ارسال نمایند. برای این کار هکر به اسب تروایی که بر روی سیستم قرار دارد، از طریق درگاهی خاص، وصل شده و برای انجام وظایفی مورد نظر خود (به عنوان مثال گرفتن یک تصویر از صفحه کار کاربر) درخواست صادر می کند. اسب تروا وظیفه مورد نظر را انجام داده و تصویر را از طریق درگاه باز برای هکر ارسال می کند. در نمونه های جدید اسب تروا شماره درگاه به سادگی قابل تغییر است و بنابراین شناسایی آنها از طریق شماره درگاه ها به دشواری انجام می شود.

برای بستن درگاه ها ابزارها و روش های متنوعی وجود دارد. استفاده از حفاظ ها به عنوان یکی از رایج ترین این روش هاست. استفاده از این ابزار با توجه به هزینه های انواع مختلف آن و همینطور پیچیدگی استفاده از آن می تواند برای بعضی از کاربران مشکل آفرین باشد.

در این قسمت ضمن معرفی مفهوم درگاه روش هایی برای بستن درگاه ها به صورت دستی مورد معرفی قرار می گیرند.

درگاه چیست؟

درگاه کانالی ارتباطی است برای کامپیوترهای موجود بر روی شبکه.

برای برقراری ارتباط بین کامپیوترهای مختلف متصل به شبکه استانداردهای متنوعی تدوین شده اند. این استانداردها به روش های انتقال اطلاعات می پردازند و هدف آنها بوجود آوردن امکان تبادل اطلاعات بین سیستم های مختلف است. استاندارد TCP/IP یکی از این استانداردهاست و پروتکلی نرم افزاری برای ساختاردهی و انتقال داده بر روی شبکه (مانند اینترنت) می باشد. از مهمترین مزایای این پروتکل ها عدم وابستگی آنها به سیستم عامل کامپیوترها است و بنابراین انتقال اطلاعات بین کامپیوترهای مختلف موجود بر روی شبکه امکان پذیر می شود.

هر کامپیوتر برای ورود به دنیای اینترنت باید یک آدرس IP معتبر داشته باشد. آدرس IP ساختاری به صورت زیر دارد:

###.###.###.###

این آدرس از چهار بخش تشکیل شده است که با نقطه از هم جدا شده اند. هر بخش می تواند مقداری بین ۰ تا ۲۵۵ داشته باشد.با دانستن آدرس IP هر کامپیوتر می توان با آن ارتباط برقرار نموده و داده رد و بدل کرد. اما هنوز در مفهوم ارتباط یک نکته مبهم وجود دارد. کامپیوتر دریافت کننده اطلاعات چگونه باید بفهمد که چه برنامه ای باید داده را دریافت و پردازش کند.

برای حل این مشکل از سیستم درگاه استفاده شده است. به عبارت دیگر با مشخص کردن درگاه برای هر بسته ارسالی برنامه دریافت کننده هم مشخص می شود و به این ترتیب کامپیوتر گیرنده می تواند داده را در اختیار برنامه مربوطه قرار دهد. هر بسته ای که بر روی شبکه قرار می گیرد باید آدرسIP کامپیوتر گیرنده اطلاعات و همینطور شماره درگاه مربوطه را نیز در خود داشته باشد.

در مقام مقایسه می توان شماره درگاه را با شماره تلفن داخلی مقایسه نمود. شماره تلفن مانند آدرس IP به صورت یکتا مقصد تماس را مشخص می کند و شماره داخلی نشانگر فردی است که تماس باید با او برقرار شود.

شماره درگاه می تواند عددی بین ۰ تا ۶۵۵۳۶ باشد. این بازه به سه دسته اصلی زیر تقسیم بندی شده است:

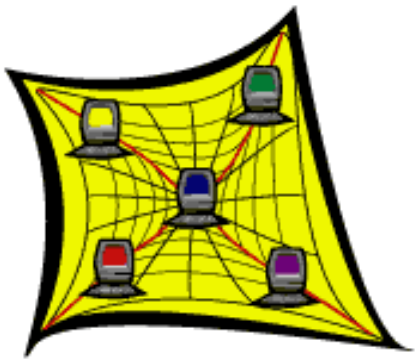
- ۰ تا ۱۰۲۳ که «درگاه های شناخته شده» هستند و برای خدماتی خاص مانند FTP (درگاه ۲۱)، SMTP (درگاه ۲۵)، HTTP (درگاه ۸۰)، POP3 (درگاه ۱۱۰) رزرو شده اند.
- درگاه های ۱۰۲۴ تا ۴۹۱۵۱ «درگاه های ثبت شده» هستند. به عبارت دیگر این درگاه ها برای خدمات، ثبت شده اند.
- درگاه های ۴۹۱۵۲ تا ۶۵۵۳۶ «درگاه های پویا و/ یا اختصاصی» هستند. به عبارت دیگر هر شخصی می تواند در صورت نیاز از آنها استفاده نماید.

راه های بستن درگاه ها بدون استفاده از حفاظ

هر درگاه باز یک ورودی بالقوه برای حمله کنندگان به سیستم هاست. بنابراین باید سیستم را به گونه ای پیکربندی نمود که حداقل تعداد درگاه های باز بر روی آن وجود داشته باشد.

در رابطه با درگاه ها باید توجه داشت که هر درگاه بازی الزاما خطرآفرین نیست. سیستم های کامپیوتری تنها در صورتی از ناحیه درگاه ها در معرض خطر قرار دارند که

برنامه مرتبط با درگاه کد خطرناکی در خود داشته باشد. بنابراین لزومی ندارد که همه درگاه ها بر روی سیستم بسته شوند. در حقیقت بدون وجود درگاه های باز امکان اتصال به اینترنت وجود ندارد.



یک درگاه باز شیء فیزیکی نیست و چنین نیست که با بسته شدن آن از بین برود. اگر درگاهی در یک کامپیوتر باز باشد به این معناست که برنامه فعالی بر روی دستگاه وجود دارد که با استفاده از این شماره درگاه با سایر کامپیوترها بر روی شبکه ارتباط برقرار می کند. در واقع درگاه توسط سیستم عامل باز نمی شود، بلکه برنامه خاصی که در انتظار دریافت داده از این درگاه است آن را باز می کند.

یکی از موثرترین روش هایی که می توان برای بستن درگاه های باز مورد استفاده قرار داد، متوقف نمودن سرویسی است که بر روی درگاه به ارتباطات گوش فرا داده است. این کار را در Windows 2000 می توان با استفاده از ابزار Control Panel > Administrative Tools > Services و متوقف نمودن سرویس هایی که مورد نیاز نیستند، انجام داد. به عنوان مثال اگر Web services در سیستم مورد نیاز نیست می توان IIS را متوقف نمود. در Unix باید فایل های /etc/rc.d را ویرایش نمود، و

یا از یکی از ابزارهایی که برای این کار در سیستم های Unix و شبیه Unix وجود دارد (مانند linuxconf) بهره گرفت.

غیر از متوقف کردن سرویس ها، می توان درگاه ها را نیز بر روی ماشین فیلتر نمود. در ویندوز این کار با استفاده از مکانیزم فیلترینگ داخلی انجام پذیر است. برای سیستم عامل ویندوز ۲۰۰۰ می توان از ابزار پیکربندی که در Control Panel > Network> Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties > Advanced > Options > TCP/IP Filtering مخفی شده است بهره گرفت. با استفاده از این گزینه می توان بسته های TCP و UDP را به گونه ای فیلتر نمود که فقط درگاه های خاصی باز باشند و بسته های اطلاعاتی سایر درگاه ها اجازه عبور نداشته باشند. علاوه بر این، در ویندوز می توان فیلترهای محلی (برای درگاه ها و یا میزبان ها) هم تعریف نمود. برای این کار باید مسیر زیر را طی نمود:

Control Panel > Administrative Tools> Local Security Policy> IP Security Policies on Local Machine> Secure Server(Require Security)> Add

علاوه بر این بیشتر حفاظ های شخصی هم قابلیت فیلتر بسته های اطلاعاتی مربوط به درگاه های خاص را دارا هستند.

در سیستم عامل های Linux و شبهUnix نیز تعداد زیادی از ابزارهای متنوع برای فیلتر کردن درگاه های ورودی وجود دارد. IPChains که به صورت پیش فرض بر روی بسیاری از نسخه های جدید Linux نصب می شود از جمله ابزارهای مناسب است.

- Open ports
- Firewall
- Internet Protocol

امضای دیجیتال

شاید تاکنون نامه های الکترونیکی متعددی را دریافت داشته اید که دارای مجموعه ای از حروف و اعداد در انتهای آنان می باشند. در اولین نگاه ممکن است اینگونه تصور گردد که اطلاعات فوق بی فایده بوده و شاید هم نشاندهنده بروز یک خطاء در سیستم باشد! در حقیقت ما شاهد استفاده از امضای دیجیتال در یک نامه الکترونیکی می باشیم. به منظور ایجاد امضای دیجیتال از یک الگوریتم ریاضی به منظور ترکیب اطلاعات در یک کلید با اطلاعات پیام، استفاده می شود. ماحصل عملیات، تولید رشته ای مشتمل بر مجموعه ای از حروف و اعداد است. یک امضای دیجیتال صرفا" به شما نخواهد گفت که " این شخص یک پیام را نوشته است" بلکه در بردارنده این مفهوم مهم است که: "این شخص این پیام را نوشته است".

علت استفاده از یک امضای دیجیتال چیست ؟

اجازه دهید برای پاسخ به سوال فوق، سوالات دیگری را مطرح کنیم!

- برای تشخیص و تائید هویت فرد ارسال کننده یک نامه الکترونیکی از چه مکانیزمهائی استفاده می شود؟
- فرض کنید یک نامه الکترونیکی را از یکی از دوستان خود دریافت داشته اید که از شما درخواست خاصی را می نماید ، پس از مطالعه پیام برای شما دو سوال متفاوت مطرح می گردد : **الف**) آیا این نامه را واقعا" وی ارسال نموده است؟ **ب**) آیا محتوای نامه ارسالی واقعی است و وی دقیقا" همین درخواست را داشته است ؟
- آیا وجود هر نامه الکترونیکی در صندوق پستی، نشاندهنده صحت محتوا وتائید هویت فرد ارسال کننده آن است؟

همانگونه که در مطلب" مراقب ضمائم نامه های الکترونیکی باشید"، اشاره گردید، سوءاستفاده از آدرس های Email برای مهاجمان و ویروس ها به امری متداول تبدیل شده است و با توجه به نحوه عملکرد آنان در برخی موارد شناسائی هویت فرد ارسال کننده یک پیام بسیار مشکل و گاها" غیرممکن است. تشخیص غیرجعلی بودن نامه های الکترونیکی در فعالیت های تجاری و بازرگانی دارای اهمیت فراوانی است.

یک نامه الکترونیکی شامل یک امضای دیجیتال، نشاندهنده این موضوع است که محتوای پیام از زمان ارسال تا زمانی که به دست شما رسیده است، تغییر نکرده است. در صورت بروز هر گونه تغییر در محتوای نامه، امـــضای دیجـــیتال همراه آن از درجه اعتبار ساقط می شود.

نحوه عملکرد یک امضای دیجیتال

قبل از آشنائی با نحوه عملکرد یک امضای دیجیتال، لازم است در ابتدا با برخی اصطلاحات مرتبط با این موضوع بیشتر آشنا شویم:

- **کلیدها (Keys)** . از کلیدها به منظور ایجاد امضاهای دیجیتال استفاده می گردد. برای هر امضای دیجیتال ، یک کلید عمومی و یک کلید خصوصی وجود دارد: **کلید خصوصی** ، بخشی از کلید است که که شما از آن به منظور امضای یک پیام استفاده می نمائید . کلید خصوصی یک رمزعبور حفاظت شده بوده و نمی بایست آن را در اختیار دیگران قرار داد. **کلید عمومی**، بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد. زمانی که کلید فوق برای یک حلقه کلید عمومی (key ring public) و یا یک شخص خاص ارسال می گردد، آنان با استفاده از آن قادر به بررسی امضای شما خواهند بود.
- **حلقه کلید (Key Ring)**، شامل کلید های عمومی است. یک حلقه کلید از کلید های عمومی افرادی که برای شما کلید مربوط به خود را ارسال نموده و یا کلیدهائی که از طریق یک سرویس دهنده کلید عمومی دریافت نموده اید، تشکیل
-

می گردد. یک سرویس دهنده کلید عمومی شامل کلید افرادی است که امکان ارسال کلیدعمومی در اختیار آنان گذاشته شده است.

- **اثرانگشت** : زمانی که یک کلید تائید می گردد، در حقیقت منحصربفرد بودن مجموعه ای از حروف و اعداد که اثرانگشت یک کلید را شامل می شوند. تائید می گردد.
- **گواهینامه های کلید** : در زمان انتخاب یک کلید از روی یک حلقه کلید، امکان مشاهده گواهینامه (مجوز) کلید وجود خواهد داشت. دراین رابطه می توان به اطلاعات متفاوتی نظیر صاحب کلید، تاریخ ایجاد و اعتبار کلید دست یافت.

نحوه ایجاد و استفاده از کلید ها :

- **تولید یک کلید** با استفاده از نرم افزارهائی نظیر PGP (اقتباس شده از کلمات Pretty Good Privacy)و یا GnuPG (اقتباس شده از کلمات GNU Privacy Guard)
- **معرفی کلید تولید شده** به سایر همکاران و افرادی که دارای کلید می باشند.
- **ارسال کلید تولید شده به یک حلقه کلید عمومی** تا سایر افراد قادر به بررسی و تائید امضای شما گردند .
- **استفاده از امضای دیجیتال در زمان ارسال نامه های الکترونیکی** . اکثر برنامه های سرویس دهنده پست الکترونیکی دارای پتانسیلی به منظور امضاء یک پیام می باشند.

بیومتریک و تجهیزات مربوطه- قسمت اول

برای صدور اجازه ورود برای یک فرد نیاز داریم وی را شناسایی و هویت وی را تایید کنیم و مورد نظر ما انجام بررسیهایی است که بصورت خودکار توسط یک سیستم صورت بگیرد.

در اصل تمام روشهای شناسایی با سه مورد زیر ارتباط دارد:

۱- آنچه که شما میدانید (یک کلمه عبور یا PIN)

۲- آنچه که شما دارید (یک کارت یا نشانه های دیگر)

۳- آنچه که شما هستید (مشخصات فیزیکی یا رفتاری)

مورد آخر به نام زیست سنجی (Biometrics) نیز شناخته میشود.

هرکدام از این موارد مزایا و معایبی دارد: کلمات عبور ممکن است حدس زده شوند یا از دست داده شوند اما به کاربر اجازه میدهند که قدرت خود را در اختیار کسی دیگر قرار دهد. بسیاری از افراد براحتی کلمات عبور را فراموش میکنند، مخصوصا اگر بندرت از آنها استفاده کنند. نشانه ها میتوانند گم یا دزدیده شوند اما میتوانند در صورت لزوم به کس دیگر منتقل یا قرض داده شوند. مشخصات فیزیکی انعطاف ندارند. برای مثال، نمیتوان آنها را از طریق خطوط تلفن به کس یا جای دیگر منتقل کرد. طراحان سیستمهای امنیتی باید این پرسش را مطرح کنند که آیا کاربران باید توانایی انتقال اختیارشان را به دیگران داشته باشند یا خیر. پاسخ این پرسش در انتخاب روش و ابزار شناسایی و تعیین هویت موثر است.

روشهای شناسایی میتوانند بصورت ترکیبی مورد استفاده قرار گیرند: یک کارت و یک کلمه عبور یا کارت و زیست سنجی معمول هستند. این ترکیب میتواند مطابق با نیازها متفاوت باشد. برای مثال، ممکن است فقط از یک کارت برای ورود به ساختمان استفاده کنیم، از یک کارت و یک PIN برای ورود به اتاق کامپیوتر، اما از یک کارت و اثرانگشت برای عملیات انتقال پول در سیستمهای کامپیوتری.

۱- (خصوصیات رفتاری و فیزیکی) Behavioral and Physiometric

بررسیهای زیست سنجی به دو گروه تقسیم میشود:

تکنیکهای *رفتاری* که طرز انجام کاری توسط کاربر را مانند امضا کردن یا بیان کردن یک عبارت میسنجند

سنجش *اعضاء* که یک خصوصیت فیزیـــکی را مانند اثرانگشت یا شکل یک دست میسنجند.

رفتار با زمان و حال شخص تغییر میکند. تکنیکهای سنجش رفتاری هنگامی به بهترین نحو عمل میکنند که مرتبا استفاده شوند، و به این ترتیب سطوح تغییرات هر فرد مورد توجه قرار گیرد. مدلهای سنجشهای رفتاری باید این تغییرات را لحاظ کنند. از طرف دیگر، سنجشهای مشخصات فیزیکی به ابزار سنجش بزرگتر و نرم افزارپیچیده تری احتیاج دارند. به عنوان مثال، آنها مجبورند موقعیت دست را با الگو تطبیق دهند.

باید میان سیستمهایی که برای تشخیص فرد طراحی شده اند (آیا یک فرد تشخیص داده شده است و اگر اینگونه است، چه کسی را؟) و آنهایی که باید فقط هویت یک فرد را تایید کنند (آیا این فرد همانی است که خودش ادعا میکند؟) تفاوت قائل شویم. عمل دوم بسیار آسانتر است و پارامترهای تایید هویت میتوانند بر پایه همان شخص تنظیم گردند. این روش حالت طبیعی برای سیستمهای کارت هوشمند است که الگوی مرجع (که template نامیده میشود) در کارت یا یک سیستم مرکزی نگه داری میشود.

یک تست زیست سنجی شامل سه مرحله است. ثبت مشخصات، اسـتفاده و بروز رسانی. کاربران با سنجشهای اولیه در سیستم ثبت نام میشوند. این عمل معمولا سه مرتبه یا بیشتر برای ثبت اطلاعات دقیقتر انجام میگیرد. مدت زمان انجام این عمل در این مرحله بیشـتر از زمانی است که سیستم برای تشخیص کاربر مورد استفاده قرار میگیرد.

وقتی که سنجش انجام گرفت هنگام استفاده، نمونه با الگوی مرجع مقایسه میشود. در اینجا تعیین سطوح مناسب تفاوت مجاز (tolerance) مخصوصا برای سنجشهای رفتاری مهم است.

بیشتر سیستمهای زیست سنجی مخصوصا آنهایی که از مشخصات رفتاری استفاده میکنند، باید برای بروز رسانی الگوی مرجع تدارک دیده شده باشند. در حالت تشخیص صدا و امضا، معمولا یک فانکشن تطبیقی استفاده میشود که با هر بار سنجش توسط سیستم، بروز رسانی الگوی مرجع انجام میگیرد. برای مشخصاتی که تغییر کندتر است، سیستم میتواند درصد تطبیق یا تعداد دفعاتی که یک شخص پذیرفته نمیشود را اعلام کند و در مواقعی که لازم است، عمل ثبت مجددا انجام گیرد. ثبت تراکنش اغلب یک ویژگی مفید است و میتواند براحتی در یک سیستم بر پایه کارت هوشمند ایجاد گردد.

یک سیستم زیست سنجی شامل موارد زیر است:

- یک *ابزار اندازه گیری*، که واسط کاربر را تشکیل میدهد. راحتی استفاده یک فاکتور مهم دیگر برای زیست سنجی است: ابزار باید مطابق با غریزه باشد و فضای کمی برای خطا ایجاد کند. و باید قابل استفاده برای دامنه وسیعی از مردم و بخصوص افراد ناتوان باشد.
- *نرم افزار عامل*، که شامل الگوریتمهای ریاضی است که پارامترهای سنجش شده را با الگوی مرجع مقایسه میکنند. جدیدترین الگوریتمها وابستگی کمی به مدلسازی آماری دارند و بیشتر بر پایه برنامه ریزی دینامیک، شبکه های عصبی و منطق فازی هستند که انعطاف پذیری را افزایش میدهد. لذا احتمال اینکه مثلا شخصی بخاطر لکه یا کثیفی جزیی پذیرفته نشود، کم است البته چنانچه بقیه الگو تطبیق دقیقی داشته باشند.
- *سخت افزار و سیستمهای بیرونی*: قابلیت استفاده، قابلیت اطمینان و هزینه سیستم اغلب حداقل به همان اندازه که به ابزار سنجش بستگی دارد، به سخت افزار بستگی دارد. بعضی سیستمها (مانند تست اثرانگشت) فی نفسه برای استفاده در سیستمهای توزیع شده مناسب هستند، در حالیکه بقیه (مانند تشخیص صدا) برای سیستمهای متمرکز مناسب هستند.

هزینه ابزار زیست سنجی بسرعت در حال کاهش است. اکنون، برای ATMها و ابزار کنترل دسترسی مخصوصی مناسب هستند. هنوز یک افت هزینه دیگری لازم است تا اینکه زیست سنجی ها در خرید و فروش های خودکار و محیط های کنترل دسترسی مورد استفاده قرار بگیرد.

۱ Behavioral (خصوصیات رفتاری)

چندین تکنیک رفتاری برای تایید هویت وجود دارد که به اختصار به اهم آنها اشاره می کنیم.

۱-۱ تایید امضا

بررسی خودکار امضاء تعمیمی از یک پروسه آشناست. در حالیکه اپراتور انسانی شکل نهایی امضاء را بررسی میکند، بیشتر شکلهای خودکار تایید امضاء، تاکید بیشتری روی حرکتهای پروسه امضا کردن دارند. سرعت نسبی که خطها کشیده میشوند و فشار وارده، سیستم را قادر میسازد که سنجشهای انجام شده را بین امضاها حتی جایی که محیط کاملا متفاوت است، مقایسه کند و بیشتر تلاشها برای جعل امضا را با شکست مواجه کند.

الگوی مرجع امضا معمولا ۱ کیلو بایت است که این حجم کم دیتا این تکنیک را برای استفاده آنلاین یا بهمراه کارت هوشمند مناسب میسازد. یک فایده جانبی بیشتر سیستمهای تایید امضا این است که با ثبت امضاء بعنوان اثبات تراکنش صورت گرفته، باعث کم شدن سیستمهای برپایه کاغذ میشود و احتیاج به مستندسازی کاغذی را مرتفع میکند.

۱-۲ الگو و دینامیک تایپ کلید

روشی که یک نفر با صفحه کلید تایپ میکند با امضا کردن تشابهاتی دارد. تایپیستهای ماهر تقریبا خیلی زود از الگوهای تایپ کردنشان تشخیص داده میشوند. پیاده سازی های فعلی بدلیل مشکلات یکسان نبودن صفحه کلیدها و تاخیرهای نرم افزار سیستم

به آزمایشگاه محدود هستند. از طرف دیگر، هزینه اضافی پایین و عملیات شفاف، این روش را به یک تکنیک بسیارجذاب برای کاربردهایی مثل محافظت کردن ازتعداد کمی از کاربرهای با الویت بالا در سیستم کامپیوتری، تبدیل میکند.

۱-۳ تشخیص صدا

سیستمهای تشخیص صدا به راحتی توسط مشتریها پذیرفته میشوند، اما متاسفانه هنوز به سطح کارایی که مورد نیاز بیشتر محیطهای تجاری هستند، نرسیده اند. استفاده از تشخیص صدا اجازه بررسی بیش از یک مورد را میدهد: سیستم میتواند تست کند که چه چیز گفته میشود بعلاوه اینکه چگونه گفته میشود. در بعضی از محیطها پیاده سازی این سیستم هزینه خیلی کمی دارد. تشخیص صدا شاخه ای از تکنولوژی پردازش صوت است که کاربردهای بسیار وسیعتری در زمینه های دیگر، بخصوص در سیستمهای تلفنی دیجیتالی و کنفرانس تصویری دارد. نکته جالب توجه اینست که مشخصاتی از صدا که توسط این سیستمها سنجیده میشود با آنهایی که یک انسان شنونده توجه میکند، تفاوت دارند، در حالیکه شخصی که با تقلید صدا میخواهد خود را جای شخص دیگر جا بزند، روی مشخصات انسانی تمرکز میکند.

بیومتریک و تجهیزات مربوطه - قسمت دوم

۲- Physiometric (خصوصیات فیزیکی)

سنجش اعضا از قدیمی ترین روشهای تشخیص هویت است که با پیشرفت تکنولوژی به تنوع آن افزوده شده است.

۲-۱ اثر انگشت

این روش قدیمی ترین روش آزمایش تشخیص هویت از راه دور است. اگرچه قبلا اثر انگشت تنها در زمینه جرم قابل بحث بود، تحقیقات در بسیاری کشورها سطحی از پذیرش را نشان میدهد که به این روش اجازه استفاده در برنامه های عمومی را می دهد. سیستمها میتوانند جزئیاتی از اثر انگشت (نقاطی مانند تقاطعها یا کناره های برجستگیها) یا کل تصویر را بگیرند. الگوهای مرجع که برای حفظ این جزئیات بکار میرود در حدود ۱۰۰ بایت هستند که در مقایسه با تصویر کاملی که از اثر انگشت با حجم ۵۰۰ تا ۱۵۰۰ بایت میباشد،بسیار کوچکتر هستند.

در برنامه های عمومی مشکلاتی در ثبات وجود دارد. بعضی کارگران و معتادان شدید به سیگار، اغلب انگشتانی دارند که تحلیل اثرانگشت آنان مشکل است. با این وجود، طرحهای بلند مدت و موفق زیادی در استفاده از اثر انگشت وجود داشته است.

در حال حاضر اثر انگشت خوانهای زیادی در دامنه وسیعی وجود دارند که به همراه بعضی کارتخوانهااستفاده میشوند. اگرچه در حال حاضر قیمت آنها چندان پایین نیست اما میزان عرضه آنان در فروشگاههای کامپیوتر عادی باعث افت سریع قیمت آنان خواهد شد.

۲-۲ هندسه دست

هندسه دست امتیاز بالایی در راحتی استفاده بدلیل بزرگ بودن کسب میکند و میتواند با استفاده از سیستم راهنما در جای ثابتی قرار بگیرد. دست توسط مجموعه ای برجستگیهای مشخص به موقعیت صحیح برای اسکن شدن هدایت میشود و تصویر توسط یک دوربین CCD گرفته میشود. الگوی مرجع میتواند از نظر حجم خیلی کوچک باشد. (محصولی که بیشترین وسعت استفاده تجاری را در حال حاضر دارد تنها از۹ بایت استفاده میکند). اگرچه تغییرات روزانه مانند کثیفی روی کارایی آن تاثیر ندارد اما سنجش میتواند بوسیله جراحت یا افزایش سن تاثیر بپذیرد و اگر الگو مرتبا نتواند بروز شود، عملیات ثبت مجدد در هر زمانی لازم است.

۲-۳ اسکن شبکیه

اسکنرهای شبکیه مشخصات الگوهای رگهای خونی روی شبکیه را با استفاده از لیزر مادون قرمز کم قدرت و دوربین میسنجند. در این روش، برای بدست آوردن یک تصویر متمرکز، چشم باید نزدیک دوربین قرار بگیرد. الگوهای مرجع بسیار کوچک هستند (۳۵ بایت در بیشتر سیستمهای تجاری معمول). تحقیقات پزشکی اخیر نشان داده است که مشخصات شبکیه برخلاف آنچه در گذشته تصور میشد، پایدار نیست و توسط بعضی بیماریها که حتی ممکن است خود شخص مطلع نباشد تغییر میکنند. بسیاری از افراد نگران قرار دادن چشم خود درتماس نزدیک با منبع نور هستند. به همین دلیل، این روش جای خود را به اسکن عنبیه داده است.

۲-۴ اسکن عنبیه

اسکنرهای عنبیه رگه‌های موجود در عنبیه چشم را می سنجند. این تکنیک بعنوان نتیجه ای از تعداد زیادی از ویژگیها، سطح بالایی از تفاوت را بوجود می آورد و نسبت به گذشت زمان پایداری بالایی دارد.

کاربر باید از فاصله ۳۰ سانتیمتری یا بیشتربرای چند ثانیه به دوربین نگاه کند. سیستم با عینک و لنزهای تماسی کاربران تطابق دارد، هرچند که سنسور باید طوری قرار بگیرد یا تغییر کند که برای کابران با قدهای متفاوت و آنهایی که روی صندلی چرخدار قرار دارند، مناسب باشد.

اسکن عنبیه از تمام مواردی که شرح آنها رفت، جدیدتر است.

سایر موارد

از نظر تئوری، هر بخش از ساختمان بدن انسان میتواند در زیست سنجی قابل استفاده قرار گیرد. اما طرحهای تجاری روی آنهایی تمرکز شده است که براحتی سنجیده میشوند و از طرف جامعه آسان تر پذیرفته میشوند. گاهی لازم است بررسی شود که سنجش

برروی یک شخص زنده انجام میشود تا یک کپی. یک روش که مستقیما از خوصیات زنده استفاده میکند اسکن سیاهرگ است. موقعیت سیاهرگ از طریق جریان خون گرم سنجیده میشود.

تشخیصهای مربوط به صورت – تکنیکی که بیشتر توسط انسانها استفاده میشود- یک زیست سنجی قابل دوام است، مخصوصا جایی که دوربینها از قبل استفاده میشوند و جایی که بررسی کلی، همه آن چیزی است که مورد نیاز است. ویژگیهای مشخص یا نقاط برجسته سنجیده برای ایجاد الگوی مرجع استفاده میشوند.

آخرین زیست سنجی مربوط به تحلیل DNA است. بهر حال، با اطمینان میتوان گفت که هنوز خیلی سال مانده است تا این روش در بررسی هویت در فروشگاههای عادی یا هنگام سوار شدن به اتوبوس مورد استفاده قرار گیرد.

زیست سنجی و کارتها

بعضی تکنیکهای شناسایی، مشخصا کلمات عبور و PINها، استثنائا برای پیاده سازی در سیستم توزیع شده مناسب شده اند. آنها کمترین حجم ذخیره سازی و پردازش را دارند، اما همچنان که دیدیم، بعنوان ابزار چندان امنی شناخته نمیشوند.

بهرحال احتیاجات فضای ذخیره سازی یک عامل محدودکننده است. بیشتر الگوهای مرجع به ۴۰ تا ۱۵۰۰ بایت برای ذخیره شدن احتیاج دارند. الگوهای مرجع کوچکتر میتوانند روی کارتهای مغناطیسی یا بارکدها ذخیره شوند. برای الگوهای بزرگتر می توان از بارکدهای دوبعدی یا هلوگرام ها استفاده کرد، اماراضی کننده ترین پاسخ در تقریبا هر جایی که ذخیره امن مورد نیاز است، استفاده از کارت هوشمند است. کارتها ابزار مناسبی برای ترکیب زیست سنجی ها هستند. اگر دو یا سه عامل زیست سنجی روی کارت ذخیره شوند، اشتباهات در عدم تایید افراد ذیحق به حداقل میرسد. یا همان کارت میتواند در محیطهای متفاوت مورد استفاده قرار گیرد: تشخیص صدا برای سیستم تلفن، اثرانگشت برای کار با کامپیوتر یا ATM ، و یک PIN برای خرید و فروش. استفاده از چنین زیست سنجیهای لایه بندی شده ای امروزه در حال آغاز در کاربردهای تجاری هستند.

BCC و ضرورت استفاده از آن

به منظور ارسال نامه های الکترونیکی از برنامه های متعددی نظیر Outlook استفاده می گردد. برای مشخص نمودن آدرس دریافت کنندگان یک Email می توان از فیلدهای To و یا CC استفاده نمود. در برخی موارد استفاده از فیلد BCC گزینه ای مناسب و در عین حال ایمن تر به منظور ارسال نامه های الکترونیکی است.

BCC چیست؟

BCC از کلمات blind carbon copy ، اقتباس شده است. با استفاده از BCC ، امکان مخفی نگه داشتن آدرس دریافت کنندگان یک Email ، فراهم می گردد. بر خلاف آدرس هائی که در فیلد To و یا CC درج و امکان مشاهده آنان توسط سایر دریافت کنندگان وجود دارد، امکان مشاهده آدرس های درج شده در فیلد BCC توسط سایر دریافت کنندگان وجود نخواهد داشت(ارسال نسخه ای از نامه به شخص ثالث بدون این که به دریافت کننده اولیه نامه اطلاعی داده شده باشد).

چرا می بایست از BCC استفاده نمود ؟

در این رابطه می توان به دلایل زیر اشاره نمود:

- **محرمانگی**: در برخی موارد لازم است که به دریافت کنندگان یک Email این امکان داده شود تا بدانند چه افراد دیگری نیز آن را دریافت داشته اند. در برخی حالات دیگر ممکن است شما قصد ارسال یک Email برای چندین
-
- دریافت کننده را دارید و نمی خواهید آنان نسبت به این موضوع آگاه گردند که نامه ارسالی توسط چه افراد دیگری نیز دریافت شده است. مثلا" زمانی که شما
-

- یک Email را به نمایندگی از سازمان و یا یک موسسه تجاری برای مشتریان خود ارسال می نمائید، صیانت از لیست مشتریان، بسیار حائز اهمیت می باشد. در صورتی که از فیلدهای To و یا CC به منظور ارسال یک Email برای دریافت کنندگان متعددی استفاده می گردد، دریافت کنندگان Email هرگونه پاسخی که به پیام ارسالی داده خواهد شد را نیز دریافت خواهند کرد(مگر این که فرستنده آنان را از لیست حذف نماید).
- **پیگیری**: در صورتی که قصد پیگیری، دستیابی و یا آرشیو نامه های الکترونیکی ارسالی بر روی یک account دیگر را داشته باشید، می توان از BCC استفاده نمود. در چنین مواردی یک نسخه از نامه های الکترونیکی ارسالی به صورت اتوماتیک به یک account دیگر و بدون اطلاع دریافت کنندگان Email ارسال می گردد.
- **رعایت حقوق دریافت کنندگان**: نامه های الکترونیکی فورووارد شده، اغلب شامل لیست های طولانی از آدرس هائی است که توسط فرستنده قبلی و با استفاده از فیلد CC، ارسال شده است. اینگونه آدرس ها عموما" فعال و معتبر بوده و خوراک مناسبی برای توزیع کنندگان نامه های الکترونیکی ناخواسته، خواهند بود. علاوه بر این، تعداد زیادی از نامه های الکترونیکی حاوی ویروس از آدرس های Email موجود در پیام هائی که شما دریافت می نمائید، استفاده نموده و اقدام به جمع آوری آدرس های فوق می نمایند. بنابراین، وجود اینگونه لیست های طولانی در پیام های فورووارد شده، تمامی آدرس های موجود در لیست را در معرض تهدید قرار خواهد داد (در صورت آلودگی پیام های دریافتی).

تعداد زیادی از استفاده کنندگان نامه های الکترونیکی، پیام های دریافتی را با استفاده از فیلد CC برای تمامی اعضاء موجود در دفترچه آدرس خود، فوروارد می نمایند. پیشنهاد می گردد، دوستان خود را تشویق نمائید در مواردی که قصد فوروارد پیام هائی را برای شما دارند از فیلد BCC، استفاده نمایند. در چنین مواردی، امکان مشاهده آدرس Email شما توسط سایر افراد کمتر می گردد. به منظور پیشگیری در مقابل اینگونه مسائل، پیشنهاد می گردد علاوه بر استفاده از BCC در صورت فوروارد نمودن پیام ها، تمامی آدرس های Email موجود در پیام، نیز حذف گردد.

چگونه می توان از BCC استفاده نمود ؟

اکثر برنامه های ارسال Email دارای گزینه ای به منظور استفاده از فیلد BCC (پائین تر از فیلد To)، می باشند. در برخی موارد، ممکن است گزینه فوق به صورت پیش فرض فعال نشده باشد و لازم است از یک گزینه دیگر به منظور فعال نمودن آن استفاده گردد. مثلا" در برنامه Outlook به منظور فعال نمودن فیلد BCC ، می توان از طریق منوی View گزینه headers All را در زمان ایجاد یک نامه الکترونیکی جدید، انتخاب نمود.

در صورتی که قصد دارید تمامی دریافت کنندگان یک Email را در فیلد BCC مشخص نمائید و برنامه ارسال کننده، اجازه ارسال یک نامه الکترونیکی بدون درج یک آدرس در فیلد To را نمی دهد، می توانید آدرس Email خود را در فیلد To درج نمائید. بدین ترتیب، علاوه بر مخفی نگه داشتن هویت سایر دریافت کنندگان، می توان از ارسال موفقیت آمیز یک پیام نیز اطمینان حاصل نمود.

مقدمه ای بر شبکه خصوصی مجازی (VPN)

VPN

شبکه خصوصی مجازی یا Virtual Private Network که به اختصار VPN نامیده می شود، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولا از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می شود. منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می شود که از نظر دو شبکه خصوصی، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می دهد. پیاده سازی VPN معمولا اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمز شده انجام می شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می ماند. VPN را می توان بسته به شیوه پیاده سازی و اهداف پیاده سازی آن به انواع مختلفی تقسیم کرد.

دسته بندی VPN براساس رمزنگاری

VPN را می توان با توجه به استفاده یا عدم استفاده از رمزنگاری به دو گروه اصلی تقسیم کرد:

۱- VPNرمزشده: VPN های رمز شده از انواع مکانیزم های رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این VPN ها، شبکه های خصوصی مجازی اجرا شده به کمک IPSec هستند.

۲- VPN رمزنشده: این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه یکدیگر ایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می شوند. (MPLS VPN) در این مواقع می توان در لایه های بالاتر از رمزنگاری مانند SSL استفاده کرد.

هر دو روش ذکر شده می توانند با توجه به سیاست امنیتی مورد نظر، امنیت مناسبی را برای مجموعه به ارمغان بیاورند، اما معمولاً VPN های رمز شده برای ایجاد VPN امن به کار می روند. سایر انواع VPN مانند MPLS VPN بستگی به امنیت و جامعیت عملیات مسیریابی دارند.

دسته بندی VPN براساس لایه پیاده سازی

VPN بر اساس لایه مدل OSI که در آن پیاده سازی شده اند نیز قابل دسته بندی هستند. این موضوع از اهمیت خاصی برخوردار است. برای مثال در VPN های رمز شده، لایه ای که در آن رمزنگاری انجام می شود در حجم ترافیک رمز شده تاثیر دارد. همچنین سطح شفافیت VPN برای کاربران آن نیز با توجه به لایه پیاده سازی مطرح می شود.

۱- VPN لایه پیوند داده: با استفاده از VPN های لایه پیوند داده می توان دو شبکه خصوصی را در لایه ۲ مدل OSI با استفاده از پروتکلهایی مانند ATM یا Frame Relay به هم متصل کرد. با وجودی که این مکانیزم راه حل مناسبی به نظر می رسد اما معمولا روش ارزنی نیست چون نیاز به یک مسیر اختصاصی لایه ۲ دارد. پروتکلهای Frame Relay و ATM مکانیزمهای رمزنگاری را تامین نمی کنند. آنها فقط به ترافیک اجازه می دهند تا بسته به آن که به کدام اتصال لایه ۲ تعلق دارد، تفکیک شود. بنابراین اگر به امنیت بیشتری نیاز دارید باید مکانیزمهای رمزنگاری مناسبی را به کار بگیرید.

۲- VPN لایه شبکه: این سری از VPN ها با استفاده از tunneling لایه ۳ و یا تکنیکهای رمزنگاری استفاده می کنند. برای مثال می توان به IPSec Tunneling و پروتکل رمزنگاری برای ایجاد VPN اشاره کرد. مثالهای دیگر پروتکلهای GRE و L2TP هستند. جالب است اشاره کنیم که L2TP در ترافیک لایه ۲ تونل می زند اما از لایه ۳ برای این کار استفاده می کند. بنابراین در VPN های لایه شبکه قرار می گیرد. این لایه برای انجام رمزنگاری نیز بسیار مناسب است. در بخشهای بعدی این گزارش به این سری از VPN ها به طور مشروح خواهیم پرداخت.

۳- VPN لایه کاربرد: این VPN ها برای کار با برنامه های کاربردی خاص ایجاد شده اند. VPN های مبتنی بر SSL از مثالهای خوب برای این نوع از VPN

هستند. SSL رمزنگاری را بین مرورگر وب و سروری که SSL را اجرا می کند، تامین می کند. SSH مثال دیگری برای این نوع از VPN ها است.

SSH به عنوان یک مکانیزم امن و رمز شده برای login به اجزای مختلف شبکه شناخته می شود. مشکل VPNها در این لایه آن است که هرچه خدمات و برنامه های جدیدی اضافه می شوند، پشتیبانی آنها در VPN نیز باید اضافه شود.

دسته بندی VPN براساس کارکرد تجاری

VPN را برای رسیدن به اهداف تجاری خاصی ایجاد می شوند. این اهداف تجاری تقسیم بندی جدیدی را برای VPN بنا می کنند.

۱- VPN اینترانتی: این سری از VPN ها دو یا چند شبکه خصوصی را در درون یک سازمان به هم متصل می کنند. این نوع از VPN زمانی معنا می کند که می خواهیم شعب یا دفاتر یک سازمان در نقاط دور دست را به مرکز آن متصل کنیم و یک شبکه امن بین آنها برقرار کنیم.

VPN اکسترانتی : این سری از VPN ها برای اتصال دو یا چند شبکه خصوصی از دو یا چند سازمان به کار می روند. از این نوع VPN معمولا برای سناریوهای B2B که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازند، استفاده می شود.

مقدمه ای بر IPSec

IP Security یا IPSec رشته ای از پروتکل هاست که برای ایجاد VPN مورد استفاده قرار می گیرند. مطابق با تعریف IETF (Internet Engineering Task Force) پروتکل IPSec به این شکل تعریف می شود:

یک پروتکل امنیتی در لایه شبکه تولید خواهد شد تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از تایید هویت، جامعیت، کنترل دسترسی و محرمانگی بپردازد.

در اکثر سناریوها مورد استفاده، IPSec به شما امکان می دهد تا یک تونل رمزشده را بین دو شبکه خصوصی ایجاد کنید. همچنین امکان تایید هویت دو سر تونل را نیز برای شما فراهم می کند. اما IPSec تنها به ترافیک مبتنی بر IP اجازه بسته بندی و رمزنگاری می دهد و درصورتی که ترافیک غیر IP نیز در شبکه وجود داشته باشد، باید از پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد.

IPSec به استاندارد de facto در صنعت برای ساخت VPN تبدیل شده است. بسیاری از فروشندگان تجهیزات شبکه، IPSec را پیاده سازی کرده اند و لذا امکان کار با انواع مختلف تجهیزات از شرکتهای مختلف، IPSec را به یک انتخاب خوب برای ساخت VPN مبدل کرده است.

انواع IPSec VPN

شیوه های مختلفی برای دسته بندی IPSec VPN وجود دارد اما از نظر طراحی، IPSec برای حل دو مسئله مورد استفاده قرار می گیرد:

۱- اتصال یکپارچه دو شبکه خصوصی و ایجاد یک شبکه مجازی خصوصی

۲- توسعه یک شبکه خصوصی برای دسترسی کاربران از راه دور به آن شبکه به عنوان بخشی از شبکه امن

بر همین اساس ، IPSec VPN ها را نیز می توان به دو دسته اصلی تقسیم کرد:

۱- پیاده سازی LAN-to-LAN IPSec

این عبارت معمولا برای توصیف یک تونل IPSec بین دو شبکه محلی به کار می رود. در این حالت دو شبکه محلی با کمک تونل IPSec و از طریق یک شبکه عمومی با هم ارتباط برقرار می کنند به گونه ای که کاربران هر شبکه محلی به منابع شبکه محلی دیگر، به عنوان عضوی از آن شبکه، دسترسی دارند. IPSec به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزنگاری شود.

۲- پیاده سازی Remote-Access Client IPSec

این نوع از VPN ها زمانی ایجاد می شوند که یک کاربر از راه دور و با استفاده از IPSec client نصب شده بر روی رایانه اش، به یک روتر IPSec یا Access server متصل می شود. معمولا این رایانه های دسترسی از راه دور به یک شبکه عمومی یا اینترنت و با کمک روش dialup یا روشهای مشابه متصل می شوند. زمانی که این رایانه به اینترنت یا شبکه عمومی متصل می شود، IPSec client موجود بر

روی آن می تواند یک تونل رمز شده را بر روی شبکه عمومی ایجاد کند که مقصد آن یک دستگاه پایانی IPSec ،مانند یک روتر، که بر لبه شبکه خصوصی مورد نظر که کاربر قصد ورود به آن را دارد، باشد.

در روش اول تعداد پایانه های IPSec محدود است اما با کمک روش دوم می توان تعداد پایانه ها را به ده ها هزار رساند که برای پیاده سازی های بزرگ مناسب است.

ساختار IPSec

IPSec برای ایجاد یک بستر امن یکپارچه، سه پروتکل را با هم ترکیب می کند:

۱- پروتکل مبادله کلید اینترنتی(Internet Key Exchange یا IKE)

این پروتکل مسئول طی کردن مشخصه های تونل IPSec بین دو طرف است.

وظایف این پروتکل عبارتند از:

- طی کردن پارامترهای پروتکل
- مبادله کلیدهای عمومی
- تایید هویت هر دو طرف
- مدیریت کلیدها پس از مبادله

IKE مشکل پیاده سازی های دستی و غیر قابل تغییر IPSec را با خودکار کردن کل پردازه مبادله کلید حل می کند. این امر یکی از نیازهای حیاتی IPSec است.

IKE خود از سه پروتکل تشکیل می شود :

- SKEME : مکانیزمی را برای استفاده از رمزنگاری کلید عمومی در جهت تایید هویت تامین می کند.
- Oakley : مکانیزم مبتنی بر حالتی را برای رسیدن به یک کلید رمزنگاری، بین دو پایانه IPSec تامین می کند.
- ISAKMP : معماری تبادل پیغام را شامل قالب بسته ها و حالت گذار تعریف می کند.

IKE به عنوان استاندارد RFC 2409 تعریف شده است. با وجودی که IKE کارایی و عملکرد خوبی را برای IPSec تامین می کند، اما بعضی کمبودها در ساختار آن باعث شده است تا پیاده سازی آن مشکل باشد، لذا سعی شده است تا تغییراتی در آن اعمال شود و استاندارد جدیدی ارائه شود که IKE v2 نام خواهد داشت.

۲- پروتکل Encapsulating Security Payload یا ESP

این پروتکل امکان رمزنگاری، تایید هویت و تامین امنیت داده را فراهم می کند.

۳- پروتکل سرآیند تایید هویت (Authentication Header یا AH)

این پروتکل برای تایید هویت و تامین امنیت داده به کار می رود.

امنیت در شبکه‌های بی‌سیم (۱)

قسمت اول : مقدمه

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه‌ها با تأکید بر ابعاد امنیتی آن‌ها، به روش‌های پیکربندی صحیح که احتمال رخ‌داد حملات را کاهش می‌دهند بپردازیم.

شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه

شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عمل‌کرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهای جیبی

برتری قابل‌توجه‌یی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد. به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند.

منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.

- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.
- اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.
- حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به‌راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن(که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.
- در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد شبکه نیز وجود دارد.

امنیت در شبکه‌های بی‌سیم (۲)

قسمت دوم : شبکه‌های محلی بی‌سیم

در این قسمت، بررسی امنیت در شبکه‌های بی‌سیم، به مرور کلی شبکه‌های محلی بی‌سیم می‌پردازیم. اطلاع از ساختار و روش عملکرد این شبکه‌ها، حتی به صورت جزءیی، برای بررسی امنیتی لازم به‌نظر می‌رسد.

پیشینه

تکنولوژی و صنعت WLAN به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌های محلی بی‌سیم به کندی صورت می‌پذیرفت. با ارایه‌ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه‌های محلی امکان‌پذیر می‌ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل‌ها و استانداردهای خانواده‌ی IEEE 802.11 است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می‌دهد:

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می‌کند. با این وجود تعداد کانال‌های قابل استفاده در نوع b در مقایسه با نوع a، بیش‌تر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می‌کند. در حالت معمول، مقصود از WLAN استاندارد 802.11b است.

استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به 802.11g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل 2.4GHz عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی‌شدن و معرفی آن نمی‌گذرد، بیش از یک‌سال است که آغاز شده و با توجه سازگاری آن با استاندارد 802.11b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

معماری شبکه‌های محلی بی‌سیم

استاندارد 802.11b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه –همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود– و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شودوبا روش‌هایی می‌توان یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS(Basic Service Set) می‌نامند. مجموعه‌ی تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS(Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

در سمت هریک از سخت‌افزارها که معمولاً مخدوم هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند.

AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :

همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یک نقطه‌ی مرکزی برای دسترسی وجود ندارد و سخت‌افزارهای همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایل – با ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خوانده می‌شوند. شکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد :

شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان خادم وجود ندارد.

در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

در قسمت بعد، به دسته‌بندی اجزای فعال یک شبکه‌ی محلی بی‌سیم پرداخته و شعاع پوشش این دسته از شبکه‌ها را مورد بررسی قرار خواهیم داد.

امنیت در شبکه‌های بی‌سیم (۳)

قسمت سوم : عناصر فعال و سطح پوشش WLAN

عناصر فعال شبکه‌های محلی بی‌سیم

در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد :

- ایستگاه بی سیم

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویشگر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.

- نقاط **دسترسی**

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

برد و سطح پوشش

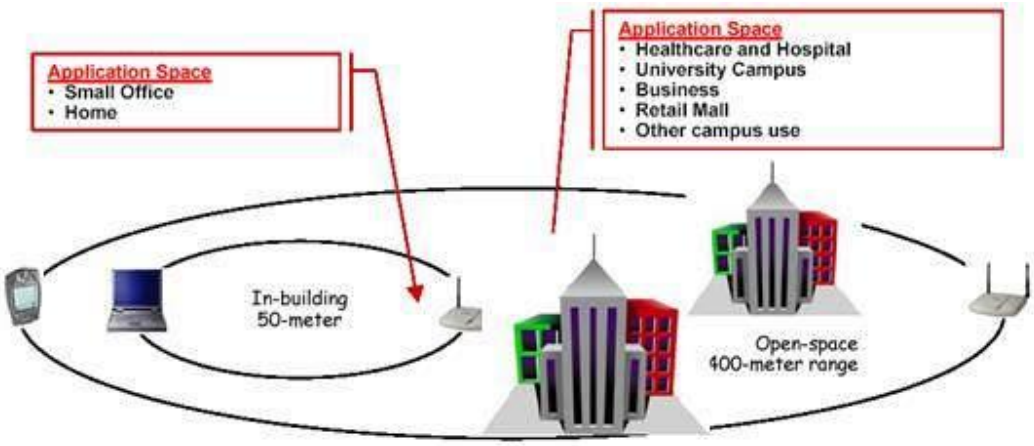
شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بستگی دارد که برخی از آن‌ها به شرح زیر هستند :

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹ متر(برای فضاهای بسته‌ی داخلی) و ۴۸۵متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرتمندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.

با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عملکرد مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :

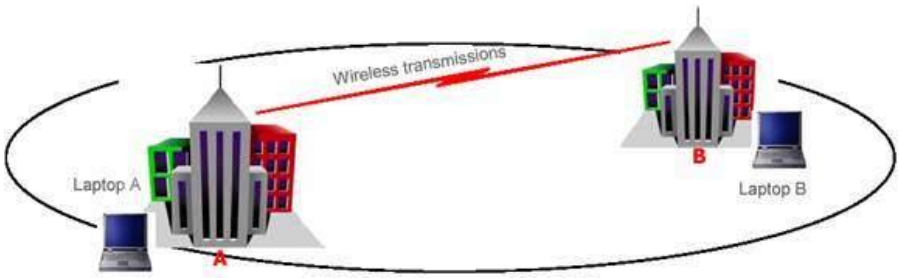


یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.

اتصال میان نقاط دسترسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد.

شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می‌دهد :



از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دسترسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

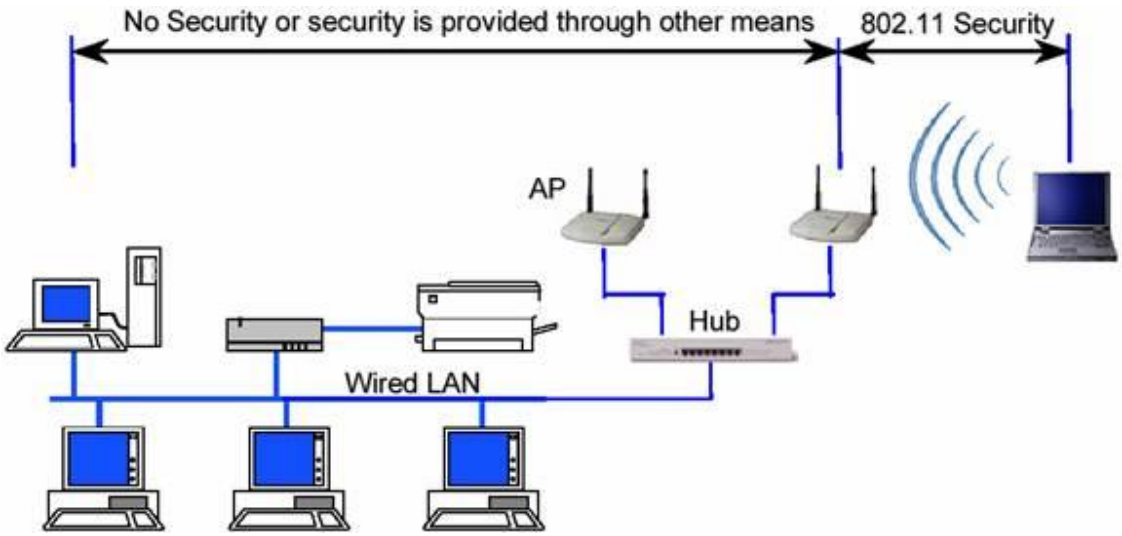
در قسمت بعد به مزایای معمول استفاده از شبکه‌های محلی بی‌سیم و ذکر مقدماتی در مورد روش‌های امن سازی این شبکه‌ها می‌پردازیم.

امنیت در شبکه‌های بی‌سیم (۴)

قسمت چهارم : امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن‌که در سه قسمت قبل به مقدمه‌یی در مورد شبکه‌های بی‌سیم محلی و عناصر آن‌ها پرداختیم، از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد.

استاندارد 802.11 سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل بالا محدوده‌ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می‌دهد.

قابلیت‌ها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سیم‌یی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد:

- **Authentication**

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دسترسی به شبکه‌ی بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

- **Confidentiality**

محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

- **Integrity**

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.

نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing و Authorization در میان سرویس‌های ارایه شده توسط این پروتکل است.

در قسمت‌های بعدی از بررسی امنیت در شبکه‌های محلی بی‌سیم به بررسی هریک از این سه سرویس می‌پردازیم.

امنیت در شبکه‌های بی‌سیم (۵)

قسمت پنجم : سرویس‌های امنیتی WEP – Authentication

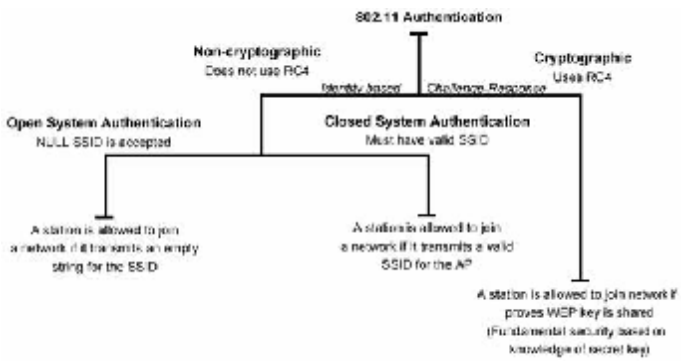
در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم.

در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

Authentication

استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد:



همان‌گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می‌کند و روش دیگر از هیچ تکنیک رمزنگاری‌یی استفاده نمی‌کند.

Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدومِ متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.

در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاهداری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

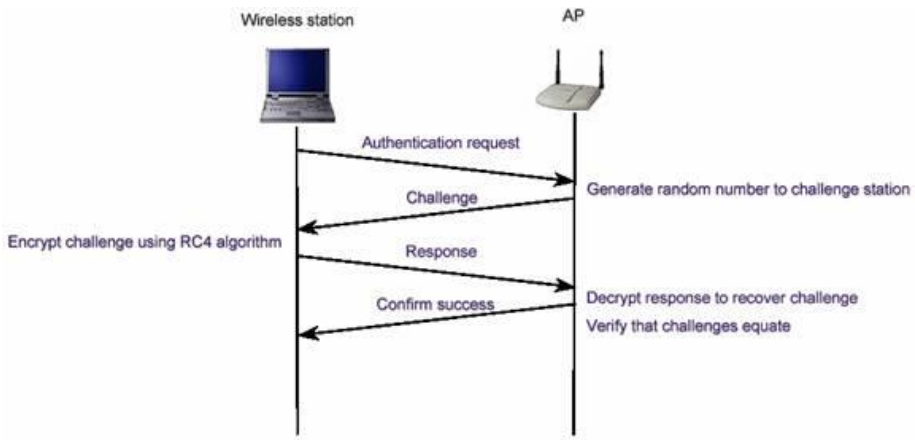
در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که با شبکه‌یی در

حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ‌دادن حملات نیز خود تضمینی ندارد!

Authentication با رمزنگاری RC4

این روش که به روش«کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد:



در این روش، نقطه‌ی دسترسی(AP) یک رشته‌ی تصادفی تولید کرده و آن را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده(که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت همسانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم

کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است:

الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هریک از دو طرف را گمراه می‌کند.

در قسمت بعد به سرویس‌های دیگر پروتکل WEP می‌پردازیم.

امنیت در شبکه‌های بی‌سیم (۶)

قسمت ششم : سرویس‌های امنیتی 802.11b – Privacy و Integrity

در قسمت قبل به سرویس اول از سرویس‌های امنیتی 802.11b پرداختیم. این قسمت به بررسی دو سرویس دیگر اختصاص دارد. سرویس اول Privacy (محرمانه‌گی) و سرویس دوم Integrity است.

Privacy

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی‌که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

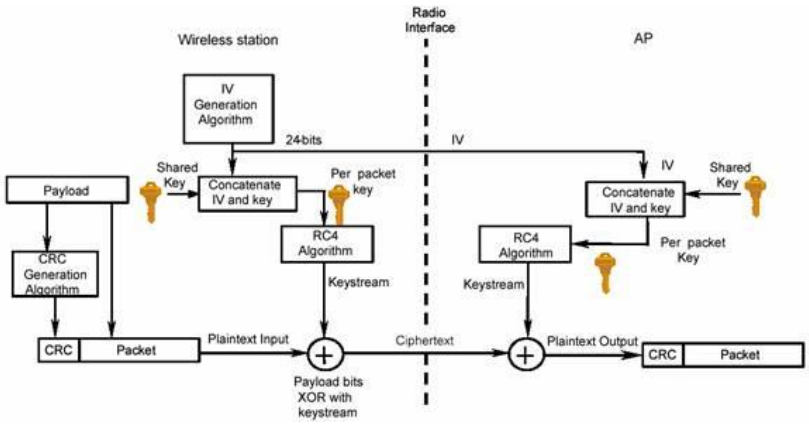
در استاندارد 802.11b، از تکنیک‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به‌بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه‌های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های

محلی بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV(مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی۸۰ بیت(که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این‌ست که روش تأمین محرمانه‌گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است:



Integrity

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.

در استاندارد 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به‌معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به‌صورت دستی پیاده‌سازی گردد. ازآنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتی با فرض تلاش برای جلوگیری از رخ‌داد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

در قسمت بعد به مشکلات و ضعف‌هایی که سرویس‌های امنیتی در استاندارد 802.11b دارند می‌پردازیم.

امنیت در شبکه‌های بی‌سیم (۷)

قسمت هفتم : ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمنِ ذکر هریک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌یی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

نکته‌یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید(تا ۱۰۴ بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دست‌یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی‌های بسیاری را برای تعیین حفره‌های امنیتی این استاندارد انجام داده‌اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی‌های انجام شده فهرستی از ضعف‌های اولیه‌ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به‌راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال‌های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

از آن‌جایی‌که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمزشده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن‌جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

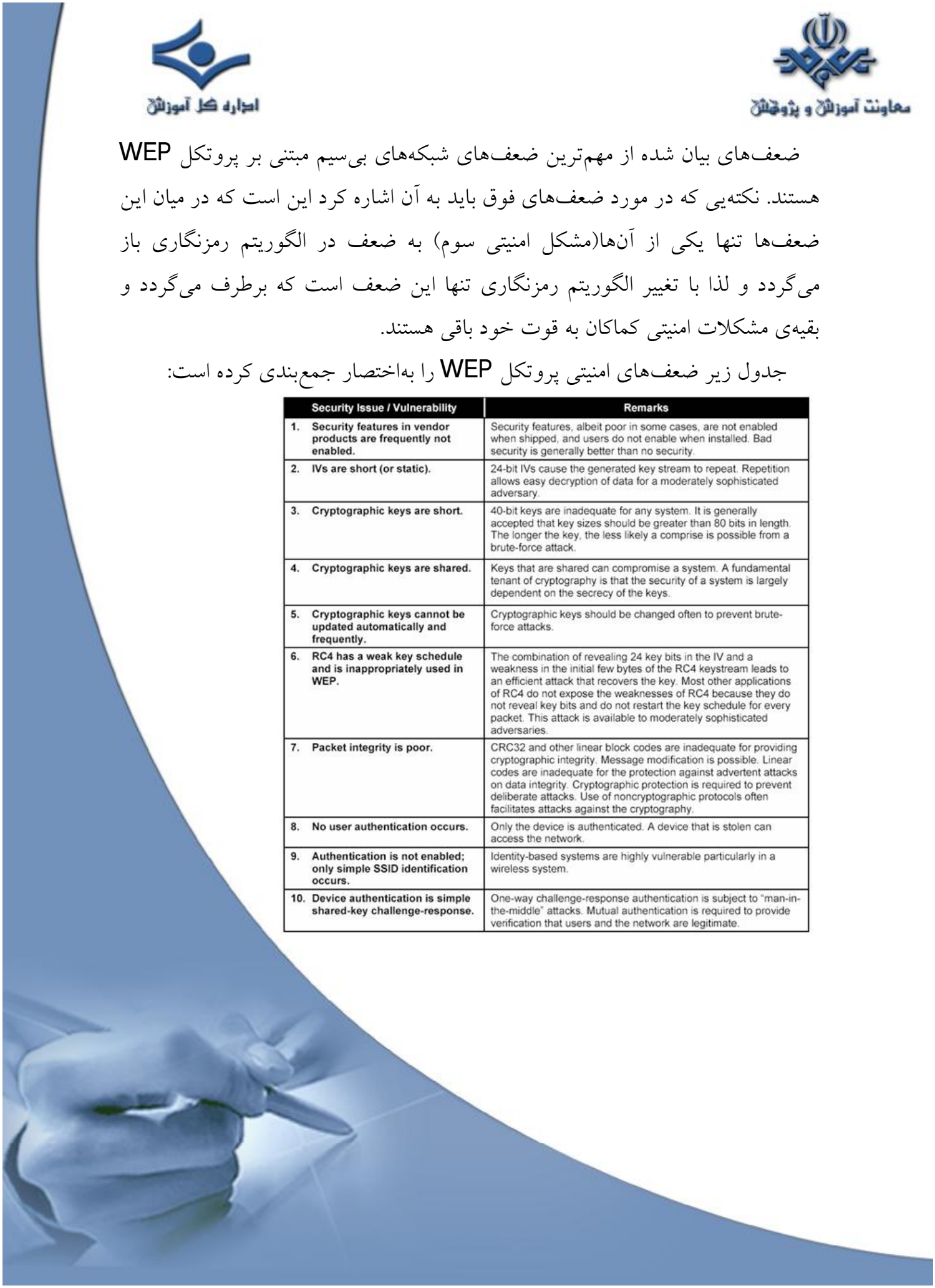
۴. استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دسترسی بی‌سیم به‌سوی گیرنده ارسال می‌شود بر اساس یک CRC رمزنشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به‌راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دسترسی بماند که آیا بسته‌ی تأیید را صادر می کند یا خیر.

ضعف‌های بیان شده از مهم‌ترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌یی که در مورد ضعف‌های فوق باید به آن اشاره کرد این است که در میان این ضعف‌ها تنها یکی از آن‌ها(مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می‌گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می‌گردد و بقیه‌ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول زیر ضعف‌های امنیتی پروتکل WEP را به‌اختصار جمع‌بندی کرده است:

Security Issue / Vulnerability	Remarks
1. **Security features in vendor products are frequently not enabled.**	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. **IVs are short (or static).**	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. **Cryptographic keys are short.**	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. **Cryptographic keys are shared.**	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. **Cryptographic keys cannot be updated automatically and frequently.**	Cryptographic keys should be changed often to prevent brute-force attacks.
6. **RC4 has a weak key schedule and is inappropriately used in WEP.**	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. **Packet integrity is poor.**	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. **No user authentication occurs.**	Only the device is authenticated. A device that is stolen can access the network.
9. **Authentication is not enabled; only simple SSID identification occurs.**	Identity-based systems are highly vulnerable particularly in a wireless system.
10. **Device authentication is simple shared-key challenge-response.**	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

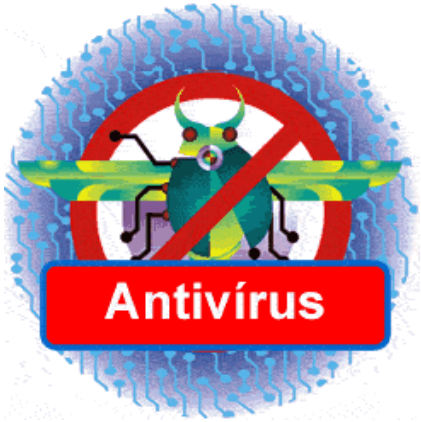


۱۰ نکته برای حفظ امنیت

هر روزه اخبار جدیدی در مورد حملات و تهدیدات کامپیوتری در رسانه های مختلف انتشار می یابد. این تهدیدات شامل ویروس های جدید و یا انواع هک و نفوذ در سیستم های کامپیوتری است. انتشار این گونه اخبار باعث شیوع اضطراب و نگرانی در بین کاربرانی می شود که به صورت مستمر از کامپیوتر بهره می گیرند و یا اطلاعاتی ارزشمند بر روی کامپیوترهای خود دارند.

۱. **استفاده از نرم افزارهای محافظتی (مانند ضدویروس ها) و به روز نگه داشتن آنها**

از وجود ضدویروس بر روی دستگاه خود اطمینان حاصل کنید. این نرم افزارها برای محافظت از کامپیوتر در برابر ویروس های شناخته شده به کارمی روند و در صورت استفاده از آنها کاربر نیاز به نگرانی در مورد ویروس ها نخواهد داشت. در شرایطی که روزانه ویروس های جدید تولید شده و توزیع می شوند، نرم افزارهای ضدویروس برای تشخیص و از بین بردن آنها باید به صورت منظم به روز شوند. برای این کار می توان به سایت شرکت تولید کننده ضدویروس مراجعه کرد و اطلاعات لازم در مورد نحوه به روز رسانی و نیز فایل های جدید را دریافت نمود. عموما نرم افزارهای ضدویروس ابزار های به روز رسانی و زمان بندی این فرایند را در خود دارند.



۲. باز نکردن نامه های دریافتی از منابع ناشناس

این قانون ساده را پیروی کنید، «اگر فرستنده نامه را نمی شناسید، نسبت به نامه و پیوست های آن بسیار با دقت عمل نمایید». هرگاه یک نامه مشکوک دریافت کردید، بهترین عمل حذف کل نامه همراه با پیوست های آن است.

برای امنیت بیشتر حتی اگر فرستنده نامه آشنا باشد هم باید با احتیاط بود. اگر عنوان نامه نا آشنا و عجیب باشد، و بالاخص در صورتی که نامه حاوی لینک های غیرمعمول باشد باید با دقت عمل کرد. ممکن است دوست شما به صورت تصادفی ویروسی را برای شما فرستاده باشد. ویروس "I Love You" دقیقا به همین صورت میلیون ها کامپیوتر را در سراسر دنیا آلوده نمود. تردید نکنید، نامه های مشکوک را پاک نمایید.

۳. استفاده از گذرواژه های مناسب

گذرواژه تنها در صورتی دسترسی غریبه ها به منابع موجود را محدود می کند که حدس زدن آن به سادگی امکان پذیر نباشد. گذرواژه های خود را در اختیار دیگران قرار ندهید و از یک گذرواژه در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت. قانون طلایی برای انتخاب گذرواژه شامل موارد زیر است:

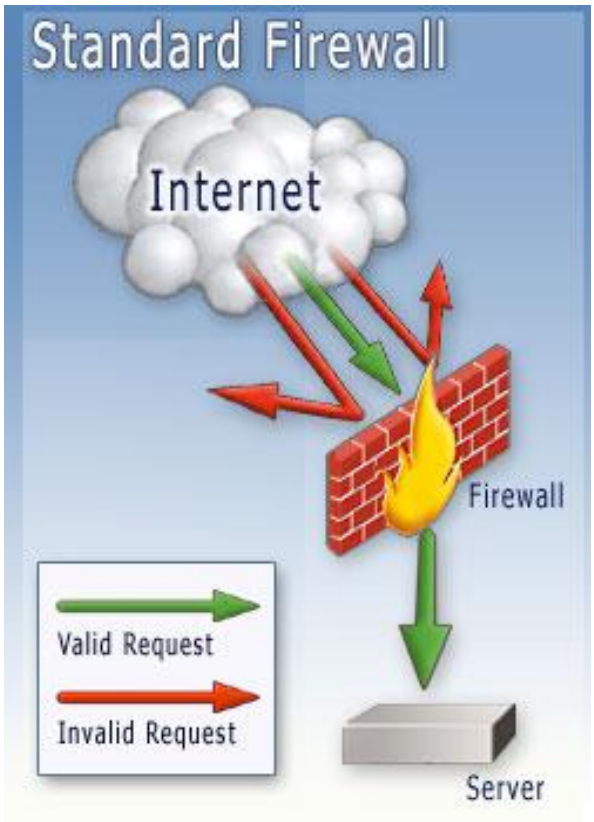
- گذرواژه باید حداقل شامل ۸ حرف بوده، حتی الامکان کلمه ای بی معنا باشد. در انتخاب این کلمه اگر از حروف کوچک، بزرگ و اعداد استفاده شود (مانند xk27D8Fy) ضریب امنیت بالا تر خواهد رفت.
- به صورت منظم گذرواژه های قبلی را عوض نمایید.
- گذرواژه خود را در اختیار دیگران قرار ندهید.

در مقاله انتخاب و محافظت از کلمات عبور نکات دقیق تری در این رابطه بیان شده است.

٤. محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظ(Firewall)

حفاظ دیواری مجازی بین سیستم کامپیوتری و دنیای بیرون ایجاد می کند. این محصول به دو صورت نرم افزاری و سخت افزاری تولید می شود و برای حفاظت کامپیوترهای شخصی و نیز شبکه ها به کار می رود. حفاظ داده های غیر مجاز و یا داده هایی که به

صورت بالقوه خطرناک می باشند را فیلتر کرده و سایر اطلاعات را عبور می دهد. علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است، مانع دسترسی افراد غیرمجاز به کامپیوتر می شود.



۵. خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه

سیستم های عامل این امکان را برای کاربران خود فراهم می آورند که با هدف به اشتراک گذاری فایل، دسترسی دیگران را از طریق شبکه و یا اینترنت به دیسک سخت محلی فراهم آورند. این قابلیت امکان انتقال ویروس از طریق شبکه را فراهم می آورد. از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک گذاشتن فایل ها به عمل نیاورد، امکان مشاهده فایل های خود را به دیگرانی که مجاز نیستند ایجاد می کند. بنابراین درصورتی که نیاز واقعی به این قابلیت ندارید، به اشتراک گذاری فایل را متوقف نمایید.

٦. قطع اتصال به اینترنت در مواقع عدم استفاده

به خاطر داشته باشید که بزرگ راه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند. قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد.

٧. تهیه پشتیبان از داده های موجود بر روی کامپیوتر

همواره برای از بین رفتن اطلاعات ذخیره شده بر روی حافظه دستگاه خود آمادگی داشته باشید. امروزه تجهیزات سخت افزاری و نرم افزاری متنوعی برای تهیه نسخه های پشتیبان توسعه یافته اند که با توجه به نوع داده و اهمیت آن می توان از آنها بهره گرفت. بسته به اهمیت داده باید سیاست گذاری های لازم انجام شود. در این فرایند تجهیزات مورد نیاز و زمان های مناسب برای تهیه پشتیبان مشخص می شوند. علاوه بر این باید همواره دیسک های Start up در دسترس داشته باشید تا در صورت وقوع اتفاقات نامطلوب بتوانید در اسرع وقت سیستم را بازیابی نمایید.

٨. گرفتن منظم وصله های امنیتی (Patches)

بیشتر شرکت های تولید کننده نرم افزار هر از چند گاهی نرم افزارهای به روز رسان و وصله های امنیتی جدیدی را برای محصولات خود ارائه می نمایند. با گذر زمان اشکالات جدید در نرم افزارهای مختلف شناسایی می شوند که امکان سوءاستفاده را برای هکرها بوجود می آورند. پس از شناسایی هر اشکالی شرکت تولید کننده محصول اقدام به نوشتن وصله های مناسب برای افزایش امنیت و از بین بردن راه های نفوذ به سیستم می کنند. این وصله ها بر روی سایت های وب شرکت ها عرضه می شود و کاربران باید برای تامین امنیت سیستم خود همواره آخرین نسخه های وصله ها را گرفته و بر روی

سیستم خود نصب کنند. برای راحتی کاربران ابزارهایی توسعه داده شده اند که به صورت اتوماتیک به سایت های شرکت های تولید کننده محصولات وصل شده، لیست آخرین وصله ها را دریافت می نمایند. سپس با بررسی سیستم موجود نقاط ضعف آن شناسایی و به کاربر اعلام می شود. به این ترتیب کاربر از وجود آخرین نسخه های به روز رسان آگاه می شود.

۹. بررسی منظم امنیت کامپیوتر

در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید. انجام این کار در هر سال حداقل دو بار توصیه می شود. بررسی پیکربندی امنیتی نرم افزارهای مختلف شامل مرورگرها و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فرایند انجام می شوند.

۱۰.حصول اطمینان از آگاهی اعضای خانواده و یا کارمندان از نحوه برخورد با کامپیوترهای آلوده

هر کسی که از کامپیوتر استفاده می کند باید اطلاعات کافی در مورد امنیت داشته باشد. چگونگی استفاده از ضدویروس ها و به روز رسانی آنها، روش گرفتن وصله های امنیتی و نصب آنها و چگونگی انتخاب گذرواژه مناسب از جمله موارد ضروری می باشد.

بخش ششم: رمزنگاری

Encryption

رمزنگاری

۱- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که بعنوان ***plaintext*** شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (که بعنوان ***ciphertext*** شناخته می‌شود) بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمزنوشته ***(cryptanalysis)*** کند. بخاطرداشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموما بعنوان scrambling شناخته می‌شود. بصورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد. البته دیتای اولیه نمی‌تواند از hashed value بازسازی شود. Hash functionها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.

یک چک تایید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

۲- الگوریتم‌ها

طراحی الگوریتمهای رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف

الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

۲-۱ سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای ۶۴بیتی دیتا توسط یک کلید تنها که معمولا ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES ۴۰بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶بیتی عموما توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته

می‌شوند. رمزنگاری DESسه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر) مطابق شکل زیر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.

الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتمهایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزینی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برای پیاده‌سازی در پردازنده‌های توان‌ـپایین مثلا در کارتهای هوشمند طراحی شد.

در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها Skipjack و مبادله کلید را که در کارتهای Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود.

برای رمزنگاری جریانی (streaming encryption) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۲-۲ سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عمومی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند. بعبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولترین سیستم نامتقارن بعنوان RSA شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی Rivest، Shamir و Adlemen است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشاندادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

- امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛
- رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن

رمزشده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Y^k \pmod r$

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزئیات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌های بایتی بخصوص روی ۸ بیتی‌ها که در کارتهای هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده می‌شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

سایر سیستمهای کلید نامتقارن شامل سیستمهای لگاریتم گسسته می‌شوند مانند Diffie-Hellman، ElGamal و سایر طرحهای چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرحها عملکردهای یک‌ـطرفه‌ای دارند که اجازه تاییدهویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین بخوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.

طولهای کلیدها برای این طرحهای جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چیپ‌کارتها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از این الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می‌رود.

کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده‌ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

۱- کلیدهای محرمانه (Secret keys)

الگوریتمهای متقارن مانند DES از کلیدهای محرمانه استفاده می‌کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می‌سازد. کارتهای هوشمند معمولا برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم **نباید در مخاطره قرار گیرد.**

۲- کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستمهای کلید نامتقارن این است که آنها اجازه می‌دهند که یک کلید (کلید اختصاصی) با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر (کلید عمومی)می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیامها فرستاده شوند یا در فهرستها لیست شوند (شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام‌رسانی الکترونیکی ITU X.۵۰۰ وجود دارد)، و از یک شخص به شخص بعدی داده شوند. مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیررسمی باشد.

محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد. کلیدهای اختصاصی نباید هرگز بصورت رمزنشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند. در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمانهای بزرگ معمولا نباید در یک کارت ذخیره شود.

۳- کلیدهای اصلی و کلیدهای مشتق‌شده (Master keys and derived keys)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می‌شوند. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق‌شده استفاده می‌شود که بعدا برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادرکننده با تعداد زیادی کارت سروکار دارد، می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق‌شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق‌شده با استفاده از tokenها که محاسبه‌گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می‌شوند. آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یک PIN وارد شده توسط کاربر و تاریخ و زمان استفاده کنند. خود token شامل الگوریتم و یک کلید اصلی است. چنینی tokenهایی اغلب برای دسترسی به سیستمهای کامپیوتری امن استفاده می‌شوند.

۴- کلیدهای رمزکننده‌کلید (Key-encrypting keys)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می‌رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمزشده منطقی بنظر می‌رسد. کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسانتر محافظت شوند تا آنهایی که ارسال می‌شوند.

اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می‌شود، مورد استفاده قرار می‌گیرد.

از مفهوم دامنه کلید (domain key) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه‌شان استفاده می‌کنیم. معمولا یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده‌کلید محلی ذخیره می‌شوند.هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب بعنوان کلید کنترل ناحیه (key zone control) شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر بصورتی که بیان گردید منتقل می‌شوند.

۵- کلیدهای نشست (Session keys)

برای محدودکردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود.

بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرفنظر است. چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است. (توضیح اینکه روشهای رمز متقارن از نامتقارن بمراتب سریعتر هستند بنابراین می‌توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد.)

شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستمهای پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

رمزنگاری اطلاعات، حفاظت از اطلاعات حساس

گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است. امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است. کاربران اینترنت در زمان استفاده از شبکه، اطلاعات حساس و مهمی را بدفعات ارسال و یا دریافت می دارند. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است. اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم، موارد متعددی را شامل می شود. برخی از اینگونه اطلاعات بشرح زیر می باشند:

- اطلاعات کارت اعتباری
- شماره های عضویت در انحمن ها
- اطلاعات خصوصی
- جزئیات اطلاعات شخصی
- اطلاعات حساس در یک سازمان
- اطلاعات مربوط به حساب های بانکی

تاکنون برای امنیت اطلاعات بر روی کامپیوتر و یا اینترنت از روش های متعددی استفاده شده است. ساده ترین روش حفاظت از اطلاعات نگهداری اطلاعات حساس بر روی محیط های ذخیره سازی قابل انتقال نظیر فلاپی دیسک ها است. متداولترین روش حفاظت اطلاعات، رمز نمودن آنها است. دستیابی به اطلاعات رمز شده برای افراد غیر

مجاز امکان پذیر نبوده و صرفا" افرادیکه دارای کلید رمز می باشند، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند.

رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمز نگاری است. استفاده از علم رمز نگاری دارای یک سابقه طولانی و تاریخی است. قبل از عصر اطلاعات، بیشترین کاربران رمزنگاری اطلاعات، دولت ها و مخصوصا" در موارد نظامی بوده است. سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می گردد. امروزه اغلب روش ها و مدل های رمزنگاری اطلاعات در رابطه با کامپیوتر بخدمت گرفته می شود. کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت.

اکثر سیستم های رمزنگاری اطلاعات در کامپیوتر به دو گروه عمده زیرتقسیم می گردند:

- رمزنگاری کلید – متقارن
- رمزنگاری کلید – عمومی

رمز نگاری کلید – متقارن

در روش فوق، هر کامپیوتر دارای یک کلید رمز (کد) بوده که از آن برای رمزنگاری یک بسته اطلاعاتی قبل از ارسال اطلاعات برروی شبکه و یا کامپیوتر دیگر،استفاده می نماید. دراین روش لازم است در ابتدا مشخص گردد که کدامیک از کامپیوترها قصد مبادله اطلاعاتی با یکدیگر را دارند، پس از مشخص شدن هر یک از کامپیوترها، در ادامه کلید رمز بر روی هر یک از سیستم ها می بایست نصب گردد. اطلاعات ارسالی توسط کامپیوترهای فرستنده با استفاده از کلید رمز، رمز نگاری شده وسپس اطلاعات رمز شده ارسال خواهند شد. پس از دریافت اطلاعات رمز شده توسط کامپیوترهای گیرنده،با استفاده از کلید رمز اقدام به بازگشائی رمز و برگرداندن اطلاعات بصورت اولیه و قابل استفاده خواهد شد. مثلا" فرض کنید پیامی را برای یکی از دوستان

خود رمز و سپس ارسال می نمائید. شما برای رمز نگاری اطلاعات از روشی استفاده نموده اید که بر اساس آن هر یک از حروف موجود در متن پیام را به دو حرف بعد از خود تبدیل کرده اید. مثلا" حروف A موجود در متن پیام به حروف C و حروف B به حروف D تبدیل می گردند.

پس از ارسال پیام رمز شده برای دوست خود، می بایست با استفاده از یک روش ایمن و مطمئن کلید رمز را نیز برای وی مشخص کرد. در صورتیکه گیرنده پیام دارای کلید رمز مناسب نباشد، قادر به رمز گشائی و استفاده از اطلاعات نخواهد بود. در چنین حالتی می بایست به دوست خود متذکر گردید که کلید رمز، " شیفت دادن هر حرف بسمت جلو و به اندازه دو واحد است". گیرنده پیام با انجام عملیات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود.

رمزنگاری کلید – عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" متعلق به کامپیوتر فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهائی که قصد برقراری ارتباط با یکدیگر را دارند، گذاشته می شود. برای رمزگشائی یک پیام رمز شده، کامپیوتر می بایست از کلید عمومی که توسط فرستنده ارائه شده، بهمراه کلید خصوصی خود استفاده نماید. یکی از متداولترین برنامه های رمزنگاری در این رابطه(**PGP**(Pretty Good Privacy است. با استفاده از PGP می توان هر چیز دلخواه را رمز نمود.

بمنظور پیاده سازی رمزنگاری کلید، عمومی در مقیاس بالا نظیر یک سرویس دهنده وب، لازم است از رویکردهای دیگری در این خصوص استفاده گردد." امضای دیجیتال" یکی از رویکردهای موجود در این زمینه است، یک امضای دیجیتالی صرفا" شامل اطلاعات محدودی بوده که اعلام می نماید، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام "امضای مجاز"، امین اطلاعات است. "امضای مجاز" بعنوان یک میانجی بین دو کامپیوتر ایفای وظیف می نماید. هویت و مجاز بودن هر یک از کامپیوترها

برای برقراری ارتباط توسط سرویس دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.

یکی از متداولترین نمونه های پیاده سازی شده از رمزنگاری کلید- عمومی، روش **SSL**(Secure Sokets Layer) است. روش فوق در ابتدا توسط "نت اسکیپ" پیاده سازی گردید. SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب بمنظور ارسال اطلاعات حساس، استفاده می گردد. SSL اخیرا" بعنوان بخشی از پروتکل **TLS**(Transport Layer Security) در نظر گرفته شده است.

در مرورگر می توان زمان استفاده از یک پروتکل ایمن نظیر TLS را با استفاده از روش های متعدد اعلام کرد. استفاده از پروتکل "https" درعوض پروتکل "http" یکی از روش های موجود است. در چنین مواردی در بخش وضعیت پنجره مرورگر یک "Padlock" نشان داده خواهد شد.

رمزنگاری کلید - عمومی، مدت زمان زیادی را صرف انجام محاسبات می نماید. بنابراین در اکثر سیستمها از ترکیب کلید عمومی و متقارن استفاده می گردد. زمانیکه دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می نمایند، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید – عمـومی، ارسال خواهد کرد. در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگاری کلید متقارن می باشند. پس از اتمام ارتباط، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد، می بایست مجددا" فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن ، ...)

مقدار Hash

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash، استوار است. مقدار فوق، بر اساس یک مقدار ورودی که دراختیار الگوریتم hashing گذاشته می گردد، ایجاد می گردد. در حقیقت مقدار hash ، فرم خلاصه شده ای از مقدار اولیه ای خود است. بدون آگاهی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید بنظر می رسد. مثال زیر نمونه ای در این زمینه را نشان می دهد:

عدد ورودی	الگوریتم	مقدار Hash
10,667	Input # x 143	1,525,381

تسخیص اینکه عدد ۱،۵۲۵،۳۸۱ (مقدار hash) از ضرب دو عدد ۱۰،٦٦۷ و ۱٤۳ بدست آمده است، کار بسیار مشکلی است. در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است، تشخیص عدد دوم کار بسیار ساده ای خواهد بود. (عدد ۱۰،٦٦۷). رمز نگاری مبتنی بر کلید عمومی بمراتب پیچیده تر از مثال فوق می باشند. مثال فوق صرفا" ایده اولیه در این خصوص را نشان می دهد. کلیدهای عمومی عموما" از الگوریتم های پیچیده و مقادیر Hash بسیار بزرگ برای رمزنگاری استفاده می نمایند. در چنین مواردی اغلب از اعداد ٤۰ و یا حتی ۱۲۸ بیتی استفاده می شود. یک عدد ۱۲۸ بیتی دارای $۲^{۱۲۸}$ حالت متفاوت است.

آیا شما معتبر هستید ؟

همانگونه که در ابتدای بخش فوق اشاره گردید، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر، در ابتدا رمز و سپس ارسال خواهند شد. کامپیوتر دوم (گیرنده)، پس از دریافت اطلاعات می بایست، اقدام به رمزگشائی آنان نماید. یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات

توسط یک منبع ایمن و مطمئن، استفاده از روش معروف" اعتبارسنجی"است. در صورتیکه اطلاعات "معتبر" باشند، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده اند. با ترکیب فرآیندهای رمزنگاری و اعتبار سنجی می توان یک محیط ایمن را ایجاد کرد.

بمنظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر روی یک کامپیوتر از روش های متعددی استفاده می شود:

- **رمز عبور** . استفاده از نام و رمز عبور برای کاربران، متداولترین روش "اعتبار سنجی" است . کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق، بررسی می گردند. در صورتیکه نام و یا رمز عبور نادرست باشند، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد.

- **کارت های عبور** . این نوع کارت ها دارای مدل های متفاوتی می باشند. کارت های دارای لایه مغناطیسی (مشابه کارت های اعتباری) و کارت های هوشمند (دارای یک تراشه کامپیوتر است) نمونه هائی از کارت های عبور می باشند.

- **امضای دیجتالی** . امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی (نظیر: نامه الکترونیکی، فایل های متنی و...) است. استاندارد امضای دیجیتالی (DSS)، بر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای دیجیتالی (DSA) ایجاد می گردد. الگوریتم فوق شامل یک کلید عمومی (شناخته شده توسط صاحب اولیه سند الکترونیکی – امضاء کننده) و یک کلید عمومی است. کلید عمومی دارای چهار بخش است. در صورتیکه هر چیزی پس از درج امضای دیجیتالی به

یک سند الکترونیکی، تغییر یابد، مقادیر مورد نظری که بر اساس آنها امضای دیجیتالی با آن مقایسه خواهد شد، نیز تغییر خواهند کرد.

سیستم های متعددی برای "اعتبار سنجی" تاکنون طراحی و عرضه شده است. اکثر سیستم های فوق از زیست سنجی برای تعیین اعتبار استفاده می نمایند. در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می گردد. برخی از روش های اعتبار سنجی مبتنی بر زیست شناسی کاربران، بشرح زیر می باشند:

- پیمایش اثر انگشت (انگشت نگاری)
- پیمایش شبکیه چشم
- پیمایش صورت
- مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است. می بایست این اطمینان بوجود آید که اطلاعات دریافت شده، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده اند. در این راستا از روش های متعددی استفاده می گردد:

- **Checksum** . یکی از قدیمی ترین روش های استفاده شده برای اطمینان از صحت ارسال اطلاعات است. Checksum، به دو صورت متفاوت محاسبه می گردد. فرض کنید Checksum یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن (صفر و یا یک) را می تواند داشته باشد. در چنین حالتی ۲۵٦ وضعیت متفاوت می تواند وجود داشته باشد. با توجه به اینکه در اولین وضعیت، تمام هشت بیت مقدار صفر را دارا خواهند بود، می تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، ۲۵۵ و یا کمتر باشد، مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، بیش از ۲۵۵ باشد، Checksum معادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵٦ تقسیم نمائیم. مثال زیر، عملکرد CheckSum را نشان می دهد.

Checksum	Total	Byte 8	Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1
127	1,151	80	179	15	244	135	54	232	212

- 1,151 / 256 = 4.496 (round to 4)
- 4 x 256 = 1,024
- 1,151 - 1,024 = 127

● CRC(Cyclic Redundancy Check). روش CRC در مفهوم مشابه روش Checksum است. روش فوق از تقسیم چند جمله ای برای مشخص کردن مقدار CRC استفاده می کند. طول CRC معمولا" ١٦ و یا ۳۲ بیت است. صحت عملکرد روش فوق بسیار بالا است. در صورتیکه صرفا" یک بیت نادرست باشد، CRC با مقدار مورد نظر مطابقت نخواهد کرد. روش های Checksum وCRC امکانات مناسبی برای پیشگیری از بروز خطای تصادفی درارسال اطلاعات می باشند، روش های فوق در رابطه با حفاظت اطلاعات و ایمن سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات، امکانات محدودتری را ارائه می نمایند. رمزنگاری متقارن و کلید عمومی، امکانات بمراتب مناسب تری در این زمینه می باشند.

بمنظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه های اختصاصی، از روش های متعدد ایمنی استفاده می گردد. ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر: تلفن، پست ایمن تر می باشد. برای تحقق امرفوق می بایست از روش های متعدد رمزنگاری و پروتکل های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه های کامپیوتری خصوصا" اینترنت استفاده کرد.

شکستن کلیدهای رمزنگاری

چه طول کلیدی در رمزنگاری مناسب است؟

امنیت هر الگوریتم مستقیماً به پیچیده بودن اصولی مربوط است که الگوریتم بر اساس آن بنا شده است. امنیت رمزنگاری بر اساس پنهان ماندن کلید است نه الگوریتم مورد استفاده. در حقیقت، با فرض اینکه که الگوریتم از قدرت کافی برخوردار است (یعنی که ضعف شناخته‌شده‌ای که بتوان برای نفوذ به الگوریتم استفاده کرد، وجود نداشته باشد) تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است.

در بیشتر انواع حمله، حمله‌کننده تمام کلیدهای ممکن را تولید و روی متن رمزشده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتمهای رمزنگاری در برابر این نوع حمله آسیب‌پذیر هستند، اما با استفاده از کلیدهای طولانی‌تر، می‌توان کار را برای حمله‌کننده مشکل‌تر کرد. هزینه امتحان کردن تمام کلیدهای ممکن با تعداد بیتهای استفاده شده در کلید بصورت نمایی اضافه می‌شود، و این در حالیست که انجام عملیات رمزنگاری و رمزگشایی بسیار کمتر افزایش می‌یابد.

الگوریتمهای متقارن

DES که یک الگوریتم کلید متقارن است معمولا از کلیدهای ۶۴ بیتی برای رمزنگاری و رمزگشایی استفاده می‌کند. الگوریتم متن اولیه را به بلوکهای ۶۴ بیتی می‌شکند و آنها را یکی‌یکی رمز می‌کند.

DES۳ الگوریتم پیشرفته‌تر است و در آن الگوریتم DES سه بار اعمال می‌شود (در مقاله رمزنگاری به آن اشاره شده است). نسخه دیگری از این الگوریتم (پایدارتر از قبلیها) از کلیدهای ۵۶بیتی و با فضای کلید موثر ۱۶۸بیت استفاده می‌کند و سه بار عملیات رمزنگاری را انجام می‌دهد.

جدول زیر زمان لازم برای یافتن کلید در الگوریتم DES را نشان میدهد.

طول کلید	تعداد کلیدهای ممکن	زمان مورد نیاز برای ۱ رمزگشایی در هر میلی‌ثانیه	زمان مورد نیاز برای ۱،۰۰۰،۰۰۰ رمزگشایی در هر میلی‌ثانیه
۳۲ بیت	$۲^{۳۲}$= ۴/۳×$۱۰^{۹}$	۳۵/۸ دقیقه = $۲^{۳۱}$میلی‌ثانیه	۲/۱۵ میلی‌ثانیه
۵۶ بیت	$۲^{۵۶}$= ۷/۲×$۱۰^{۱۶}$	۱۱۴۲ سال = $۲^{۵۵}$میلی‌ثانیه	۱۰ ساعت
۱۲۸ بیت	$۲^{۱۲۸}$= ۳/۴×$۱۰^{۳۸}$	۵/۴×$۱۰^{۲۴}$ سال = $۲^{۱۲۷}$میلی‌ثانیه	۵/۴×$۱۰^{۱۸}$ سال
۱۶۸ بیت	$۲^{۱۶۸}$= ۳/۷×$۱۰^{۵۰}$	۵/۹×$۱۰^{۳۶}$ سال = $۲^{۱۶۷}$میلی‌ثانیه	۵/۹×$۱۰^{۳۰}$ سال

ستون سوم مربوط به کامپیوترهایی است که می‌توانند در هر میلی‌ثانیه یک رمزگشایی را انجام دهند که برای کامپیوترهای امروزی توان محاسباتی معقولی محسوب می‌شود. ستون آخر برای سیستمهای بسیار بزرگ محاسباتی است بطوریکه قدرت پردازش یک میلیون برابر زیاد شده باشد. بدون در نظر گرفتن طول کلید، الگوریتمهای متقارن قوی نیز نمی‌توانند امنیت الگوریتمهای نامتقارن را داشته باشند، زیرا کلید باید بین دو طرف ارتباط مبادله شود.

الگوریتمهای نامتقارن

عموماً سیستمی امن محسوب می‌شود که هزینه شکستن آن بیشتر از ارزش دیتایی باشد که نگهداری می‌کند. اما در ذهن داشته باشید که با افزایش قدرت محاسباتی، سیستمهای رمزنگاری، آسانتر توسط روشهای سعی و خطا مورد حمله قرار خواهند گرفت.

برای مثال، طبق گزارشی از سایت RSA، تخمین زده می شود که یک کلید ۲۱۵ بیتی می تواند با هزینه ای کمتر از ۱ میلیون دلار و یک تلاش ۸ ماهه شکسته شود. RSA توصیه میکند که کلیدهای ۲۱۵ بیتی در حال حاضر امنیت کافی ایجاد نمی کنند و باید بنفع کلیدهای ۸۶۷ بیتی برای استفاده های شخصی کنار بروند! به همین ترتیب برای استفاده شرکتها کلیدهای ۱۰۲۴ بیتی و از ۲۰۴۸ بیت برای کلیدهای فوق العاده ارزشمند استفاده شود. البته پیش بینی شده است که این مقادیر تا حداقل سال ۲۰۰۴ معتبر خواهد بود. با پیشرفتهای موجود احتمالا در این زمان نیاز به افزودن بر طول کلید ها خواهد بود.

جدول زیر نشاندهنده افراد یا گروههایی است که توانایی شکستن کلیدها با طولهای متفاوت را دارند.

طول کلید	نفوذگران بالقوه
۲۵۶ بیتی	افراد عادی
۳۸۴ بیتی	گروههای تحقیق دانشگاهی و شرکتها
۵۱۲ بیتی	گروههای دولتی با تمام امکانات
۷۶۸ بیتی	امن برای کوتاه مدت
۱۰۲۴ بیتی	امن تا آینده نزدیک
۲۰۴۸	امن احتمالا تا چند ده سال!

پروتکل های انتقال فایل امن

در این قسمت برای شما بطور مختصر از پروتکل هایی خواهیم گفت که امکانFT یا (File Transfer) یا انتقال فایل را فراهم می آورند یا از بلوکهای سازنده پروتکل های ذکر شده در مقاله رمزنگاری در پروتکل های انتقال استفاده می کنند تا امکان FT امن را ایجاد کنند. درحالیکه پروتکلهای ذکر شده در مقاله مذکور سیستمهای امنیتی عمومی هستند که قابل کاربرد برای FT نیز هستند، آنچه در اینجا اشاره می شود، مشخصاً برای FT ایجاد شده اند:

AS2

AS۲ (Applicability Statement 2) گونه ای EDI (Electronic Date Exchange) یا تبادل دیتای الکترونیکی (اگرچه به قالبهای EDI محدود نشده) برای استفاده های تجاری با استفاده از HTTP است. AS2 در حقیقت بسط یافته نسخه قبلی یعنی AS1 است. AS2 چگونگی تبادل دیتای تجاری را بصورت امن و مطمئن با استفاده از HTTP بعنوان پروتکل انتقال توصیف می کند. دیتا با استفاده از انواع محتوایی MIME استاندارد که XML، EDI ، دیتای باینری و هر گونه دیتایی را که قابل توصیف در MIME باشد، پشتیبانی می کند، بسته بندی می شود. امنیت پیام (تایید هویت و محرمانگی) با استفاده از S/MIME پیاده سازی می شود. AS1 در عوض از SMTP استفاده می کند. با AS2 و استفاده از HTTP یا HTTP/S (HTTP با SSL) برای

انتقال، ارتباط بصورت زمان حقیقی ممکن می شود تا اینکه از طریق ایمیل انجام گیرد.

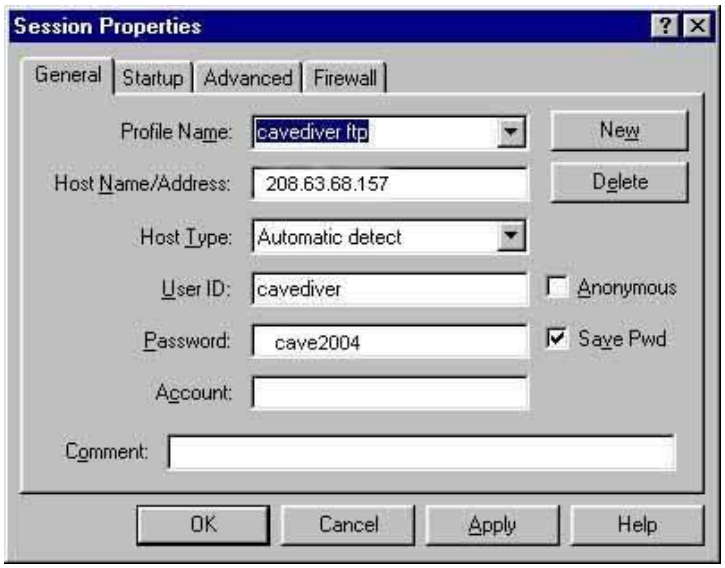
امنیت، تایید هویت، جامعیت پیام، و خصوصی بودن با استفاده از رمزنگاری و امضاهای دیجیتال تضمین می شود، که برپایه S/MIME هستند و نه SSL. استفاده از HTTP/S بجای HTTP استاندارد بدلیل امنیت ایجادشده توسط S/MIME کاملاً انتخابی است. استفاده از S/MIME اساس ویژگی دیگری یعنی انکارناپذیری را شکل می دهد، که امکان انکار پیام های ایجادشده یا فرستاده شده توسط کاربران را مشکل می سازد، یعنی یک شخص نمی تواند منکر پیامی شود که خود فرستاده است.

- برای FT :

(File Transfer

AS۲ مشخصاً برای درکنارهم قراردادن ویژگیهای امنیتی با انتقال فایل یعنی تایید هویت، رمزنگاری، انکارناپذیری توسط S/MIME و SSL انتخابی، طراحی شده است. از آنجا که AS2 یک پروتکل در حال ظهور است، سازمانها باید تولید کنندگان را به پشتیبانی سریع از آن تشویق کنند. قابلیت وجود انکارناپذیری در تراکنش های برپایه AS2 از اهمیت خاصی برای سازمانهایی برخوردار است که می خواهند پروسه های تجاری بسیار مهم را به سمت اینترنت سوق دهند. وجود قابلیت برای ثبت تراکنش پایدار و قابل اجراء برای پشتبانی از عملکردهای بسیار مهم مورد نیاز است. AS۲ از MDN (Message Disposition Notification) بر پایه RFC 2298 استفاده می کند. MDN (که می تواند در اتصال به سایر پروتکل ها نیز استفاده شود) بر اساس محتوای MIME است که قابل خواندن توسط ماشین است و قابلیت آگاه سازی و اعلام وصول

پیام را بوجود می آورد، که به این ترتیب اساس یک ردگیری نظارتی پایدار را فراهم می سازد.



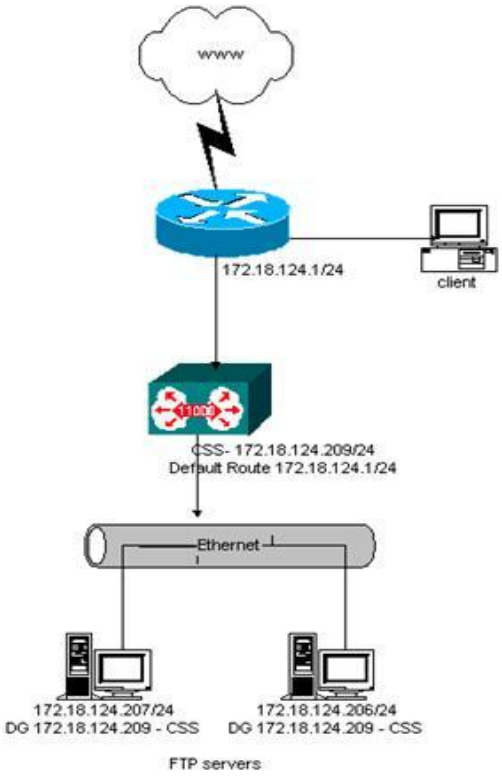
(File Transfer Protocol) **FTP**

FTP یا پروتکل انتقال فایل به منظور انتقال فایل از طریق شبکه ایجاد گشته است، اما هیچ نوع رمزنگاری را پشتیبانی نمی کند. FTP حتی کلمات عبور را نیز بصورت رمزنشده انتقال می دهد، و به این ترتیب اجازه سوءاستفاده آسان از سیستم را می دهد. بسیاری سرویس ها FTP بی نام را اجراء می کنند که حتی نیاز به کلمه عبور را نیز مرتفع می سازد (اگرچه در این صورت کلمات عبور نمی توانند شنیده یا دزدیده شوند)

- برای **FT**:

FTP بعنوان یک روش امن مورد توجه نیست، مگر اینکه درون یک کانال امن مانند SSL یا IPSec قرار گیرد.

گرایش زیادی به FTP امن یا FTP بر اساس SSL وجود دارد.
(می‌توانید به SFTP و SSL مراجعه کنید)



FTPS و SFTP

SFTP به استفاده از FT بر روی یک کانال که با SSH امن شده، اشاره دارد، در حالیکه منظور از FTPS استفاده از FT بر روی SSL است. اگرچه SFTP دارای استفاده محدودی است، FTPS (که هر دو شکل FTP روی SSL و FTP روی TLS را بخود می گیرد) نوید کارایی بیشتری را می دهد. RFC 2228 (FTPS) رمزنگاری کانالهای دیتا را که برای ارسال تمام دیتا و کلمات عبور استفاده شده اند، ممکن می سازد اما کانالهای فرمان را بدون رمزنگاری باقی می گذارد (بعنوان کانال فرمان شفاف شناخته

می شود). مزیتی که دارد این است که به فایروالهای شبکه های مداخله کننده اجازه آگاهی یافتن از برقراری نشست ها و مذاکره پورتها را می دهد. این امر به فایروال امکان تخصیص پورت پویا را می دهد، بنابراین امکان ارتباطات رمزشده فراهم می شود بدون اینکه نیاز به این باشد که تعداد زیادی از شکاف های دائمی در فایروال پیکربندی شوند.

اگرچه معمول ترین کاربردهای FTP (مخصوصاً بسته های نرم افزاری کلاینت) هنوز کاملاً FTPS (FTP روی SSL) را پشتیبانی نمی کنند و پشتیبانی مرورگر برای SSL، برای استفاده کامل از مجموعه کامل فانکشن های RFC 2228 FTPS کافی نیست، اما این امر در حال پیشرفت است. بسیاری از تولیدکنندگان برنامه های کاربردی در حال استفاده از SSL استاندارد در کنار FTP استاندارد هستند. بنابراین، گرچه در بعضی موارد مسائل تعامل همچنان وجود دارند، اما امیدواری برای پشتیبانی گسترده از FT امن در ترکیب با SSL وجود دارد. (و حتی امیدواری برای پذیرش گسترده مجموعه کامل فانکشن های RFC 2228 FTPS)

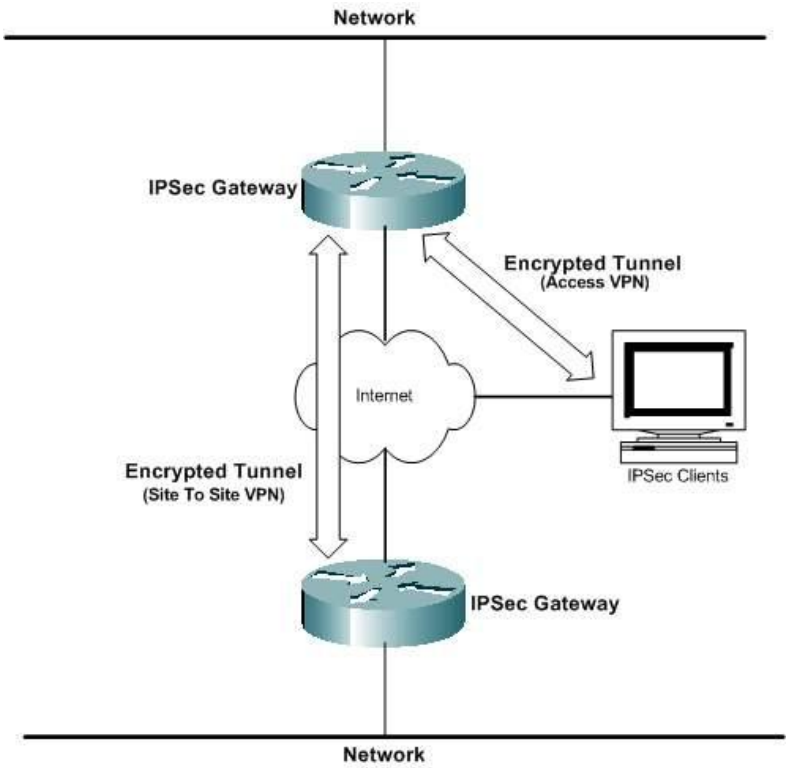
رمزنگاری در پروتکل‌های انتقال

تمرکز بیشتر روش‌های امنیت انتقال فایل بر اساس رمزنگاری دیتا در طول انتقال از طریق شبکه‌های عمومی مانند اینترنت است. دیتایی که در حال انتقال بین سازمانهاست بوضوح در معرض خطر ربوده شدن در هر کدام از محلها قرار دارد. – مثلا در شبکه‌های محلی برای هر یک از طرفین یا مرزهای Internet-LAN که سرویس‌دهندگان‌اینترنت از طریق آنها مسیر دیتا را تا مقصد نهایی مشخص می‌کنند. حساسیت دیتا ممکن است بسیار متغییر باشد، زیرا دیتای انتقالی ممکن است بهر شکلی از رکوردهای مالی بسته‌بندی شده تا تراکنش‌های مستقیم باشند. در بعضی موارد، ممکن است علاوه بر محافظت دیتا روی اینترنت، نیاز به محافظت دیتا روی LAN نیز باشد. مشخصاً، محافظت از دیتا در مقابل حملات LAN مستلزم رمزنگاری دیتای انتقالی روی خود LAN است. به این ترتیب، بهرحال، نیاز به بسط امنیت تا برنامه‌هایی است که خود دیتا را تولید و مدیریت می‌کنند، و تنها اطمینان به راه‌حلهای محیطی کفایت نمی‌کند و به این ترتیب بر پیچیدگی مسأله امنیت افزوده می‌شود.

پروتکل‌ها

اگرچه ثابت‌شده است که رمزنگاری راه‌حل بدیهی مسائل محرمانگی است، اما سردرگمی در مورد دو نوع رمزنگاری (برنامه در مقابل شبکه) همچنان وجود دارد و بدلیل وجود پروتکلهای ارتباطی گوناگون است که نیازهای تعامل بیشتر آشکار می‌شود. (مانند IPSec ، S/MIME، SSL و TLS) اگرچه این پروتکلها قول تعامل را می‌دهند،

اما تعامل کامل بدلیل مستقل بودن محصولات پروتکلها در حال حاضر وجود ندارد. آزمایشهایی در حال حاضر در حال انجام هستند که به حل شدن این مسائل کمک می‌کنند، اما کاربران باید مطمئن شوند که تعامل بین محصول انتخابیشان و محصولات سایر شرکای تجاری امری تثبیت شده است. پروتکل‌های ساده‌تر (SSL/TLS، IPSec و تا حدی پایین‌تر S/MIME) عموماً مسائل کمتری از نظر تعامل دارند.



پروتکل‌های رمزنگاری انتقال

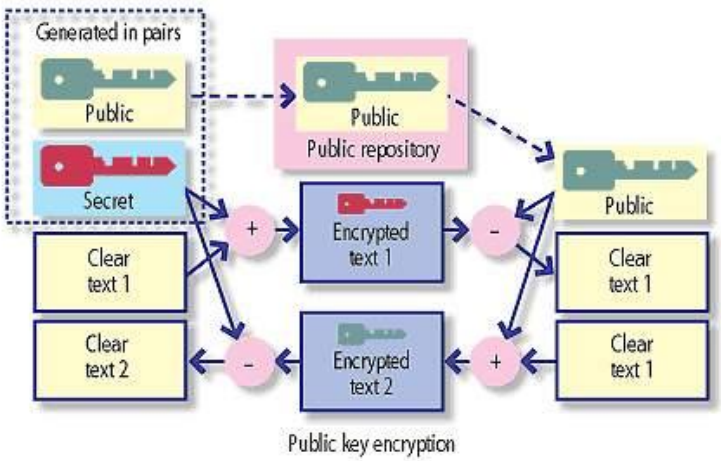
با ترکیب توانایی‌ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه‌های امنیت را فراهم می‌کنند. تقریباً تمام پروتکلها نیازهای جامعیت را پشتیبانی می‌کنند به طوری که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آنها از Non-Repudiation پشتیبانی نمی‌کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند می‌دهند، ندارند.

به این چند پروتکل به طور مختصر اشاره می‌شود:

SSL

تکنولوژی SSL (Secure Socket Layer) اساس World Wide Web امن را تشکیل می‌دهد. SSL که در مرورگرهای وب کاملاً جاافتاده است، توسط بسیاری از سازمانها برای رمزنگاری تراکنش‌های وبی خود و انتقال فایل استفاده می‌شود. بعلاوه SSL بصورت روزافزون بعنوان یک مکانیسم امنیت در تلاقی با پروتکلهای پرشمار دیگر استفاده می‌شود و بهمین ترتیب ابزاری برای ارتباط سروربه‌سرور امن است. SSL ارتباطات رمزشده و بشکل آغازین خود تایید هویت سرور از طریق استفاده از گواهی را (در حالت کلاینت‌به‌سرور) پشتیبانی می‌کند. کاربران اغلب برای استفاده از برنامه‌ها از طریق کلمه عبور تایید هویت می‌شوند، و با پیشرفت SSL استاندارد (مثلا SSL V.3.0) تایید هویت کلاینت از طریق گواهی به این پروتکل اضافه شده است.

- **برای FT (انتقال فایل)**: ابزار FT اغلب از SSL برای انتقال فایل در یکی از دو حالت استفاده می‌کنند. اولی، مد کلاینت‌به‌سرور است که کاربر را قادر می‌سازد، در حالیکه در حال استفاده از یک مرورگر وب استاندارد است مستندات را از یک سرور دریافت یا آنها را به سرور منتقل کند. که این قابلیت نیاز به نرم‌افزار مختص انتقال در کلاینت را برطرف می‌سازد و بسیار راحت است، اما اغلب فاقد بعضی ویژگیهای پیشرفته مانند نقاط آغاز مجدد و انتقالهای زمانبندی‌شده است که سازمانها نیاز دارند. SSL همچنین می‌تواند برای اتصالات سروربه‌سرور امن – برای مثال، در اتصال با FTP و سایر پروتکلها – مورد استفاده قرار گیرد.



TLS

TLS (Transport Layer Security)، جانشین SSL، برپایه SSL3.0 بنا شده است، اما به کاربران یک انتخاب کلید عمومی و الگوریتمهای Hashing می‌دهد. (الگوریتمهای Hashing فانکشن‌های یک‌طرفه‌ای برای حفظ جامعیت پیامها هستند و توسط بیشتر پروتکلها استفاده می‌شوند.) اگرچه TLS و SSL تعامل ندارند، اما چنانچه یکی از طرفین ارتباط TLSرا پشتیبانی نکند، ارتباط با پروتکل SSL3.0 برقرار خواهد شد. بیشتر مزایا و معایب SSL به TLS هم منتقل می‌شود، و معمولا وجه تمایز خاصی وجود ندارد، و از همه نسخه‌ها به عنوان SSL یاد می‌شود.

S/MIME

S/MIME (Secure Multipurpose Internet Mail Extention) که اختصاصاً برای پیام‌رسانی ذخیره- و- ارسال طراحی شده است، بعنوان استاندارد امنیت ایمیل برتر شناخته شده است. مانند بیشتر پروتکل‌های رمزنگاری (مثلا SSL ، TLS و IPSec)، S/MIME با رمزنگاری تنها سروکار ندارد. بهرحال، علاوه بر تصدیق هویت کاربران و ایمن‌سازی جامعیت پیامها (برای مثال مانند آنچه SSL انجام می‌دهد)، S/MIME توسط امضای دیجیتال، رکوردهای پایداری از صحت پیامها ایجاد می‌کند (ضمانت هویت فرستنده چنانچه به محتوای پیام مشخصی مرتبط شده). این عمل باعث می‌شود فرستنده پیام نتواند ارسال آن‌را انکار کند.

- برای FT :

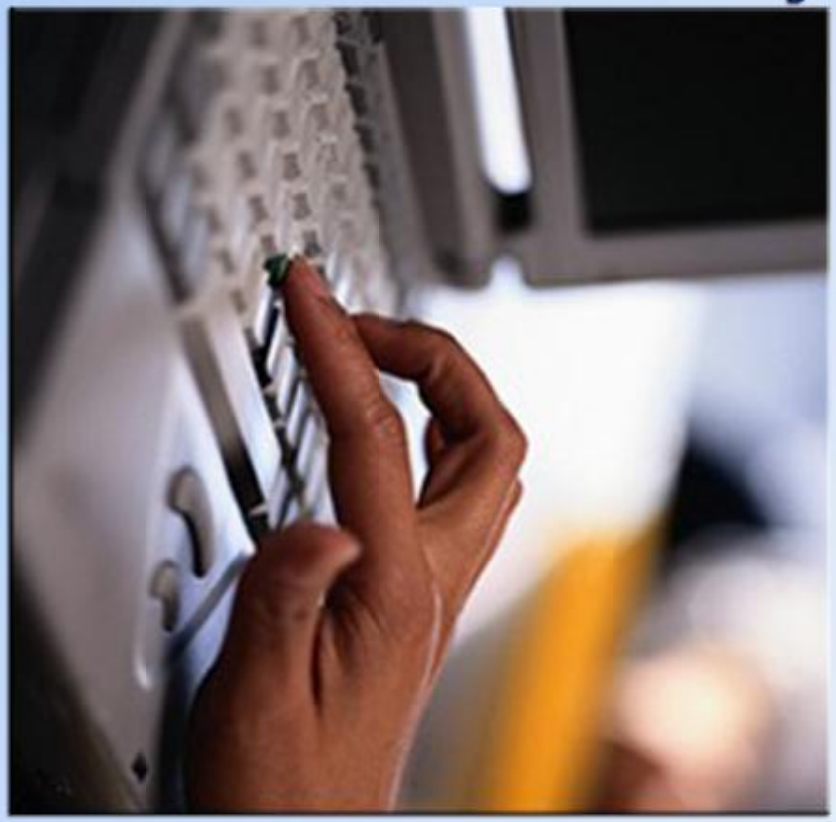
سیستم‌های ایمیل رمزشده (با استفاده از S/MIME) می‌توانند برای ارسال فایل‌های کوچک استفاده شوند (محدودیت حجم فایل بخاطر داشتن محدودیت حجم فایل در بیشتر سرورهای ایمیل است)، ولی S/MIME کلاً می‌تواند برای انتقال فایل‌های بزرگتر توسط پروتکلهای انتقال فایل استفاده شود.

SSH

SSH (Secure Shell) هم یک برنامه و یک پروتکل شبکه بمنظور وارد شدن و اجرای فرمانهایی در یک کامپیوتر دیگر است. به این منظور ایجاد شد تا یک جایگزین رمزشده امن برای دسترسی‌های ناامن به کامپیوترهای دیگر مثلا rlogin یا telnet باشد. نسخه بعدی این پروتکل تحت نام SSH2 با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک‌های SSH منتشر شد.

SSH می تواند برای پشتیبانی انتقال فایل رمزشده (به شکل SFTP) استفاده شود اما طبیعت خط فرمان بودن آن به این معنی است که بیشتر توسط مدیران سیستمها برای ارسال درون سازمان استفاده می‌شود تا برای انتقال فایل تجاری. بعلاوه استفاده از SSH نیاز به نرم‌افزار یا سیستم عاملهای سازگار با SSH در دو طرف اتصال دارد، که به این ترتیب SSH برای سروربه سرور انجام می‌گیرد.

Internet Security



حفاظت کامپیوتر قبل از اتصال به اینترنت (۱)

تعداد بسیار زیادی از کاربران اینترنت را افرادی تشکیل می دهند که فاقد مهارت های خاصی در زمینه فن آوری اطلاعات بوده و از امکانات حمایتی مناسبی نیز برخوردار نمی باشند. سیستم های اینگونه کاربران دارای استعداد لازم به منظور انواع تهاجمات بوده و بطور غیر مستقیم شرایط مناسبی را برای مهاجمان به منظور نیل به اهداف مخرب آنان، فراهم می نمایند. بر اساس گزارشات متعددی که در چندین ماه اخیر منتشر شده است، تعداد حملات و آسیب پذیری اینگونه سیستم ها، بطرز کاملا" محسوسی افزایش یافته است. علت این امر را می توان در موارد زیر جستجو نمود:

- تعداد بسیاری از تنظیمات پیش فرض کامپیوترها ، غیر ایمن می باشد.
- کشف نقاط آسیب پذیر جدید در فاصله بین زمانی که کامپیوتر تولید و پیکربندی می گردد و تنظیماتی که اولین مرتبه توسط کاربر انجام می شود.
- در مواردی که ارتقاء یک نرم افزار از طریق رسانه های ذخیره سازی نظیر CD و یا DVD انجام می شود، همواره این احتمال وجود خواهد داشت که ممکن است نقاط آسیب پذیر جدیدی نسبت به زمانی که نرم افزار بر روی رسانه مورد نظر مستقر شده است، کشف شده باشد.
- مهاجمان دارای آگاهی لازم در خصوص دامنه های آدرس های IP از نوع Dial-up و یا Broadband بوده و آنان را بطور مرتب پویش می نمایند.
- کرم های بسیار زیادی بطور مرتب و پیوسته بر روی اینترنت در حال فعالیت بوده تا کامپیوترهای آسیب پذیر را شناسائی نمایند.

با توجه به موارد فوق، متوسط زمان لازم به منظور یافتن کامپیوترهای آسیب پذیر در برخی شبکه های کامپیوتر به مرز دقیقه رسیده است.

توصیه های استاندارد به کاربران خانگی، Download و نصب Patch های نرم افزاری در اسرع وقت و پس از اتصال یک کامپیوتر جدید بر روی اینترنت است. فرآیند فوق ، با توجه به این که مهاجمان به صورت دائم اقدام به پویش و یافتن قربانیان خود می نمایند، ممکن است در موارد متعددی توام با موفقیت کامل نگردد.

به منظور حفاظت کامپیوترها قبل از اتصال به اینترنت و نصب هر یک از Patch های مورد نیاز، موارد زیر پیشنهاد می گردد:

- **در صورت امکان، کامپیوتر جدید را از طریق یک فایروال شبکه ای (مبتنیظبر سخت افزار) و یا روتر فایروال به شبکه متصل نمائید.**

یک فایروال شبکه ای و یا روتر فایروال، سخت افزاری است که کاربران می توانند آن را بین کامپیوترهای موجود در یک شبکه و دستگاههای Broadband نظیر مودم کابلی و یا DSL نصب نمایند . با بلاک نمودن امکان دستیابی به کامپیوترهای موجود بر روی یک شبکه محلی از طریق اینترنت، یک فایروال سخت افزاری قادر به ارائه یک سطح حفاظتی مناسب برای کاربران در خصوص دریافت و نصب patch های نرم افزاری ضروری خواهد بود. در صورتی که قصد اتصال کامپیوتر خود به اینترنت را از طریق یک فایروال و یا روتری با پتانسیل NAT:Networirk Address Translation، داشته باشید و یکی از موارد زیر درست باشد: الف) ماشین جدید تنها کامپیوتر متصل شده به شبکه محلی از طریق فایروال است. ب) سایر ماشین های متصل شده به شبکه محلی پشت فایروال نسبت به نصب patch های مورد نیاز بهنگام بوده و بر روی آنان کرم ها و یا ویروس هائی وجود ندشته باشد، ممکن است به وجود یک فایروال نرم افزاری نیاز نباشد.

- **در صورت امکان، از فایروال نرم افزاری همراه کامپیوتر نیز استفاده نمائید.**

در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده می باشد، پیشنهاد می گردد آن را فعال نموده تا امکان اتصال سایرین به شما وجود نداشته باشد. همانگونه که اشاره گردید، در صورتی که کامپیوتر شما از طریق یک فایروال به شبکه متصل است و تمامی کامپیوترهای موجود در شبکه محلی نسبت به نصب هر یک از Patch های مورد نیاز بهنگام شده می باشند، این مرحله می تواند اختیاری باشد .علیرغم موضوع فوق، در بخشی از استراتژی "دفاع در عمق" به این موضوع اشاره شده است که بهتر است فایروال نرم افزاری ارائه شده همراه سیستم عامل،همواره فعال گردد. در صورتی که سیستم عامل موجود برروی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده نمی باشد، می توان یک نرم افزار فایروال مناسب را تهیه نمود. پیشنهاد می گردد که اینگونه نرم افزارها از طریق رسانه های ذخیره سازی نظیر CD و یا DVD نصب گردند (در مقابل اتصال به یک شبکه و دریافت نرم افزار مورد نیاز از یک کامپیوتر حفاظت نشده). در غیر اینصورت همواره این احتمال وجود خواهد داشت که کامـــپیوتر شما قبل از اینکه قادر به دریافت و نصب اینچنین نرم افزارهائی گردد، مورد تهاجم واقع شود.

- **غیر فعال نمودن سرویس های غیرضروری نظیر "اشتراک فایل و چاپگر"**

اکثر سیستم های عامل به صورت پیش فرض پتانسیل "اشتراک فایل و چاپ " را فعال نمی نمایند. در صورتی که شما سیستم خود را به یک سیستم عامل جدید ارتقاء داده اید و کامپیوتر دارای گزینه فعال "اشتراک فایل و چاپ" می باشد، بدیهی است که سیستم عامل جدید نیز این گزینه را فعال نماید. سیستم عامل جدید ممکن است دارای نقاط آسیب پذیری باشد که شما آنان را در نسخه قبلی سیستم عامل مربوطه از طریق نصب تمامی patchهای مورد نیاز، برطرف کرده

- باشید و در سیستم عامل جدید این وضعیت وجود ندارد. برای حل مشکل فوق پیشنهاد می گردد قبل از ارتقاء سیستم عامل، پتانسیل "اشتراک فایل و چاپ " را غیر فعال نموده و در ادامه فرآیند ارتقاء را انجام دهید. پس از ارتقاء سیستم و نصب Patch های مورد نیاز، می توان در صورت ضرورت اقدام به فعال نمودن پتانسیل "اشتراک فایل و چاپ" نمود.
- **دریافت و نصب patch های مورد نیاز**

پس از ایمن سازی کامپیوتر در مقابل حملات با استفاده از فایروال های سخت افزاری و یا نرم افزاری و غیر فعال نمودن پتانسیل "اشتراک فایل و چاپ "، می توان با اطمینان بیشتری سیستم خود را به منظور دریافت و نصب patch های مورد نیاز به شبکه متصل نمود. به منظور دریافت patch های نرم افزاری، توصیه می گردد که حتما" از سایت های ایمن و مطمئن (وب سایت تولید کنندگان) استفاده گردد . بدین ترتیب احتمال این که یک مهاجم قادر به دستیابی سیستم شما از طریق برنامه هائی موسوم به Trojan گردد، کاهش می یابد.

حفاظت کامپیوتر قبل از اتصال به اینترنت (۲)

در این مطلب چندین راهنمایی برای اتصال یک کامپیوتر جدید (یا ارتقاء یافته) برای اولین بار به اینترنت آورده شده است و مخاطبان آن کاربران خانگی، دانشجویان، شرکت های تجاری کوچک، یا هر مکانی با اتصال پرسرعت (مودم کابلی، DSL) یا از طریق خط تلفن است.

انگیزه

این مطلب بدلیل ریسک فزاینده برای کاربران اینترنتِ بدون حمایت مختص IT است.

در ماه های اخیر، جهان شاهد گرایش به سمت سوءاستفاده از کامپیوترهای جدید یا محافظت نشده بوده است. این جریان بدلیل بعضی دلایل تشدید می شود:

بسیاری از پیکربندی های پیش فرض کامپیوترها نا امن هستند.

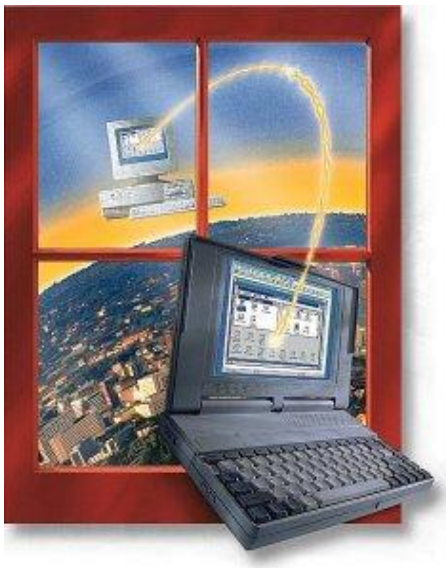
شکاف های امنیتی تازه ای ممکن است در مدت زمان ساخت و پیکربندی کامپیوتر توسط سازنده و تنظیم کامپیوتر برای اولین بار توسط کاربر، کشف شده باشد.

هنگام ارتقا نرم افزار از طریق ابزار مرسوم (مانند CD-ROM و DVD-ROM) شکافهای امنیتی جدید ممکن است از زمان ساخت دیسک تا کنون کشف شده باشد.

حمله کنندگان دامنه آدرس های IP خطوط پرسرعت و dial-up را می دانند و بطورمنظم پیمایش می کنند.

تعداد زیادی از کرمها از قبل در حال چرخیدن در اینترنت هستند و بطور پیوسته کامپیوترهای جدید را بمنظور سوءاستفاده پیمایش می کنند.

جالب است که زمان میانگین برای حمله به کامپیوترها در بعضی شبکه ها برای کامپیوترهای محافظت نشده بر حسب دقیقه اندازه گیری می شود، مخصوصاً این موضوع برای محدوده آدرس های استفاده شده توسط مودم های کابلی، DSL و dial-up صحت دارد.



توصیه ها

ادامه این مطلب به دوقسمت اختصاص دارد، اول راهنمایی عمومی و بعد گام های مختص به سیستم های عامل مشخص.

راهنمایی عمومی

هدف این مطلب فراهم آوردن حفاظت کافی برای یک کامپیوتر جدید است تا یک کاربر بتواند هر وصله نرم افزاری را که از زمان ساخت کامپیوتر یا نصب نرم افزار اولیه از

طریق CD، منتشر شده است، دانلود و نصب کند. توجه کنید که این مراحل راهنمایی کاملی برای نگه داری امن یک کامپیوتر از زمان دانلود اولیه و نصب وصله ها نیستند، بلکه قدم های اولیه و اساسی هستند.

تذکر:

- توصیه می شود که این مراحل را هنگام ارتقاء به سیستم عامل جدید و همچنین اولین اتصال یک کامپیوتر جدید به اینترنت انجام دهید.
- این مراحل را قبل از اولین اتصال به اینترنت انجام دهید.

اینها مراحلی هستند که توصیه می شوند:

۱- اگر ممکن است، کامپیوتر جدید را از طریق یک فایروال شبکه یا روتر- فایروال به اینترنت متصل کنید.

فایروال شبکه یا روتر- فایروال سخت افزاری است که کاربران می توانند بین کامپیوترها روی LAN و وسیله پرسرعت اتصال به اینترنت (مودم کابلی یا DSL) نصب کنند. با مسدود کردن دسترسی به کامپیوترهای شبکه داخلی از طریق اینترنت (البته هنوز اجازه دسترسی برای این کامپیوترها به اینترنت وجود دارد)، یک فایروال سخت افزاری اغلب می تواند حفاظت کافی را برای یک کاربر برای دانلود و نصب وصله های نرم افزاری لازم فراهم آورد. فایروال سخت افزاری درجه بالایی از حفاظت را برای کامپیوترهای تازه ای که به اینترنت متصل می شوند، ایجاد می کند.

چنانچه کامپیوتری را از طریق فایروالی که عمل NAT را انجام می دهد، به اینترنت متصل می کنید و یکی از شرایط ذیل برقرار است (الف) ماشین جدید تنها کامپیوتری است که از طریق فایروال به اینترنت متصل می شود یا (ب) تمام ماشینهای دیگر متصل به اینترنت از طریق فایروال، بروز شده باشند و آلوده به ویروسها، کرمها، یا کدهای آسیب رسان دیگر نباشند، در اینصورت شما ممکن است نیاز به فعال کردن فایروال نرم افزاری نباشید.

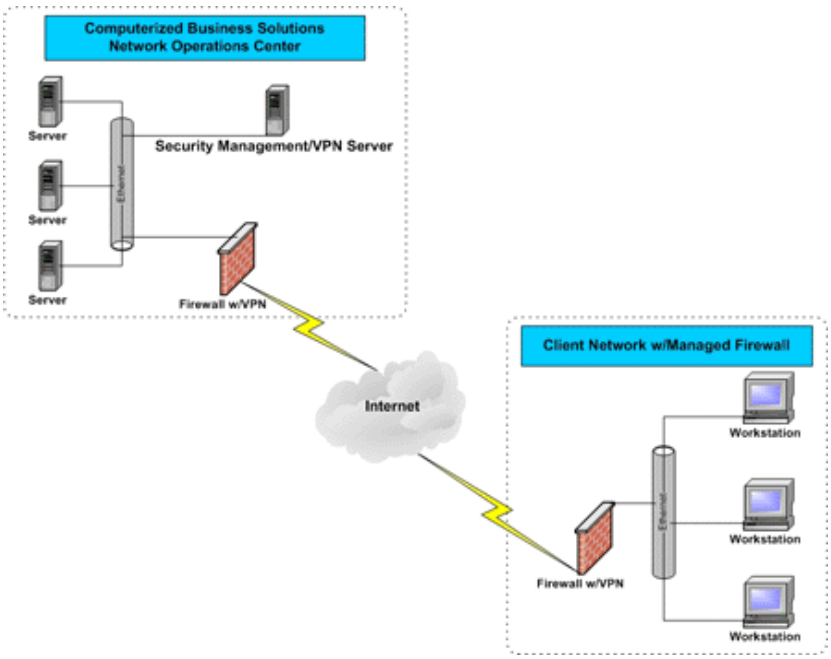
۲- اگر دسترسی دارید، فایروال نرم افزاری موجود در کامپیوتر را فعال کنید.

اگر سیستم عامل شما شامل یک فایروال نرم افزاری است، توصیه می شود که بمنظور مسدود کردن اتصالات از سایر کامپیوترهای موجود در اینترنت آن را فعال کنید.

چنانچه در بالا گفته شد، اگه کامپیوتر شما در حال متصل شدن به یک LAN است که یک فایروال سخت افزاری دارد و بقیه کامپیوترها روی این شبکه کاملاً محافظت شده و بدون کدهای زیان رسان باشند، این مرحله اختیاری است. بهرحال، به عنوان بخشی از استراتژی «دفاع در عمق»، توصیه می شود که فایروال نرم افزاری موجود در سیستم عامل فعال شود.

اگه سیستم عامل شما فاقد فایروال نرم افزاری است، ممکن است که بخواهید برنامه فایروال شخص ثالثی را نصب کنید. بسیاری از چنین برنامه هایی بطور تقریباً رایگان وجود دارند.

بهرحال، با توجه به این مسأله که مورد نظر ما در این مقاله، همان زمان کوتاه اتصال کامپیوتر محافظت نشده به اینترنت است، توصیه می شود که هر برنامه فایروال ثالثی از ابزاری مانند CD، DVD یا **Floppy** قبل از اتصال به اینترنت نصب گردد تا اینکه مستقیماً برروی کامپیوتر محافظت نشده دانلود گردد. در غیر اینصورت، ممکن است که این کامپیوتر قبل از کامل شدن دانلود و نصب نرم افزار مطلوب مورد سوءاستفاده قرار گیرد.



۳- سرویس های غیرضروری را مانند اشتراک فایل و پرینتر غیرفعال کنید.

بیشتر سیستم عامل ها بصورت پیش فرض اشتراک فایل و پرینتر را فعال نمی کنند، بنابراین نباید مسأله ای برای کاربران باشد. بهرحال، اگر کامپیوتر خود را به سیستم عامل جدید ارتقاء می دهید و اشتراک فایل آن فعال است، امکان دارد که در سیستم عامل جدید

نیز این گزینه فعال باشد. از آنجا که سیستم عامل جدید ممکن است شکاف های امنیتی داشته باشد که در نسخه قدیمی تر نبودند، اشتراک فایل را در نسخه قبلی قبل از ارتقاء سیستم عامل غیرفعال کنید. بعد از کامل شدن عمل ارتقاء و نصب تمام وصله های مربوطه، اشتراک فایل در صورت نیاز می تواند مجدداً فعال شود.

۴- وصله های نرم افزاری را در صورت نیاز دانلود و نصب کنید.

زمانی که کامپیوتر از حمله قریب الوقوع از طریق استفاده از فایروال سخت افزاری ویا نرم افزاری و غیرفعال کردن اشتراک فایل و پرینتر محافظت شده است، باید تقریباً اتصال به اینترنت بمنظور دانلود و نصب وصله های نرم افزاری لازم امن باشد. مهم است که این گام حتماً انجام گیرد چون درغیراینصورت کامپیوتر می تواند در معرض سوءاستفاده قرار گیرد اگر بعداً در زمان دیگری فایروال غیرفعال شود یا اشتراک فایل فعال شود.

وصله های نرم افزاری را از سایت های قابل اعتماد و شناخته شده (مانند سایتهای خود فروشندگان نرم افزار)، دانلود کنید تا امکان اینکه یک مزاحم از طریق استفاده از یک اسب تروا کنترل را در اختیار گیرد، به حداقل برسد.

حفاظت کامپیوتر قبل از اتصال به اینترنت (۳)

در. قسمت قبل راهنمای کلی از نظر امنیت برای نصب کامپیوترهای جدید ارائه گردید. بهرحال، عمل به بعضی از آن توصیه ها بستگی به سیستم عامل مورد استفاده دارد. این قسمت مشخصاً به سیستم های عامل ویندوز XP و Apple Macintosh OSX و چند اشاره به سایر سیستم عاملها دارد.

۱- ویندوز XP

بمنظور انجام این مراحل، شما نیاز دارید که به یک اکانت با اختیارات مدیر محلی وارد شوید.

الف. قسمت قبل را مرور کنید.

ب. در صورت امکان، از طریق یک فایروال سخت افزاری متصل شوید.

(به این مرحله در شماره قبل اشاره شده است.)

پ. Internet Connection Firewall موجود در XP را فعال کنید.

(مایکروسافت دستورهای فعال کردن این فایروال را ارائه کرده است.)

http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx

ت. اشتراکها را اگر فعال هستند، غیرفعال کنید.

۱- به Control Panel بروید.

۲- "Network and Internet Connections" را باز کنید.

۳- "Network Connections" را باز کنید.

۴- روی Connection که می خواهید تغییر ایجاد کنید کلیک راست کنید.

۵- "Properties" را انتخاب کنید.

۶- مطمئن شوید که "File and Printer Sharing for Microsoft Networking" انتخاب نشده است.

ث. به شبکه متصل شوید.

ج. به آدرس http://windowsupdate.microsoft.com بروید.

چ. دستورهای موجود در آنجا را برای نصب تمام بروز رسانیهای مهم دنبال کنید.

ح. «امن ماندن» را در زیر مرور کنید.

۲- Apple Macintosh OSX

الف. قسمت قبل را مرور کنید.

ب. در صورت امکان، از طریق یک فایروال سخت افزاری متصل شوید.

پ. فایروال نرم افزاری را فعال کنید.

۱- "System Preferences" را باز کنید.

۲- "Sharing" را انتخاب کنید.

۳- نوار "Firewall" را انتخاب کنید.

۴- روی "Start" کلیک کنید.

۵- نوار "Services" را انتخاب کنید.

۶- بررسی کنید که هیچکدام از سرویس ها انتخاب نشده باشند.

ت. به اینترنت متصل شوید.

ث. نرم افزار نصب شده را به روز کنید.

۱- "System Preferences" را باز کنید.

۲- "Software Updates" را انتخاب کنید.

۳- با انتخاب " Automatically check for updates when you have a network connection " به روزرسانی خودکار را فعال کنید.

۴- زمان بروزرسانی مناسبی انتخاب کنید (بصورت روزانه توصیه می شود)

۵- روی "Check Now" کلیک کنید.

۶- تمام به روزرسانیهای توصیه شده را نصب کنید.

ج. «امن ماندن» را در زیر مرور کنید.

۳- سایر نرم افزارها

در حالیکه یک بسته نرم افزاری آنتی ویروس به روز شده، نمی تواند در برابر تمام کدهای آسیب رسان از یک سیستم محافظت کند، برای بیشتر کاربران بهترین وسیله دفاعی در خط مقدم علیه حملات کدهای آسیب رسان است. بسیاری بسته های آنتی ویروس از بروزرسانیها پشتیبانی می کنند.

پ. اگر امکان دارد بروز رسانیهای خودکار نرم افزار را فعال کنید.

فروشندگان معمولاً هنگامی که یک شکاف امنیتی کشف می گردد، بسته های آن را ارائه می دهند. بیشتر مستندات محصولات روشی برای دریافت به روزها و وصله ها ارائه می دهند. باید بتوانید به روز رسانیها را از سایت فروشنده دریافت کنید.

بعضی برنامه ها بصورت خودکار وجود بروزرسانیها را بررسی می کنند، و بسیاری فروشندگان از طریق لیست ایمیل بصورت خودکار وجود بروزرسانی ها را اطلاع می دهند. وب سایت مورد نظر خود را برای اطلاعات در مورد این نحوه آگاهی نگاه کنید. اگر هیچ لیست ایمیل یا مکانیسم دیگر آگاه سازی بصورت خودکار ارائه نمی شود، نیاز است که وب سایت فروشنده در فواصل زمانی معین برای وجود بروزرسانی ها سرزده شود.

ت. از رفتار ناامن خودداری کنید.

- هنگام بازکردن پیوست های ایمیل یا هنگام استفاده از اشتراک نقطه به نقطه، پیام رسانی فوری یا اتاق های گفتگو، احتیاط کنید.
- اشتراک فایل را روی واسط های شبکه که به طور مستقیم در معرض اینترنت هستند، فعال نکنید.

ث. اصول کمترین حقوق دسترسی را دنبال کنید.

به استفاده از یک اکانت با تنها حقوق «کاربر» بجای حقوق «مدیر» یا سطح «ریشه» برای کارهای روزانه توجه کنید. بسته به سیستم عامل، شما تنها نیاز به استفاده از سطح دسترسی مدیر برای نصب نرم افزار جدید، تغییر پیکربندی سیستم و مانند اینها دارید. حتی بسیاری از سوءاستفاده ها از شکافهای امنیتی (مانند ویروس ها و اسب های تروا) در سطح دسترسی کاربر اجرا می شود، بنابراین بسیار خطرناکتر می شود که همواره بعنوان مدیر وارد سیستم شد.

امنیت تجهیزات شبکه

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

الف – عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می‌دهد که با دستیابی به تجهیزات امکان پیکربندی آنها را به گونه‌ای که تمایل دارند آن سخت‌افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان‌پذیر خواهد شد.

ب – برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهزات بر روی شبکه الزامی است. توسط این حمله‌ها نفوذگران می‌توانند سرویس‌هایی را در شبکه از کار بیاندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای AAA فراهم می‌شود.

در این بخش اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می‌گیرد. عناوین برخی از این موضوعات به شرح زیر هستند:

- امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
- امنیت تجهیزات شبکه در سطوح منطقی

- بالابردن امنیت تجهیزات توسط افزونگی در سرویس‌ها و سخت‌افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند:

- امنیت فیزیکی
- امنیت منطقی

۱ – امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله‌اند. با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات (که توسط عملکرد مشابه سخت‌افزار و یا سرویس‌دهنده مشابه جایگزین می‌شود) بدست می‌آید.

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق تجهزات شبکه را تهدید می‌کنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه‌حل‌ها و ترفندهای دفاعی در برار این‌گونه حملات پرداخت.

۱-۱ – افزونگی در محل استقرار شبکه

یکی از راه‌کارها در قالب ایجاد افزونگی در شبکه‌های کامپیوتری، ایجاد سیستمی کامل، مشابه شبکه‌ی اولیه‌ی در حال کار است. در این راستا، شبکه‌ی ثانویه‌ی، کاملاً مشابه شبکه‌ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که می‌تواند از نظر

جغرافیایی با شبکه‌ی اول فاصله‌ای نه چندان کوتاه نیز داشته باشد برقرار می‌شود. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم جندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

۲-۱ – توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند.

در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

الف – طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی ستاره‌ای : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از خادم اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال

نمی‌گردد. با این وجود از آنجاییکه خادم اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچاراختلال می‌شود، هرچند که با درنظرگرفتن افزونگی برای خادم اصلی از احتمال چنین حالتی کاسته می‌شود.

ج – طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

۳-۱ – محل‌های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.
- در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی می‌گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت:

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- استفاده از دوربین‌های پایش در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.
- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

۴-۱ – انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از خادم‌ها و سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه در زوج‌های تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای

نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

۵-۱ – منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۶-۱ – عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برابر عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد:

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقعایعی اطمینان حاصل کرد.

۲ – امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

۲-۱ – امنیت مسیریاب‌ها

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود:

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تآمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

۲-۲ – مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده‌ها مختص پیکربندی است. از این پرونده‌ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را

به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخه پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تآخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

۳-۲ – کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد:

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تآمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

۲-۴ – امن سازی دسترسی

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secur Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPsec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب‌ها، این روش را مرجح می‌دانند.

۲-۵ – مدیریت رمزهای عبور

مناسب‌ترین محل برای ذخیره رمزهای عبور بر روی خادم Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند. در این صورت مهمترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه است.

۳ – ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه

می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

۱-۳ – قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود:

۱ – قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ – وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می‌گردد.

۲-۳ – مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت.

امنیت در اینترنت

قطعا" تاکنون اخبار متعددی را در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آنان، یکی از روش های مناسب دفاعی است.

اهمیت امنیت در اینترنت

بدون شک کامپیوتر و اینترنت در مدت زمان کوتاهی توانسته اند حضور مشهود خود را در تمامی عرصه های حیات بشری به اثبات برسانند. وجود تحولات عظیم در ارتباطات (نظیر Email و تلفن های سلولی)، تحولات گسترده در زمینه تجهیزات الکترونیکی و سرگرمی (کابل دیجیتال، mp3)، تحولات گسترده در صنعت حمل و نقل (سیستم هدایت اتوماتیک اتومبیل، ناوبری هوائی)، تغییرات اساسی در روش خرید و فروش کالا (فروشگاههای online، کارت های اعتباری)، پیشرفت های برجسته در عرصه پزشکی، صرفا" نمونه هائی اندک در این زمینه می باشد.

اجازه دهید به منظور آشنائی با جایگاه کامپیوتر در زندگی انسان عصر حاضر و اهمیت امنیت اطلاعات، این پرسش را مطرح نمائیم که در طی یک روز چه میزان با کامپیوتر درگیر هستید و چه حجمی از اطلاعات شخصی شما بر روی کامپیوتر خود و یا سایر کامپیوترهای دیگر، ذخیره شده است؟ پاسخ به سوال فوق، جایگاه کامپیوتر و اهمیت ایمن سازی اطلاعات در عصر اطلاعات را به خوبی مشخص خواهد کرد.

امنیت در اینترنت، حفاظت از اطلاعات با استناد به سه اصل اساسی زیر است:

- نحوه پیشگیری از بروز یک تهاجم
- نحوه تشخیص یک تهاجم

- نحوه برخورد با حملات

انواع تهدیدات

اینترنت، علیرغم تمامی جنبه های مثبت دارای مجموعه ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنان بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردار می باشند:

- عملکرد ویروس های کامپیوتری که می تواند منجر به حذف اطلاعات موجود بر روی یک کامپیوتر شود.
- نفوذ افراد غیر مجاز به کامپیوتر شما و تغییر فایل ها
- استفاده از کامپیوتر شما برای تهاجم علیه دیگران
- سرقت اطلاعات حساس نظیر شماره کارت اعتباری و خرید غیر مجاز با استفاده از آن

با رعایت برخی نکات می توان احتمال بروز و یا موفقیت این نوع از حملات را به حداقل مقدار خود رساند.

نحوه حفاظت

اولین مرحله به منظور حفاظت و ایمن سازی اطلاعات ، شناخت تهدیدات و آگاهی لازم در خصوص برخی مفاهیم اولیه در خصوص ایمن سازی اطلاعات است.

- **Hacker، attacker و یا Inruder** . اسامی فوق به افرادی که همواره در صدد استفاده از نقاط ضعف و آسیب پذیر موجود در نرم افزارها می باشند، اطلاق می گردد. با این که در برخی حالات ممکن است افراد فوق اهداف غیر
- مخربی را نداشته و انگیزه آنان صرفا" کنجکاوی باشد، ماحصل عملیات آنان می تواند اثرات جانبی منفی را به دنبال داشته باشد.

- **کد مخرب** : این نوع کدها شامل ویروس ها، کرم ها و برنامه های تروجان (Trojan) بوده که هر یک از آنان دارای ویژگی های منحصر بفردی می باشند:

□ **ویروس ها** ، نوع خاصی از کدهای مخرب می باشند که شما را ملزم می نمایند به منظور آلودگی سیستم، عملیات خاصی را انجام دهید. این نوع از برنامه ها به منظور نیل به اهداف مخرب خود نیازمند یاری کاربران می باشند. باز نمودن یک فایل ضمیمه همراه Email و یا مشاهده یک صفحه وب خاص، نمونه هائی از همکاری کاربران در جهت گسترش این نوع از کدهای مخرب است.

□ **کرم ها** : این نوع از کدهای مخرب بدون نیاز به دخالت کاربر، توزیع و گسترش می یابند. کرم ها، عموما" با سوء استفاده از یک نقطه آسیب پذیر در نرم افزار فعالیت خود را آغاز نموده و سعی می نمایند که کامپیوتر هدف را آلوده نمایند . پس از آلودگی یک کامپیوتر، تلاش برای یافتن و آلودگی سایر کامپیوتر انجام خواهد شد. همانند ویروس های کامپیوتری، کرم ها نیز می توانند از طریق Email، وب سایت ها و یا نرم افزارهای مبتنی بر شبکه، توزیع و گسترش یابند. توزیع اتوماتیک کرم ها نسبت به ویروس ها یکی از تفاوت های محسوس بین این دو نوع کد مخرب، محسوب می گردد.

□ **برنامه های تروجان** : این نوع از کدهای مخرب، نرم افزارهائی می باشند که ادعای ارائه خدماتی را داشته ولی در عمل، اهداف خاص خود را دنبال می نمایند. (تفاوت در حرف و عمل). مثلا" برنامه ای که ادعای افزایش سرعت کامپیوتر شما را می نماید، ممکن است در عمل اطلاعات حساس موجود برروی کامپیوتر شما را برای یک مهاجم و یا سارق از راه دور، ارسال نماید.

محافظت در مقابل خطرات ایمیل (۱)

مقدمه

می خواهیم ببینیم چرا نرم افزار ضد ویروس به تنهایی برای محافظت سازمان شما در مقابل حمله ویروسهای کامپیوتری فعلی و آینده کافی نیست. علاوه بر اینها گاهی به ابزاری قوی برای بررسی محتوای ایمیلها برای حفاظت در مقابل حملات و ویروسهای ایمیل(منظور از ویروس ایمیل ویروسی است که ازطریق ایمیل گسترش می یابد) و جلوگیری از نشت اطلاعات نیاز است. اما در هر صورت رعایت بعضی نکات همیشه توسط کاربران الزامی است.

خطرات ویروسهای ایمیل و اسبهای تروا

استفاده گسترده از ایمیل راه ساده ای را برای گسترش محتویات مضر در شبکه ها پیش روی هکرها قرار داده است. هکرها براحتی می توانند از حصار ایجاد شده توسط یک فایروال از طریق نقب زدن از راه پروتکل ایمیل عبور کنند، زیرا فایروال محتویات ایمیل را بررسی نمی کند. CNN در ژانویه ۲۰۰۴ گزارش داد که ویروس MyDoom هزینه ای در حدود ۲۵۰ میلیون دلار را بدلیل آسیب های وارده و هزینه های پشتیبانی فنی بر شرکتها تحمیل کرده است، این در حالیست که NetworkWorld هزینه های مقابله با Blaster، SoBig.F، Wechia و سایر ویروسهای ایمیل تا سپتامبر ۲۰۰۳ را تنها برای شرکتهای ایالات متحده ۳/۵ میلیارد دلار ذکر کرد.(یعنی عدد ۳۵ با هشت تا صفر جلوش!!!)

بعلاوه، از ایمیل برای نصب اسبهای تروا استفاده می شود که مشخصاً سازمان شما را برای بدست آوردن اطلاعات محرمانه یا بدست گیری کنترل سرورتان، هدف می گیرند. این ویروسها که خبرگان امنیت از آنها بعنوان ویروسهای جاسوسی یاد می کنند، ابزار قدرتمندی در جاسوسی صنعتی بشمار میروند! یک مورد آن حمله ایمیلی به شبکه مایکروسافت در اکتبر۲۰۰۰ است که یک سخنگوی شرکت مایکروسافت از آن بعنوان "یک عمل جاسوسی ساده و تمیز" یاد کرد. برطبق گزارشها، شبکه مایکروسافت توسط یک تروای backdoor که به یک کاربر شبکه توسط ایمیل ارسال شده بود، هک شد.

خطر نشت و فاش شدن اطلاعات

سازمانها اغلب در آگاهی دادن به کارکنانشان نسبت به وجود مخاطرات دزدی داده های مهم شرکتهایشان، کوتاهی می کنند. مطالعات مختلف نشان داده است که چگونه کارمندان از ایمیل بمنظور فرستادن اطلاعات حقوقی محرمانه استفاده می کنند. گاهی آنها اینکار را از روی ناراحتی یا کینه توزی انجام می دهند. گاهی بدلیل عدم درک مناسب از ضربه مهلکی است که در اثر این عمل به سازمان وارد می شود.

گاهی کارمندان از ایمیل برای به اشتراک گذاری داده های حساسی استفاده می کنند که رسماً می بایست در داخل سازمان باقی می ماند.

بر طبق مطالعات و پرس وجوهای Hutton در انگلستان در سال ۲۰۰۳ نشان داده شد که صاحب منصبان دولتی و اعضاء هیات رئیسه BBC از ایمیل برای فاش ساختن اطلاعاتی که محرمانه بوده اند استفاده کرده اند. مقاله ای در مارس ۱۹۹۹ در PC Week به تحقیقی اشاره کرد که طی آن از میان ۸۰۰ پرسنل مورد مطالعه، ۲۱ تا ۳۱ درصد آنها به ارسال اطلاعات محرمانه ـ مانند اطلاعات مالی یا محصولات ـ به افراد خارج از شرکتشان اعتراف کرده اند.

خطر ایمیلهای دربردارنده محتویات بدخواهانه یا اهانت آور

ایمیلهای ارسالی توسط کارکنان که حاوی مطالب نژادپرستانه، امور جنسی یا سایر موضوعات ناخوشایند است، می تواند یک شرکت را از نقطه نظر قانونی آسیب پذیر نماید. در سپتامبر ۲۰۰۳ مشاوران شرکت مالی Holden Meehan مجبور به پرداخت ۱۰هزار پوند به یکی از کارکنان سابق بدلیل ناتوانی در محافظت وی در مقابل آزار ایمیلی! شدند. Chevron مجبور به پرداخت ۲/۲ میلیون دلار به چهار نفر از کارکنانش شد که به وضوح ایمیلهای آزاردهنده جنسی دریافت کرده بودند. تحت قانون انگلیس، کارفرمایان مسوول ایمیلهایی هستند که توسط کارکنانشان در مدت استخدامشان نوشته و ارسال می شود، خواه کارفرما راضی به آن ایمیل بوده باشد، خواه نباشد. مبلغی معادل ۴۵۰هزار دلار از شرکت بیمه Norwich Union طی یک توافق خارج از دادگاه بخاطر ارسال توضیحات مربوط به یک سری از مسابقات درخواست شد.

روشهای استفاده شده برای حمله به سیستم ایمیل

برای درک انواع تهدیدات ایمیلی که امروزه وجود دارد، نگاهی اجمالی به روشهای اصلی فعلی حملات ایمیلی می اندازیم:

ضمیمه هایی با محتوای آسیب رسان

Melissa و LoveLetter جزو اولین ویروسهایی بودند که مساله ضمیمه های (Attachments) ایمیل و اعتماد را نشان دادند. آنها از اعتمادی که بین دوستان و همکاران وجود داشت استفاده می کردند. تصور کنید یک ضمیمه از دوستی دریافت می کنید که از شما می خواهد آن را باز کنید. این همانی است که در Melissa، AnnaKournikova، SirCam و سایر ویروسهای ایمیلی مشابه اتفاق می افتاد. به محض اجرا شدن، چنین ویروسهایی معمولاً خودشان را به آدرسهای ایمیلی که از دفترچه آدرس شخص قربانی بدست میاورند و به ایمیلهایی که صفحات وب ذخیره می کنند، ارسال می کنند. ویروس نویسان تأکید زیادی روی اجرای ضمیمه ای که توسط قربانی دریافت می شود، دارند. بنابراین برای نام ضمیمه ها از عناوین متفاوت و جذاب مانند SexPic.cmd و me.pif استفاده می کنند.

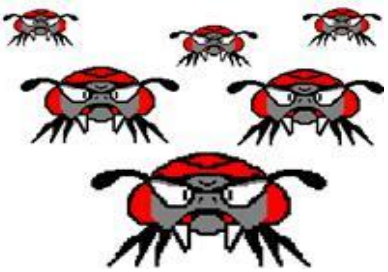
بسیاری از کاربران سعی می کنند که از سرایت ویروسهای ایمیل جلوگیری کنند و فقط روی فایلهایی با پسوندهای مشخص مانند JPG و MPG کلیک می کنند. به هرحال بعضی ویروسها، مانند کرم AnnaKournikova، از پسوند چندتایی بمنظور گول زدن کاربر برای اجرای آن استفاده می کند. ویروس AnnaKournikova از طریق ضمیمه

ایمیل و با عنوان 'AnnaKournikova.jpg.vbs' منتقل میشد که دریافت کننده را متقاعد می کرد که یک تصویر به فرمت JPG را از ستاره مشهور تنیس دریافت کرده است تا اینکه فایل ضمیمه یک اسکریپت ویژوال بیسیک حاوی کدهای آسیب رسان باشد.

بعلاوه، پسوند Class ID (CLSID) به هکرها این اجازه را می دهد که پسوند واقعی فایل را پنهان کنند و بدینوسیله این حقیقت که cleanfile.jpg یک برنامه HTML می باشد پنهان می ماند. این روش در حال حاضر نیز فیلترهای محتوای ایمیل را که از روشهای ساده بررسی فایل استفاده می کنند، فریب می دهد و به هکر امکان رسیدن به کاربر مقصد را به سادگی می دهد.

ایمیلهای راه اندازنده اکسپلویت های شناخته شده

اکسپلویت در حقیقت استفاده از شکافهای امنیتی موجود است. کرم Nimda اینترنت را با شگفتی مواجه کرد و با گول زدن بسیاری از ابزار امنیت ایمیل و نفوذ به سرورها و شبکه های بزرگ و سرایت کردن به کابران خانگی، اینترنت را فراگرفت. حقه بکارگرفته شده توسط Nimda این است که روی کامپیوترهایی که نسخه آسیب پذیری از IE یا Outlook Express را دارند، بطور خودکار اجرا می شود. Nimda از اولین ویروسهایی بود که از یکی از این شکافها بمنظور انتشار بهره برداری می کنند. برای مثال، انواعی از ویروس Bagle که در مارس ۲۰۰۴ ظهور کردند، از یکی از شکافهای اولیه Outlook برای انتشار بدون دخالت کاربر استفاده می کردند.



ایمیلهای با فرمت HTML دربردارنده اسکریپت

امروزه، تمام استفاده کنندگان ایمیل می توانند ایمیلهای HTML را ارسال و دریافت کنند. ایمیل با فرمت HTML می تواند اسکریپتها و محتویات فعالی را دربرگیرد که می توانند به برنامه یا کدها اجازه اجرا روی سیستم دریافت کننده را دهند. Outlook و محصولات دیگر از اجزا IE برای نمایش ایملهای HTML استفاده می کنند، به این معنی که اینها شکافهای امنیتی موجود در IE را به ارث می برند!

ویروسهای بر پایه اسکریپتهای HTML خطر مضاعف توانایی اجرای خودکار را، وقتی که ایمیل آسیب رسان باز می شود، دارند. آنها به ضمیمه ها متوسل نمی شوند؛ بنابراین فیلترهای ضمیمه که در نرم افزارهای ضدویروس وجود دارند در نبرد با ویروسهای اسکریپت HTML بلااستفاده هستند. برای مثال ویروس BadTrans.B از HTML برای اجرای خودکار در هنگام بازشدن استفاده می کند و از یک اکسپلویت ایمیل با فرمت HTML برای انتشار استفاده می کند. در قسمت بعدی به روشهای مقابله خواهیم پرداخت.

آسانی تولید یک ویروس در سالهای اخیر

با داشتن اطلاعات مختصری مثلا در مورد ویژوال بیسیک، می توان با بهره گیری از شکافهای امنیتی، باعث آشفتگی در شبکه ها و سیستم های استفاده کنندگان ایمیل شد. مطالعه بعضی سایتها، شما را با بعضی از شکافهای موجود در Outlook و نحوه بهره گیری از آنها آشنا خواهد کرد. حتی بعضی از کدها نیز در دسترس شما خواهد بود و با تغییرات اندکی می توانید ویروسی تولید کنید که کدهای مورد نظر شما را اجرا کند.

برای مثال می توانید ویروسی تولید کنید که شخص قربانی بمحض باز کردن ایمیل حاوی آن در Outlook، کدهای مورد نظر شما اجرا شود. به این ترتیب تمام فایلهای HTML آلوده می شود و این ویروس به تمام آدرسهای موجود در دفترچه آدرس سیستم آلوده شده فرستاده می شود. در اصل، ویژگی کلیدی این ویروس اجرا شدن آن بمحض باز شدن ایمیل حاوی HTML آسیب رسان است.

آیا نرم افزار ضدویروس یا فایروال برای مقابله کافیست؟

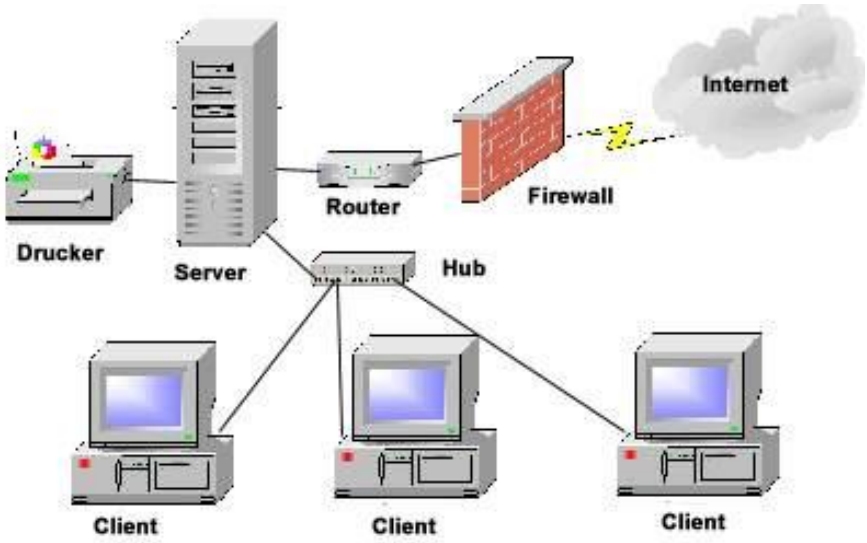
بعضی سازمانها با نصب کردن یک فایروال، خیال خود را از بابت امنیت آسوده می کنند. البته این یک گام ضروری برای محافظت از شبکه داخلیشان است اما کافی

نیست. فایروالها می توانند شبکه شما را از دسترس کاربران غیرمجاز مصون بدارند، اما محتوای ایمیلهایی را که توسط کاربران مجاز از طریق شبکه ارسال و دریافت می شود، بررسی نمی کنند. به این معنی که ویروسهای ایمیلی! می توانند از این سطح امنیتی عبور کنند.

در ضمن، نرم افزارهای ویروس یاب نیز نمی توانند سیستم ها را علیه تمام حمله ها و ویروسهای ایمیلی محافظت کنند.

تولیدکنندگان نرم افزارهای ضدویروس نمی توانند همواره برعلیه ویروسهای مهلکی که از طریق ایمیل در عرض چند ساعت در کل دنیا پراکنده می شوند(مانند کرمهای MyDoom ، NetSky.B و Beagle) مراقبت کامل کنند. بنابراین تکیه تنها بر موتور جستجوی ویروس نیز باعث مراقبت کامل نمی گردد.

برای مثال، یک مطالعه در سال ۲۰۰۴ توسط دولت بریتانیا نشان می دهد که اگرچه ٪۹۹ از شرکتهای بزرگ انگلیسی از ضدویروس استفاده می کنند، اما ٪۶۸ از آنها در طی سال ۲۰۰۳ به ویروسهای مختلف آلوده شده اند. یک تحقیق که در سال ۲۰۰۳ در آزمایشگاههای تحقیقاتی هیولت ـ پکارد در بریستول انجام شد، نشان داد که کرمها از نسخه های به روز ضدویروس ها بمراتب سریعتر گسترش پیدا می کنند.



راه حل: یک رویکرد پیشگیرانه

بنابراین چگونه می توان علیه این خطرات ایمیلی محافظت شد؟ در حقیقت به یک رویکرد پیشگیرانه نیاز است تا محتوای تمام ایمیلهایی وارد شونده و خارج شونده قبل از رسیدن به کاربران، در سطح سِرور بررسی شود. به این ترتیب، تمام محتوای مضر از ایمیل آلوده حذف می گردد و سپس به کاربر فرستاده می شود. سازمانها و شرکتها با نصب یک فیلتر جامع برای بررسی محتوای ایمیلها و یک دروازه (gateway) ضدویروس برروی سرویس دهنده ایمیل، می توانند در مقابله آسیب رسانیهای بالقوه و از بین رفتن زمان مفید کار توسط ویروسهای فعلی و آینده، خود را محافظت کنند.

در مقاله پیشین یعنی محافظت در مقابل خطرات ایمیل(۱) به نکاتی که توسط کاربران ایمیل باید رعایت شود، پرداخته شد و در اینجا به قابلیتهای یک فیلتر خوب برای نصب

در سرویس دهنده ایمیل برای جلوگیری از آلوده شدن توسط ویروسهای ایمیلی اشاره می شود.

- بررسی محتوای ایمیل
- کشف بهره برداریها از شکافهای امنیتی(اکسپلویتها)
- تحلیل خطرات
- راه حلهای ضدویروسی

موارد فوق برای ازبین بردن انواع خطراتی است که توسط ایمیلها منتقل می شود، قبل از اینکه بتوانند کاربران ایمیل را تحت تاثیر قرار دهند.

ویژگیهای زیر را نیز می توان به فیلتر مذکور اضافه کرد:

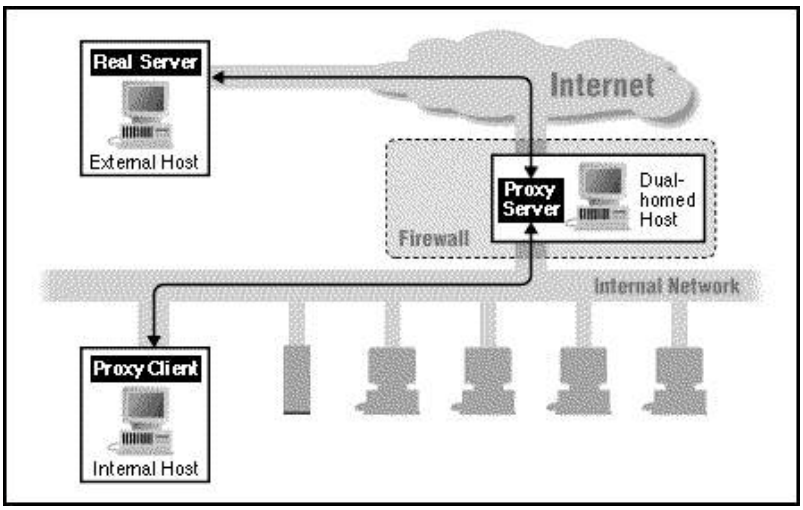
- دربرداشتن چندین موتور ویروس برای بالا بردن نرخ کشف ویروس و پاسخ سریعتر به ویروسهای جدید.
- بررسی پیوستهای ایمیلها برای مصونیت در مقابل ضمیمه های خطرناک
- یک سپر در مقابل اکسپلویتها برای محافظت در مقابل ویروسهای فعلی و آتی که برپایه اکسپلویتها ایجاد گشته اند.
- یک موتور بررسی خطرات HTML برای از کار انداختن اسکریپتهای HTML
- یک پویشگر برای ترواها و فایلهای اجرایی برای کشف فایلهای اجرایی آسیب رسان و مهم ترین و آخرین نکته که تا کنون چندین بار به آن اشاره شده است این است که ایمیلهای ناشناخته را باز نکنید.

بخش : هاشم

Security Tools

پراکسی سرور

در یک تشکیلات که از اینترنت استفاده می‌کند، یک پراکسی سرور ترکیبی از سخت‌افزار و نرم‌افزار است که بعنوان یک واسطه بین کاربر داخلی و اینترنت عمل می‌کند به طوریکه امنیت، نظارت مدیریتی و سرویس‌های caching تامین می‌شود. یک سرور پراکسی دارای پروتکل مشخصی است، بنابراین برای هرنوع پروتکلی (HTTP، FTP، Gogher و غیره) باید تنظیم شود. پراکسی سرور بعنوان بخشی از یک سرور gateway (نقطه‌ای در یک شبکه که ورودی به شبکه‌ای دیگر است) رفتار می‌کند و می‌تواند برای انجام یک یا چند فانکشن که در بخش بعد به آن اشاره می‌شود، تنظیم شود.



عملکردهایی که پراکسی سرور می‌تواند داشته باشد

با تعریفی که از یک پراکسی ارائه شد، می‌توان از پراکسی برای بهبود عملکرد یک شبکه استفاده‌هایی کرد که در اینجا به چند مورد آن به اختصار اشاره می‌کنیم:

- **Firewall (دیواره آتش)**

برای سازمانی که فایروال دارد، پراکسی سرور تقاضاهای کاربران را به فایروال می‌دهد که با آنها اجازه ورود یا خروج به شبکه داخلی را می‌دهد.

- **Caching (ذخیره سازی)**

سرور پراکسی که عمل caching را انجام می‌دهد، منابعی مانند صفحات وب و فایل‌ها را ذخیره می‌کند. هنگامی که یک منبع مورد دسترسی قرار گرفت، در سرور دخیره می‌شود و تقاضاهای بعدی برای همین منبع مشخص با محتویات cache پاسخ داده می‌شود. این عمل، دسترسی به آن منبع را برای کاربرانی که از طریق پراکسی به اینترنت متصل هستند، سرعت می‌بخشد و از طرفی از ترافیک اینترنت می‌کاهد و اجازه استفاده بهتر از پهنای باند به کاربران داده می‌شود.

- **Filtering (فیلتر کردن)**

سرور پراکسی می‌تواند ترافیک وارد شونده و خارج شونده از شبکه را بررسی کند و به آنچه که با معیارهای امنیتی یا سیاست سازمان مغایرت دارد، اجازه عبور ندهد.

- **Authentication (تصدیق هویت)**

بسیاری منابع الکترونیکی سازمانی توسط ورود با کلمه رمز یا قرار داشتن در دامنه مشخصی از IP محدود شده‌اند. کاربران دور معمولاً از یک سرویس‌دهنده اینترنت ثالث استفاده می‌کنند که در این صورت این کاربر یا IP کامپیوتر آن برای سازمان معتبر تشخیص داده نمی‌شود. برای کاربرانی که بصورت فیزیکی به شبکه داخلی سازمان متصل نشده‌اند، پراکسی طوری عمل می‌کند که به کاربران دور اجازه ورود موقت داده شود یا به آنها بطور موقت یک IP سازمان تخصیص داده شود که بتوانند به منابع محدود شده دسترسی پیدا کنند.

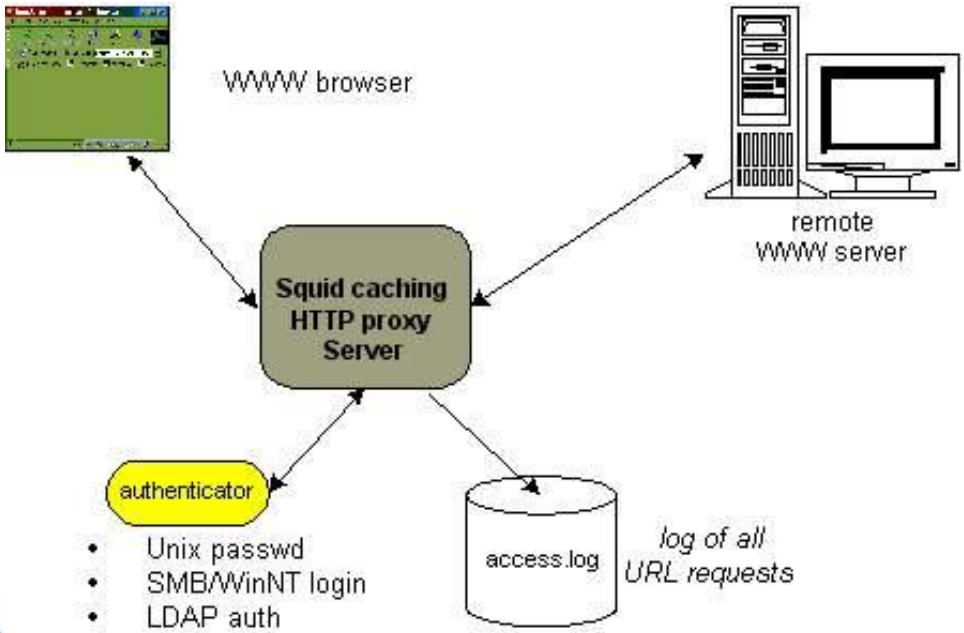
- **Anonymization (تغییر هویت)**

برای محافظت شبکه داخلی یک سازمان از کاربران موجود در اینترنت، سرور پراکسی می‌تواند هویت سیستم‌های متقاضی داخلی را تغییر دهد. اگر منبع (مثلاً صفحه وب یا فایل) تقاضا شده توسط کاربر داخلی سازمان، در cache موجود نباشد، سرور پراکسی برای آن کاربر، بعنوان کلاینت عمل می‌کند و از یکی از آدرس‌های IP خودش برای تقاضای آن منبع از سرور موجود در اینترنت استفاده می‌کند. این آدرس IP «موقت»، آدرسی نیست که واقعاً در شبکه داخلی سازمان استفاده گردد و در نتیجه از بعضی از حمله‌های نفوذگران جلوگیری می‌شود. هنگامی که صفحه تقاضا شده، از طرف سرور روی اینترنت به پراکسی سرور می‌رسد، پراکسی سرور آن را به تقاضای اولیه مرتبط

می‌کند و برای کاربر می‌فرستد. این پروسه تغییر دادن IP باعث می‌شود که تقاضا دهنده اولیه قابل ردیابی نباشد و همچنین معماری شبکه سازمان از دید بیرونی مخفی بماند.

- **Logging (ثبت کردن)**

پراکسی سرور می‌تواند تقاضاها را بهمراه اطلاعات لازم در جایی ثبت کند تا بعداً امکان پیگیری اعمال کاربران داخل سازمان فراهم شود.

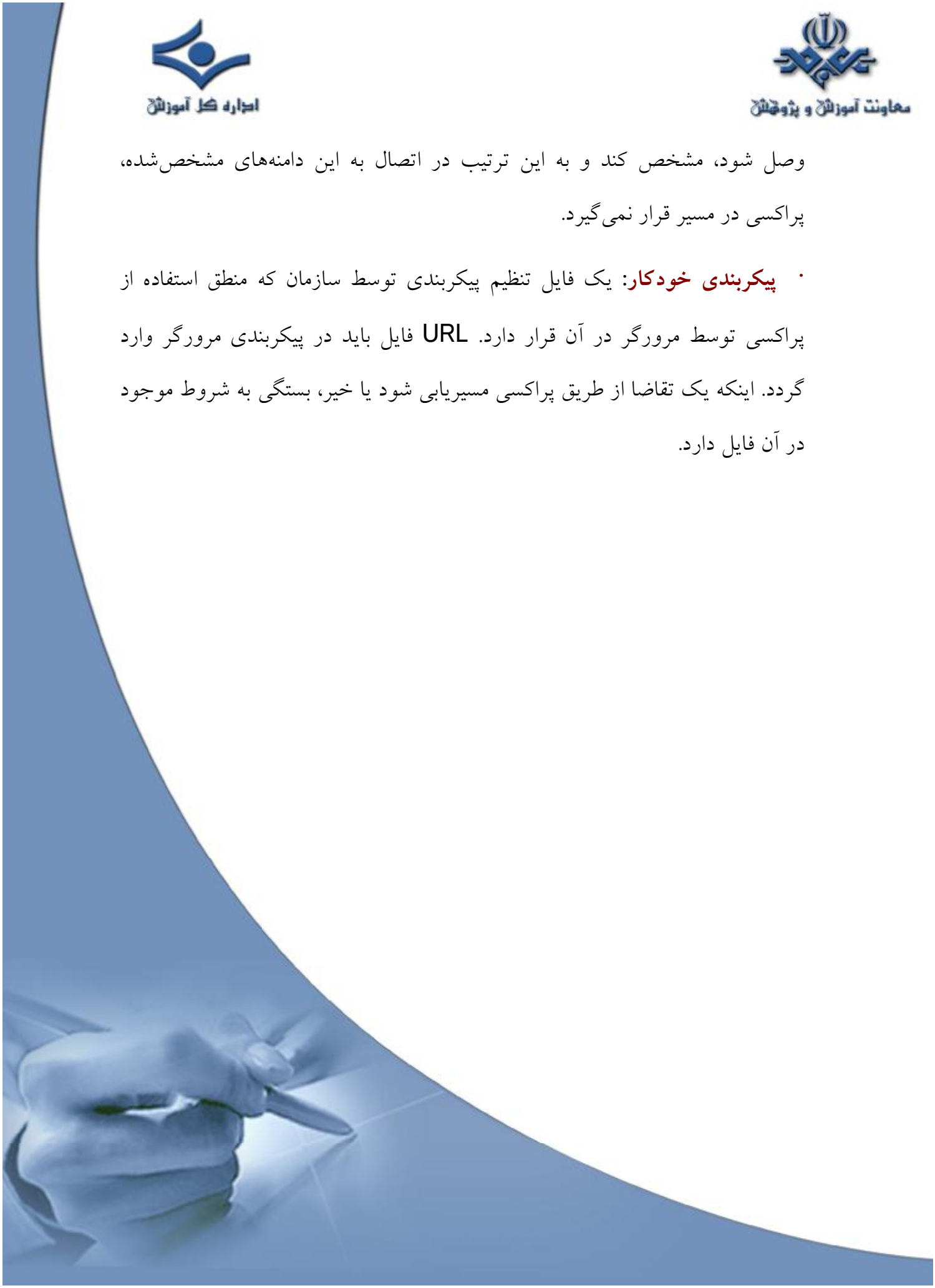


پیکربندی مرورگر

- **تعامل کاربر:** کاربر باید از ابتدا مرورگر خود را پیکربندی کند که بدین ترتیب نیاز است که اطلاعات را از پشتیبانی فنی سازمان بدست آورد.
- **پیکربندی دستی:** در این پیکربندی کاربر باید سروری را که نرم‌افزار پراکسی را اجرا می‌کند، مشخص کند. کاربر باید استثنائات هر دامنه‌ای را که می‌تواند بطور مستقیم به آن

وصل شود، مشخص کند و به این ترتیب در اتصال به این دامنه‌های مشخص‌شده، پراکسی در مسیر قرار نمی‌گیرد.

- **پیکربندی خودکار**: یک فایل تنظیم پیکربندی توسط سازمان که منطق استفاده از پراکسی توسط مرورگر در آن قرار دارد. URL فایل باید در پیکربندی مرورگر وارد گردد. اینکه یک تقاضا از طریق پراکسی مسیریابی شود یا خیر، بستگی به شروط موجود در آن فایل دارد.



کاربرد پراکسی در امنیت شبکه (۱)

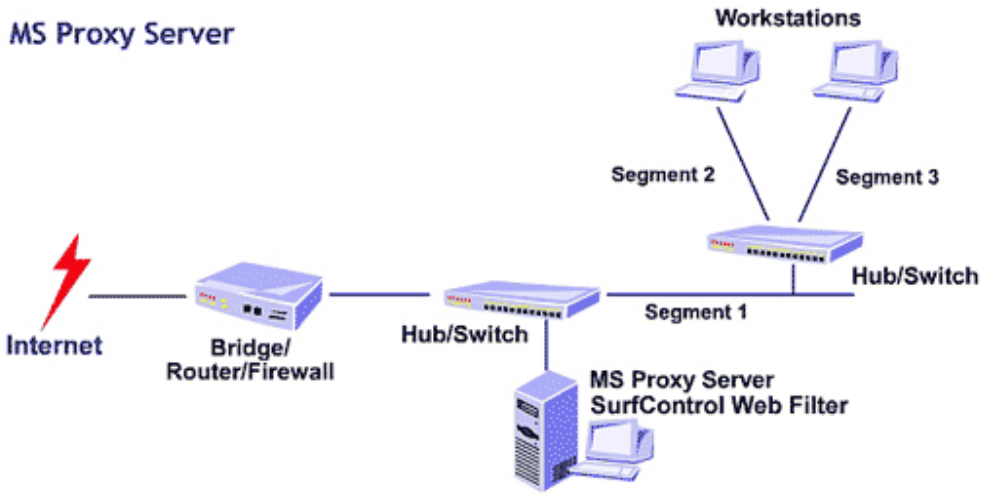
بعد از آشنایی با پراکسی «پراکسی سرور» در این قسمت به این مطلب می پردازیم که از دیدگاه امنیتی پراکسی چیست و چه چیزی نیست، از چه نوع حملاتی جلوگیری می کند و به مشخصات بعضی انواع پراکسی پرداخته می شود. البته قبل از پرداختن به پراکسی بعنوان ابزار امنیتی، بیشتر با فیلترها آشنا خواهیم شد.

پراکسی چیست؟

در دنیای امنیت شبکه، افراد از عبارت «پراکسی» برای خیلی چیزها استفاده می کنند. اما عموماً، پراکسی ابزار است که بسته های دیتای اینترنتی را در مسیر دریافت می کند، آن دیتا را می سنجد و عملیاتی برای سیستم مقصد آن دیتا انجام می دهد. در اینجا از پراکسی به معنی پروسه ای یاد می شود که در راه ترافیک شبکه ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار میگیرد و آن را می سنجد تا ببیند با سیاست های امنیتی شما مطابقت دارد و سپس مشخص می کند که آیا به آن اجازه عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور مورد نظر ارسال و بسته های ردشده دور ریخته می شوند.

پراکسی چه چیزی هست؟

پراکسی ها بعضی اوقات با دو نوع فایروال اشتباه می شوند «Packet filter و Stateful packet filter» که البته هر کدام از روش ها مزایا و معایبی دارد، زیرا همیشه یک مصالحه بین کارایی و امنیت وجود دارد.



پراکسی با Packet filter تفاوت دارد

ابتدایی ترین روش صدور اجازه عبور به ترافیک بر اساس TCP/IP این نوع فیلتر بود. این نوع فیلتر بین دو یا بیشتر رابط شبکه قرار می گیرد و اطلاعات آدرس را در IP header ترافیک دیتایی که بین آنها عبور می کند، پیمایش می کند. اطلاعاتی که این نوع فیلتر ارزیابی می کند عموماً شامل آدرس و پورت منبع و مقصد می شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و بر اساس قوانین ایجاد شده توسط مدیر شبکه بسته را می پذیرد یا نمی پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می شود. و عیب اصلی ان این است که هرگز آنچه را که در بسته وجود دارد نمی بیند و به محتوای آسیب رسان اجازه عبور از فایروال را می دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می کند و وضعیت (State) ارتباط را دنبال نمی کند.

پراکسی با Stateful packet filter تفاوت دارد

این فیلتر اعمال فیلتر نوع قبل را انجام می دهد، بعلاوه اینکه بررسی می کند کدام کامپیوتر در حال ارسال چه دیتایی است و چه نوع دیتایی باید بیاید. این اطلاعات بعنوان وضعیت (State) شناخته می شود.

پروتکل ارتباطی TCP/IP به ترتیبی از ارتباط برای برقراری یک مکالمه بین کامپیوترها نیاز دارد. در آغاز یک ارتباط TCP/IP عادی، کامپیوتر A سعی می کند با ارسال یک بسته SYN (synchronize) به کامپیوتر B ارتباط را برقرار کند. کامپیوتر B در جواب یک بسته SYN/ACK (Acknowledgement)) برمی گرداند، و کامپیوتر A یک ACK به کامپیوتر B می فرستد و به این ترتیب ارتباط برقرار می شود. TCP اجازه وضعیتهای دیگر، مثلاً FIN (finish) برای نشان دادن آخرین بسته در یک ارتباط را نیز می دهد.

هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما می پردازند. یک روش معمول ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، می فرستند. معمولاً، کامپیوتر دریافت کننده بیاید پیامی بفرستد و بگوید "I don't understand". به این ترتیب، به هکر نشان می دهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ می تواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط

TCP/IP را می فهمد و می تواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ـــ آنچه که یک فیلتر packet ردگیری نمی کند و نمی تواند انجام دهد. فیلترهای Stateful packet می توانند در همان لحظه قواعدی را مبنی بر اینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکم تر است. این امنیت محکم تر، بهرحال، تا حدی باعث کاستن از کارایی می شود. نگاهداری لیست قواعد ارتباط بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

پراکسی ها یا Application Gateways

Application Gateways که عموماً پراکسی نامیده می شود، پیشرفته ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال ها هستند. پراکسی بین کلاینت و سرور قرار می گیرد و تمام جوانب گفتگوی بین آنها را برای تایید تبعیت از قوانین برقرار شده، می سنجد. پراکسی بار واقعی تمام بسته های عبوری بین سرور و کلاینت را می سنجد، و میتواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط headerها را می سنجند، در حالیکه پراکسی ها محتوای بسته را با مسدود کردن کدهای آسیب رسان همچون فایلهای اجرایی، اپلت های جاوا، ActiveX و ... غربال می کنند.

پراکسی ها همچنین محتوا را برای اطمینان از اینکه با استانداردهای پروتکل مطابقت دارند، می سنجند. برای مثال، بعضی اَشکال حمله کامپیوتری شامل ارسال متاکاراکترها برای فریفتن سیستم قربانی است؛ حمله های دیگر شامل تحت تاثیر قراردادن سیستم با دیتای بسیار زیاد است. پراکسی ها می توانند کاراکترهای غیرقانونی یا رشته های خیلی طولانی را مشخص و مسدود کنند. بعلاوه، پراکسی ها تمام اعمال فیلترهای ذکرشده را انجام می دهند. بدلیل تمام این مزیتها، پراکسی ها بعنوان یکی از امن ترین روشهای عبور ترافیک شناخته می شوند. آنها در پردازش ترافیک از فایروالها کندتر هستند زیرا کل بسته ها را پیمایش می کنند. بهرحال «کندتر» بودن یک عبارت نسبی است.

آیا واقعاً کند است؟ کارایی پراکسی بمراتب سریعتر از کارایی اتصال اینترنت کاربران خانگی و سازمانهاست. معمولاً خود اتصال اینترنت گلوگاه سرعت هر شبکه ای است. پراکسی ها باعث کندی سرعت ترافیک در تست های آزمایشگاهی می شوند اما باعث کندی سرعت دریافت کاربران نمی شوند.

در شماره بعد بیشتر به پراکسی خواهیم پرداخت.

کاربرد پراکسی در امنیت شبکه (۲)

در مقایسه فایروال‌ها، ما مفهومی از پراکسی ارائه می‌دهیم و پراکسی را از فیلترکننده بسته‌ها متمایز می‌کنیم. با پیش‌زمینه‌ای که از پراکسی در شماره قبل بیان کردیم، می‌توانیم در اینجا مزایای پراکسی‌ها بعنوان ابزاری برای امنیت را لیست کنیم:

- با مسدود کردن روش‌های معمول مورد استفاده در حمله‌ها، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با پنهان کردن جزئیات سرورهای شبکه شما از اینترنت عمومی، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با جلوگیری از ورود محتویات ناخواسته و نامناسب به شبکه شما، استفاده از پهنای باند شبکه را بهبود می‌بخشند.
- با ممانعت از یک هکر برای استفاده از شبکه شما بعنوان نقطه شروعی برای حمله دیگر، از میزان این نوع مشارکت می‌کاهند.
- با فراهم‌آوردن ابزار و پیش‌فرض‌هایی برای مدیر شبکه شما که می‌توانند بطور گسترده‌ای استفاده شوند، می‌توانند مدیریت شبکه شما را آسان سازند.

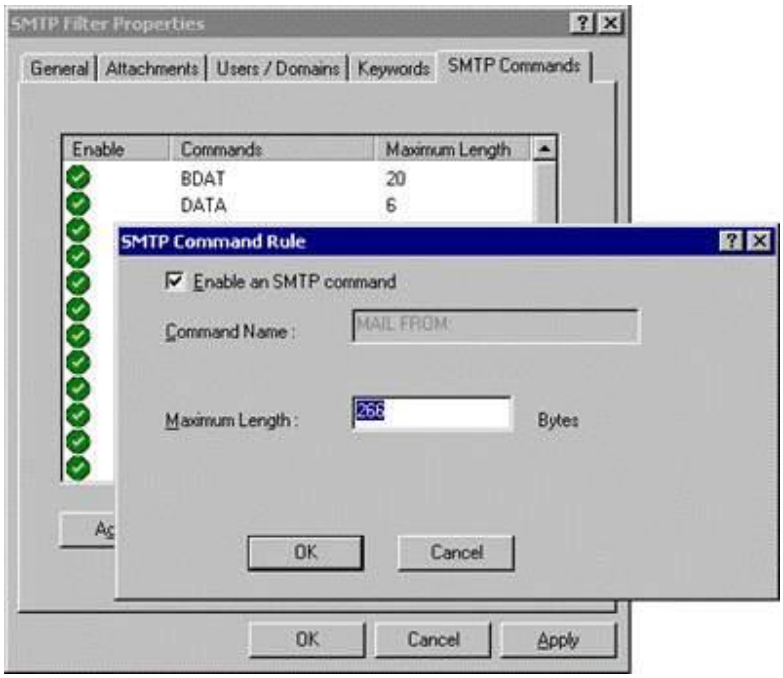
بطور مختصر می‌توان این مزایا را اینگونه بیان کرد؛ پراکسی‌ها به شما کمک می‌کنند که شبکه‌تان را با امنیت بیشتر، موثرتر و اقتصادی‌تر مورد استفاده قرار دهید. بهرحال در ارزیابی یک فایروال، این مزایا به فواید اساسی تبدیل می‌شوند که توجه جدی را می‌طلبند.

برخی انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند.

البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد. در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

- SMTP Proxy
- HTTP Proxy
- FTP Proxy
- DNS Proxy



SMTP Proxy

پراکسی SMTP (Simple Mail Transport Protocol) محتویات ایمیل‌های وارد شونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از تواناییهای آن اینها هستند:

- **مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام**: این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.
- **مشخص کردن بزرگترین اندازه پیام**: این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.

- **اجازه دادن به کاراکترهای مشخص در آدرسهای ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده است:** چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرسها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.
- **فیلترکردن محتوا برای جلوگیری از انواعی محتویات اجرایی:** معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.
- **فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول\مردود:** هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.
- **فیلترکردن Headerهای ایمیل:** Headerها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات Header برای حمله به سرورهای ایمیل یافته‌اند. پراکسی

مطمئن می‌شود که Headerها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده headerهای تغییرشکل‌داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.

- **تغییردادن یا پنهان‌کردن نامهای دامنه و IDهای پیام‌ها:** ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای header هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

در شماره بعد بررسی انواع دیگر پراکسی را ادامه خواهیم داد.

کاربرد پراکسی در امنیت شبکه (۳)

در شماره های قبل به پراکسی سرور، مقایسه پراکسی و فایروال و پراکسی SMTP پرداختیم. به بررسی انواع دیگر پراکسی می پردازیم:

HTTP Proxy

این پراکسی بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به World Wide Web ایجاد شده، نظارت می کند. این پراکسی برای مراقبت از کلاینت های وب شما و سایر برنامه ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می کند. بعضی از قابلیتهای آن اینها هستند:

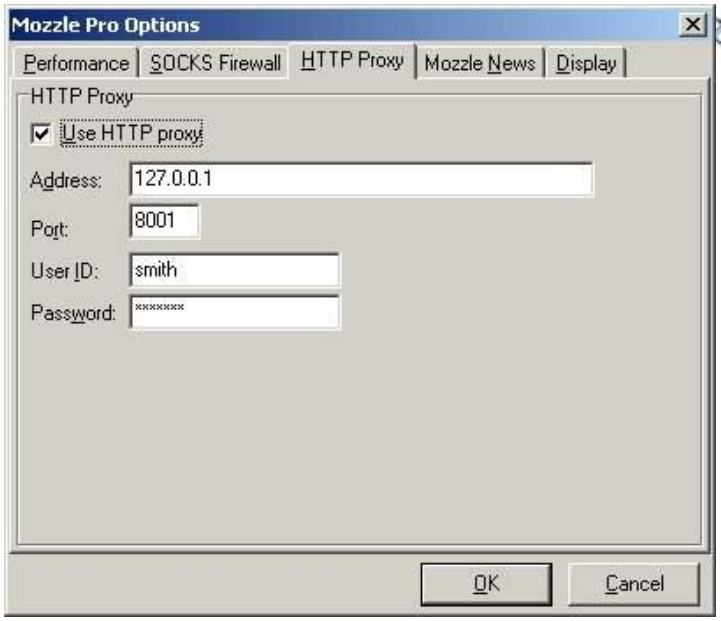
- **برداشتن اطلاعات اتصال کلاینت:** این پراکسی می تواند آن قسمت از دیتای header را که نسخه سیستم عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟
- **تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب:** در بسیاری از حمله ها، هکرها بسته های تغییرشکل داده شده را ارسال می کنند که باعث

دستکاری عناصر دیگر صفحه وب می شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی کردند، وارد می شوند.

پراکسی HTTP این اطلاعات بی معنی را نمی پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می کند.

- **فیلترکردن محتوای از نوع MIME** : الگوهای MIME به مرورگر وب کمک می کنند تا بداند چگونه محتوا را تفسیر کند تا با یک تصویرگرافیکی بصورت یک گرافیک رفتار شود، یا **.wav** فایل بعنوان صوت پخش شود، متن نمایش داده شود و غیره. بسیاری حمله های وب بسته هایی هستند که در مورد الگوی MIME خود دروغ می گویند یا الگوی آن را مشخص نمی کنند. پراکسی HTTP این فعالیت مشکوک را تشخیص می دهد و چنین ترافیک دیتایی را متوقف می کند.
- **فیلترکردن کنترلهای Java و ActiveX**: برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند بصورت خودکار آن صفحه را صفحه خانگی مرورگر آن فرد نماید). پراکسی می تواند این برنامه ها را مسدود کند و به این ترتیب جلوی بسیاری از حمله ها را بگیرد.
- **برداشتن کوکی ها:** پراکسی HTTP می تواند جلوی ورود تمام کوکی ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.

- **برداشتن Headerهای ناشناس:** پراکسی HTTP ، از headerهای HTTP که از استاندارد پیروی نمی کنند، ممانعت بعمل می آورد. یعنی که، بجای مجبور بودن به تشخیص حمله های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می ریزد. این رویکرد ساده از شما در مقابل تکنیک های حمله های ناشناس دفاع می کند.
- **فیلترکردن محتوا:** دادگاه ها مقررکرده اند که تمام کارمندان حق برخورداری از یک محیط کاری غیر خصمانه را دارند. بعضی عملیات تجاری نشان می دهد که بعضی موارد روی وب جایگاهی در شبکه های شرکت ها ندارند. پراکسی HTTP سیاست امنیتی شرکت شما را وادار می کند که توجه کند چه محتویاتی مورد پذیرش در محیط کاریتان است و چه هنگام استفاده نامناسب از اینترنت در یک محیط کاری باعث کاستن از بازده کاری می شود. بعلاوه، پراکسی HTTP می تواند سستی ناشی از فضای سایبر را کم کند. گروه های مشخصی از وب سایتها که باعث کم کردن تمرکز کارمندان از کارشان می شود، می توانند غیرقابل دسترس شوند.

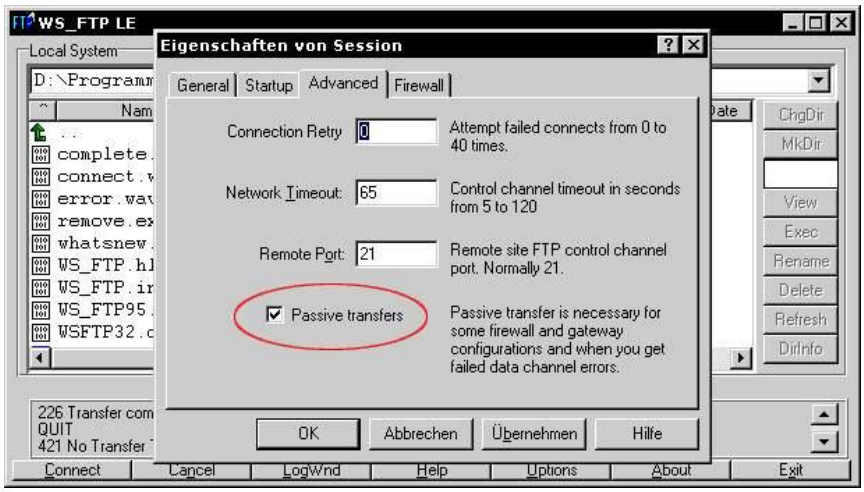


FTP Proxy

بسیاری از سازمان ها از اینترنت برای انتقال فایل های دیتای بزرگ از جایی به جایی دیگر استفاده می کنند. در حالیکه فایل های کوچک تر می توانند بعنوان پیوست های ایمیل منتقل شوند، فایل های بزرگ تر توسط FTP (File Transfer Protocol) فرستاده می شوند. بدلیل اینکه سرورهای FTP فضایی را برای ذخیره فایل ها آماده می کنند، هکرها علاقه زیادی به دسترسی به این سرورها دارند. پراکسی FTP معمولاً این امکانات را دارد:

- **محدودکردن ارتباطات از بیرون به «فقط خواندنی»**: این عمل به شما اجازه می دهد که فایل ها را در دسترس عموم قرار دهید، بدون اینکه توانایی نوشتن فایل روی سرورتان را بدهید.

- **محدود کردن ارتباطات به بیرون به «فقط خواندنی»**: این عمل از نوشتن فایل های محرمانه شرکت به سرورهای FTP خارج از شبکه داخلی توسط کاربران جلوگیری می کند.
- **مشخص کردن زمانی ثانیه های انقضای زمانی:** این عمل به سرور شما اجازه می دهد که قبل از حالت تعلیق و یا Idle request ارتباط را قطع کند.
- **ازکارانداختن فرمان FTP SITE** : این از حمله هایی جلوگیری می کند که طی آن هکر فضـایی از سرور شـــما را تسخیر می کند تا با استفاده از سیستم شما حمله بعدی خودش را پایه ریزی می کند.



DNS Proxy

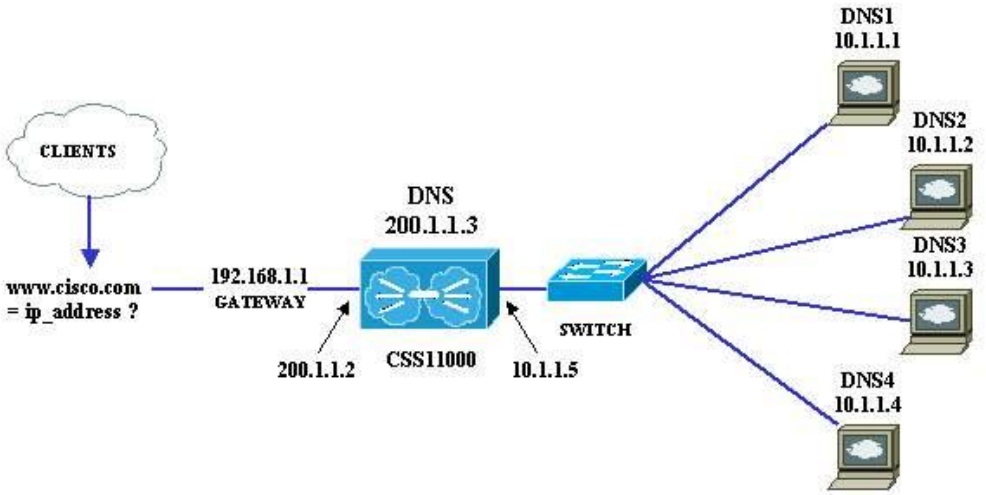
DNS (Domain Name Server) شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانند

http://www.irib.com در مرورگر وب خود تایپ کنید و وارد این سایت شوید – بدون توجه به اینکه از کجای دنیا به اینترنت متصل شده اید. بمنظور تعیین موقعیت و نمایش منابعی که شما از اینترنت درخواست می کنید، DNS نام های دامنه هایی را که می توانیم براحتی بخاطر بسپاریم به آدرس IP هایی که کامپیوترها قادر به درک آن هستند، تبدیل می کند. در اصل این یک پایگاه داده است که در تمام اینترنت توزیع شده است و توسط نام دامنه ها فهرست شده است.

بهرحال، این حقیقت که این سرورها در تمام دنیا با مشغولیت زیاد در حال پاسخ دادن به تقاضاها برای صفحات وب هستند، به هکرها امکان تعامل و ارسال دیتا به این سرورها را برای درگیرکردن آنها می دهد. حمله های برپایه DNS هنوز خیلی شناخته شده نیستند، زیرا به سطحی از پیچیدگی فنی نیاز دارند که بیشتر هکرها نمی توانند به آن برسند. بهرحال، بعضی تکنیک های هک که میشناسیم باعث می شوند هکرها کنترل کامل را بدست گیرند. بعضی قابلیت های پراکسی DNS می تواند موارد زیر باشد:

- **تضمین انطباق پروتکلی:** یک کلاس تکنیکی بالای اکسپلویت می تواند لایه Transport را که تقاضاها و پاسخ های DNS را انتقال می دهد به یک ابزار خطرناک تبدیل کند. این نوع از حمله ها بسته هایی تغییرشکل داده شده بمنظور انتقال کد آسیب رسان ایجاد می کنند. پراکسی DNS، headerهای بسته های DNS را بررسی می کند و بسته هایی را که بصورت ناصحیح ساخته شده اند دور می ریزد و به این ترتیب جلوی بسیاری از انواع سوء استفاده را می گیرد.

- **فیلترکردن محتوای header‌ها بصورت گزینشی:** DNS در سال ۱۹۸۴ ایجاد شده و از آن موقع بهبود یافته است. بعضی از حمله های DNS بر ویژگی هایی تکیه می کنند که هنوز تایید نشده اند. پراکسی DNS می تواند محتوای header تقاضاهای DNS را بررسی کند و تقاضاهایی را که کلاس، نوع یا طول header غیرعادی دارند، مسدود کند.

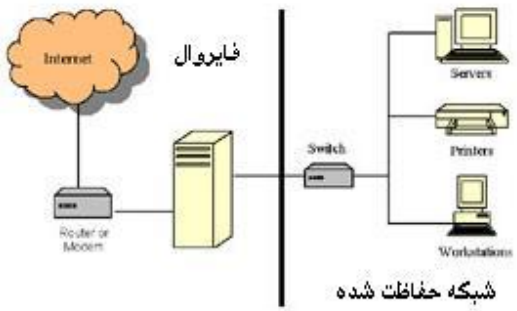


نتیجه گیری

با مطالعه این قسمت ها، تا حدی با پراکسی ها آشنا شدیم. پراکسی تمام ابزار امنیت نیست، اما یک ابزار عالیست، هنگامی که با سایر امنیت سنج ها! مانند ضدویروس های استاندارد، نرم افزارهای امنیتی سرور و سیستم های امنیتی فیزیکی بکار برده شود.

فایروال (قسمت اول)

در صورتی که تاکنون مدت زمان کوتاهی از اینترنت استفاده کرده باشید و یا در یک اداره مشغول بکار هستید که بستر لازم برای دستیابی به اینترنت فراهم شده باشد، احتمالا" واژه " **فایروال** " را شنیده اید. مثلا" اغلب گفته می شود که: " در اداره ما امکان استفاده از این سایت وجود ندارد، چون سایت فوق را از طریق فایروال بسته اند". در صورتیکه از طریق خط تلفن به مرکز ارائه دهنده خدمات اینترنت (ISP) متصل و از اینترنت استفاده می نمائید، امکان استفاده فایروال توسط ISP مربوطه نیز وجود دارد. امروزه در کشورهائی که دارای خطوط ارتباطی با سرعت بالا نظیر DSL و یا مودم های کابلی می باشند، به کاربران خانگی توصیه می گردد که هر یک از فایروال استفاده نموده و با استقرار لایه فوق بین شبکه داخلی در منزل و اینترنت، مسائل ایمنی را رعایت نمایند. بدین ترتیب با استفاده از یک فایروال می توان یک شبکه را در مقابل عملیات غیر مجاز توسط افراد مجاز و عملیات مجاز توسط افراد غیرمجاز حفاظت کرد.



فایروال چیست ؟

فایروال نرم افزار و یا سخت افزاری است که اطلاعات ارسالی از طریق اینترنت به شبکه خصوصی و یا کامپیوتر شخصی را فیلتر می نماید. اطلاعات فیلترشده، فرصت توزیع در شبکه را بدست نخواهند آورد.

فرض کنید، سازمانی دارای ۵۰۰ کارمند باشد. سازمان فوق دارای ده ها کامپیوتر بوده که بر روی هر کدام یک کارت شبکه نصب شده و یک شبکه درون سازمانی (خصوصی) ایجاد شده است. سازمان فوق دارای یک یا چند خط اختصاصی (T۱ و یا T3) برای استفاده از اینترنت است. بدون استفاده از فایروال تمام کامپیوترهای موجود در شبکه داخلی، قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت می باشند. کاربران مربوطه قادر به استفاده از برنامه هائی همچون FTP و یا Telnet بمنظور ارتباط مستقیم با افراد حقوقی و یا حقیقی موجود بر روی اینترنت می باشند. عدم رعایت مسائل ایمنی توسط پرسنل سازمان، می تواند زمینه دستیابی به اطلاعات موجود در شبکه داخلی را برای سارقین و متجاوزان اطلاعاتی اینترنت فراهم نماید.

زمانیکه در سازمان فوق از فایروال استفاده گردد، وضعیت کاملا" تغییر خواهد کرد. سازمان مربوطه می تواند برروی هر یک از خطوط ارتباطی اینترنت یک فایروال نصب نماید.فایروال مجموعه سیاست های امنیتی را پیاده سازی می نماید. مثلا" یکی از قوانین فوق می تواند بصورت زیر باشد:

تمام کامپیوترهای موجود در شبکه مجاز به استفاده از اینترنت می باشند ، فقط یک فرد مجاز به استفاده از سرویس FTP است و سایر پرسنل مجاز به استفاده از سرویس فوق نخواهند بود.

یک سازمان می تواند برای هر یک از سرویس دهندگان خود (وب ، FTP، Telnet و ...) قوانین مشابه تعریف نماید. سازمان قادر به کنترل پرسنل بهمراه لیست سایت های مشاهده خواهد بود. با استفاده از فایروال یک سازمان قادر به کنترل کاربران شبکه خواهد بود.

فایروال ها بمنظور کنترل ترافیک یک شبکه از روش های زیر استفاده می نمایند:

- **فیلتر نمودن بسته های اطلاعاتی** . بسته های اطلاعاتی با استفاده ازتعدادی فیلتر، آنالیز خواهند شد. بسته هائی که از آنالیز فوق سربلند بیرون آیند از فایروال عبور داده شده و بسته ها ئی که شرایط لازم را برای عبور از فایروال را نداشته باشند دور انداخته شده و از فایروال عبور نخواهند کرد.
- **سرویس Proxy** . اطلاعات درخواستی از طریق اینترنت توسط فایروال بازیابی و در ادامه در اختیار درخواست کننده گذاشته خواهد شد. وضعیت فوق در مواردیکه کامپیوتر موجود در شبکه داخلی، قصد ارسال اطلاعاتی را برای خارج از شبکه خصوصی داشته باشند، نیز صدق می کند.

بهینه سازی استفاده از فایروال

فایروال ها را می توان با توجه به اهداف سازمانی بصورت کاملا" سفارشی نصب و پیکربندی کرد. در این راستا امکان اضافه و یا حذف فیلترهای متعدد بر اساس شرایط متفاوت وجود خواهد داشت:

- **آدرس های IP** . هر ماشین بر روی اینترنت دارای یک آدرس منحصر بفرد با نام IP است . IP یک عدد ۳۲ بیتی بوده که بصورت چهار عدد دهدهی که توسط نقطه از هم جدا می گردند نمایش داده می شود (Octet) . در صورتیکه یک آدرس IP خارج از شبکه، فایل های زیادی را از سرویس دهنده می خواند (ترافیک و حجم عملیات سرویس دهنده را افزایش خواهد داد) فایروال می تواند ترافیک از مبداء آدرس فوق و یا به مقصد آدرس فوق را بلاک نماید.
- **اسامی دامنه ها (حوزه)**. تمام سرویس دهندگان بر روی اینترنت دارای اسامی منحصر بفرد با نام " اسامی حوزه" می باشند. یک سازمان می تواند با استفاده از فایروال، دستیابی به سایت هائی را غیرممکن و یا صرفا" امکان استفاده از یک سایت خاص را برای پرسنل خود فراهم نماید.

- **پروتکل ها** . پروتکل نحوه گفتگوی بین سرویس دهنده و سرویس گیرنده را مشخص می نماید . پروتکل های متعدد با توجه به اهداف گوناگون در اینترنت استفاده می گردد. مثلا" http پروتکل وب و Ftp پروتکل مربوط به دریافت و یا ارسال فایل ها است. با استفاده از فایروال می توان، میدان فیلتر نمودن را بر روی پروتکل ها متمرکز کرد. برخی از پروتکل های رایج که می توان بر روی آنها فیلتر اعمال نمود بشرح زیر می باشند:

- Internet Protocol(IP). پروتکل اصلی برای عرضه اطلاعات بر روی اینترنت است.
- Transport Control Protocol (TCP). مسئولیت تقسیم یک بسته اطلاعاتی به بخش های کوچکتر را دارد.
- Hyper Text Transfer Protocol (HTTP). پروتکل فوق برای عرضه اطلاعات در وب است.
- File Transfer Protocol (FTP). پروتکل فوق برای دریافت و ارسال فایل ها استفاده می گردد.
- Protocol User Datagram(UDP) . از پروتکل فوق برای اطلاعاتی که به پاسخ نیاز ندارند استفاده می شود(پخش صوت و تصویر)
- Internet control Message Protocol (ICMP). پروتکل فوق توسط روترها و بمنظور تبادل اطلاعات فی المابین استفاده می شود.
- Simple Mail Transfer Protocol(SMTP). از پروتکل فوق برای ارسال e-mail استفاده می گردد.
- Simple Network Management Protocol (SNMP).از پروتکل فوق بمنظور اخذ اطلاعات از یک کامپیوتر راه دور استفاده میشود

- Telnet . برای اجرای دستورات بر روی یک کامپیوتر از راه دور استفاده می گردد.

- **پورت ها** . هر سرویس دهنده ، خدمات مورد نظر خود را با استفاده از پورت های شماره گذاری شده بر روی اینترنت ارائه می دهد. مثلا" سرویس دهنده وب اغلب از پورت ۸۰ و سرویس دهنده Ftp از پورت ۲۱ استفاده می نماید. یک سازمان ممکن است با استفاده از فایروال امکان دستیابی به پورت ۲۱ را بلاک نماید.

- **کلمات و عبارات خاص** . می توان با استفاده از فایروال کلمات و یا عباراتی را مشخص نمود تا امکان کنترل بسته های اطلاعاتی حاوی کلمات و عبارات فراهم گردد. هر بسته اطلاعاتی که حاوی کلمات مشخص شده باشد توسط فایروال بلاک خواهد شد.

همانگونه که اشاره شد فایروال ها به دو صورت نرم افزاری وسخت افزاری استفاده می گردند.فایروال های نرم افزاری بر روی کامپیوتری نصب می گردند که خط اینترنت به آنها متصل است. کامپیوتر فوق بمنزله یک Gateway رفتار می نماید چون تنها نقطه قابل تماس، بمنظور ارتباط کامپیوتر و اینترنت است. زمانیکه فایروال بصورت سخت افزاری در نظر گرفته شود، تمام بخش فوق بصورت Gateway خواهد بود. امنیت فایروال های سخت افزاری بمراتب بیشتر از فایروال های نرم افزاری است.

تهدیدات

حمله کنندگان به شبکه های کامپیوتری از روش های متعددی استفاده می نمایند.

- **Remote Login** . امکان برقراری ارتباط با کامپیوتر و کنترل آن توسط فرد غیرمجاز است . دامنه عملیات فوق می تواند از مشاهده و دستیابی به برخی از فایل ها تا اجرای برخی برنامه ها بر روی کامپیوتر باشد.

- **Backdoors Application** . برخی از برنامه ها دارای امکانات ویژه ای برای دستیابی از راه دور می باشند. برخی دیگر از برنامه ها دارای اشکالاتی بوده بگونه ای که یک Backdoor را ایجاد و یا امکان دستیابی مخفی را ارائه می دهند. در هر حالت امکان کنترل برنامه فراهم خواهد گردید.
- **hijacking SMTP session** . پروتکل SMTP رایج ترین روش برای ارسال e-mail است. با دستیابی به لیستی از آدرس های e-mail ، یک شخص قادر به ارسال e-mail به هزاران کاربر دیگر خواهد شد.
- **اشکالات سیستم های عامل** . سیستم های عامل نظیر سایر برنامه های کاربردی ممکن است دارای Backdoors باشند.
- **انفجار E-mail** . یک شخص قادر به ارسال صدها و هزاران e-mail مشابه در مقاطع زمانی متفاوت است. با توجه به وضعیت فوق سیستم پست الکترونیکی قادر به دریافت تمام نامه های ارسالی نخواهد بود.
- **ماکرو**. اغلب برنامه های کاربردی این امکان را برای کاربران خود فراهم می نمایند که مجموعه ای از اسکریپت ها را بمنظور انجام عملیات خاصی نوشته و نرم افزار مربوطه آنها را اجراء نماید. اسکریپت های فوق " ماکرو " نامیده می شوند. حمله کنندگان به شبکه های کامپیوتری با آگاهی از واقعیت فوق، اقدام به ایجاد اسکریپت های خاص خود نموده که با توجه به نوع برنامه ممکن است داده ها را حذف و یا باعث از کار افتادن کامپیوتر گردند.

سرویس دهنده Proxy

سرویس دهنده Proxy اغلب با یک فایروال ترکیب می گردد. سرویس دهنده Proxy بمنظور دستیابی به صفحات وب توسط سایر کامپیوترها استفاده می گردد. زمانیکه کامپیوتری درخواست یک صفحه وب را می نماید، صفحه مورد نظر توسط سرویس

دهنده Proxy بازیابی و در ادامه برای کامپیوتر متقاضی ارسال خواهد شد. بدین ترتیب تمام ترافیک (درخواست و پاسخ) بین درخواست کننده یک صفحه وب و پاسخ دهنده از طریق سرویس دهنده Proxy انجام می گیرد.

سرویس دهنده Proxy می تواند کارائی استفاده از اینترنت را افزایش دهد. پس از دستیابی به یک صفحه وب، صفحه فوق بر روی سرویس دهنده Proxy نیز ذخیره (Cache) می گردد. در صورتیکه در آینده قصد استفاده از صفحه فوق را داشته باشید صفحه مورد نظر از روی سرویس دهنده Proxy در اختیار شما گذاشته می شود (الزامی به برقراری ارتباط مجدد و درخواست صفحه مورد نظر نخواهد بود)

فایروال (قسمت دوم)

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند.علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۱- توانایی ثبت و اخطار: ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می شود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲- بازدید حجم بالایی از بسته های اطلاعات: یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر

کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۳- سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه های می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

٤- امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال: اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی: یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

تفاوت در کارایی انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم، انجام می دهند، اما روش انجام کار توسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود. بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

۱- فایروالهای سطح مدار (Circuit-Level): این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲- فایروالهای پروکسی سرور: فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۳- فیلترهای Nosstateful packet : این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد

با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

٤- فیلترهای Stateful Packet : این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانندعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

٥- فایروالهای شخصی : فایروالهای شخصی، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند. آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات

ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از:

- موقعیت و محل نصب از لحاظ توپولوژیکی : معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.
- قابلیت دسترسی و نواحی امنیتی: اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی وتنظیم فایروال جهت صدور اجازه به کاربران

خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

ü مسیریابی نامتقارن : بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.

ü فایروالهای لایه ای : در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد.معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

Tools security

Ethereal

قسمت اول

Ethereal ابزاری کد-باز و رایگان است، که آن‌را می‌توان در دسته‌ی Snifferها جای داد. این نرم‌افزار با توجه به ویژگی‌هایش، یکی از متداول‌ترین ابزارهای آنالیز ترافیک شبکه است، هرچند که در حال حاضر، با وجود گذشت زمان نسبتاً زیادی از معرفی آن، هنوز در مرحله‌ی تست قرار داشته و در زمان نگارش این مطلب آخرین نگارش آن نگارش 0.10.4 است که از پایگاه www.ethereal.com قابل دریافت است. لازم به ذکر است که سورس این نرم‌افزار را نیز می‌توانید از همین آدرس دریافت کنید.

این نرم‌افزار نیز مانند WinDump، پس از نصب، از کتابخانه‌ی Winpcap برای دریافت اطلاعات بسته‌ها استفاده می‌کند، لذا پیش از نصب Ethereal، آخرین نسخه‌ی نرم‌افزار Winpcap را نصب کنید. همان‌طور که گفته شد این بسته امکان دریافت بسته‌ها و استخراج اطلاعات از آن‌ها را، تحت سیستم‌عامل Windows، فراهم می‌کند.

اگر برای اولین بار است که قصد نصب و کار با این دسته از نرم‌افزارها (Snifferها) را دارید، پیش‌نهاد می‌کنیم ابتدا قسمت اول مقاله‌ی مربوط به WinDump را، که به مقدمه‌یی در باب Snifferها پرداخته است، مطالعه کنید.

Ethereal، به عنوان نمونه‌یی از یک Sniffer، وظیفه‌ی ثبت رخدادها، اطلاعات و بسته‌های رد و بدل شده بر روی لایه‌های شبکه را بر عهده دارد. با ثبت داده‌های در حال انتقال بر روی شبکه و تجزیه‌ی آنها، می‌توان بسته‌های اطلاعاتی مربوط به پروتکل‌های

متفاوت را از یکدیگر تفکیک نمود و ارتباطات مجزا را شناسایی نمود. همان‌گونه که در معرفی این دسته از نرم‌افزارها گفته شد، این قبیل تحلیل‌ها، می‌توانند به شناسایی ارتباطات خطرناک، تلاش‌های پیاپی برای دست‌یابی به منابع شبکه و نفوذ به آن و یا از کار انداختن نرم‌افزارها و سخت‌افزارها فعال بر روی شبکه، بیانجامد. با این وجود از آنجاکه خروجی این دسته از نرم‌افزارها به حدی پیچیده‌اند که کاربران عادی قادر به تحلیل آنها نیستند، لذا این‌گونه نتیجه‌گیری‌ها و تحلیل‌ها عموماً توسط متخصصین شبکه انجام می‌پذیرد.

نرم‌افزار Ethereal بر روی سه بستر اصلی Windows، Linux و Solrais ارایه می‌شود که نسخه‌یی که ما بررسی می‌کنیم، نسخه‌ی تحت Windows آن است.

توانایی‌های این دسته از ابزارها را عموماً می‌توان به بخش‌های زیر تقسیم کرد:

- انواع پروتکل‌ها و انواع رابط‌های شبکه‌یی که توسط ابزار شناسایی شده و تفکیک می‌گردند.
- روش‌ها و قالب‌های ذخیره‌سازی خروجی برداشت و تحلیل اطلاعات شبکه
- امکان بازخوانی اطلاعات ذخیره شده توسط نرم‌افزارهای Sniffer مشابه دیگر
- امکان استفاده از فلیتر برای پروتکل‌های مختلف
- قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متنوع

البته ساده‌گی کار با نرم‌افزار، به عنوان قابلیت‌های ویژه‌ی رابط کاربری، نیز یکی دیگر از قابلیت‌هایی است که اغلب برای کاربران نیمه‌حرفه‌یی و مبتدی اهمیت ویژه‌یی دارد.

قابلیت‌های خاص Ethereal را، با توجه به تقسیم‌بندی فوق، می‌توان به شرح دسته‌بندی نمود :

- شناسایی پروتکل‌ها و رابط‌های شبکه‌ی متنوع

این نرم‌افزار قابلیت شناسایی حدود ۵۰۰ نوع پروتکل مجزا را دارد. تنوع این پروتکل‌ها به این نرم‌افزار قدرتی ویژه بخشیده است.

از باب ارتباطات نیز این نرم‌افزار قابلیت دریافت اطلاعات بسته‌های فعال ارتباطات Ethernet، FDDI، Token-Ring، IEEE 802.11، IP over ATM و رابط‌های loopback را دارد.

- ذخیره‌سازی اطلاعات

Ethereal با ایجاد فایل‌های خروجی قابل ویرایش در قالب‌های lippcap(tcpdump)، Sun snoop، Microsoft Network Monitor و Network Associate Sniffer از نظر ذخیره‌سازی اطلاعات نیز ابزاری قدرت‌مند محسوب می‌شود.

- سازگاری با خروجی نرم‌افزارها و سیستم‌های دیگر

Ethereal قابلیت بازخوانی پرونده‌های اطلاعاتی نرم‌افزارهای مشابه دیگری همچون TCPDump، NAI's Sniffer & Sniffer Pro، NetXray، MS Network Monitor، Novell LANanalyser، Cisco Secure IDS iplog و غیره را دارد.

- فیلترها

این ابزار، با محدود سازی روش دریافت و تحلیل اطلاعات جمع‌آوری شده از بسته‌ها، در بسیاری از حالات امکان استفاده از فیلترهای پرقدرتی را به کاربر

می‌دهد. در عین حال با استفاده از این فیلترهای می‌توان به جست‌وجوی بسته‌ها در میان اطلاعات ذخیره شده نیز پرداخت.

- قابلیت‌ها رابط کاربری

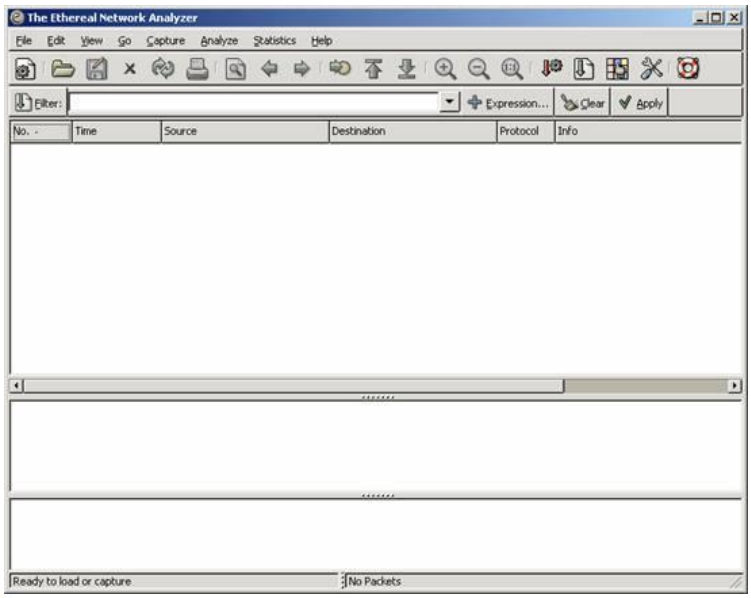
رنگ‌های متنوع برای تغییر روش نمایش اطلاعات بسته به فیلتر انتخاب شده، منوهای متنوع و دیگر امکانات رابط کاربری، که بیشتر در بخش‌ها آتی در حین معرفی چگونگی استفاده از این نرم‌افزار به آنها اشاره خواهیم کرد، به تحلیل و شناسایی بسته‌ها کمک شایانی می‌کند. همان‌طور که ذکر شد، این قابلیت جذابیت ویژه‌یی برای کاربران مبتدی و نیمه‌حرفه‌یی دارد.

در قسمت بعد به بررسی مقدماتی روش‌های استفاده از این نرم‌افزار و ارایه‌ی مثال‌هایی در این باب خواهیم پرداخت

Ethereal قسمت دوم

در قسمت اول، ضمن ارایه‌ی جمع‌بندی در مورد Snifferها، که Ethereal یکی از معروف‌ترین و قدرتمندترین نرم‌افزارهای این دسته از ابزارهاست، به ویژگی‌های برجسته‌ی این نرم‌افزار اشاره کردیم. بررسی قابلیت‌های این نرم‌افزار بر اساس جنبه‌های مختلف و متنوعی صورت گرفت که در مورد این دسته از ابزارها مد نظر قرار می‌گیرد.

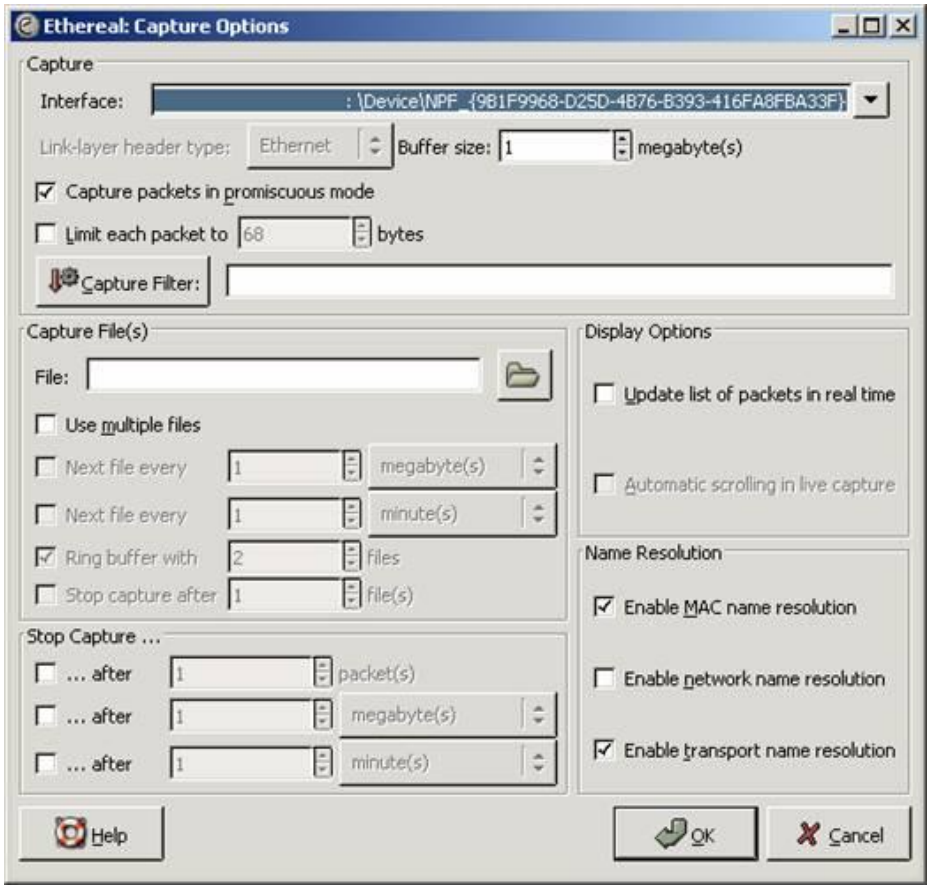
شکل زیر، رابط کاربری این نرم‌افزار پیش از شروع عملیات را نشان می‌دهد:



همان‌گونه که مشاهده می‌کنید، رابط کاربری این نرم‌افزار بسیار شبیه به رابط‌های گرافیکی متداول سیستم‌های عامل Linux است، محیط‌هایی همچون KDE و GNOME.

در منوی فایل، می‌توان خروجی عملیات انجام شده را در قالب‌های مختلف درون فایل ذخیره کرد یا فایل‌های ذخیره شده در قالب‌های مختلف، ایجاد شده توسط نرم‌افزارهای گوناگون، را باز کرد و تحلیل نمود.

شروع عمکرد این نرم‌افزار با استفاده از منوی Capture صورت می‌گیرد. شکل زیر صفحه‌ی مربوط به این منو را نشان می‌دهد:



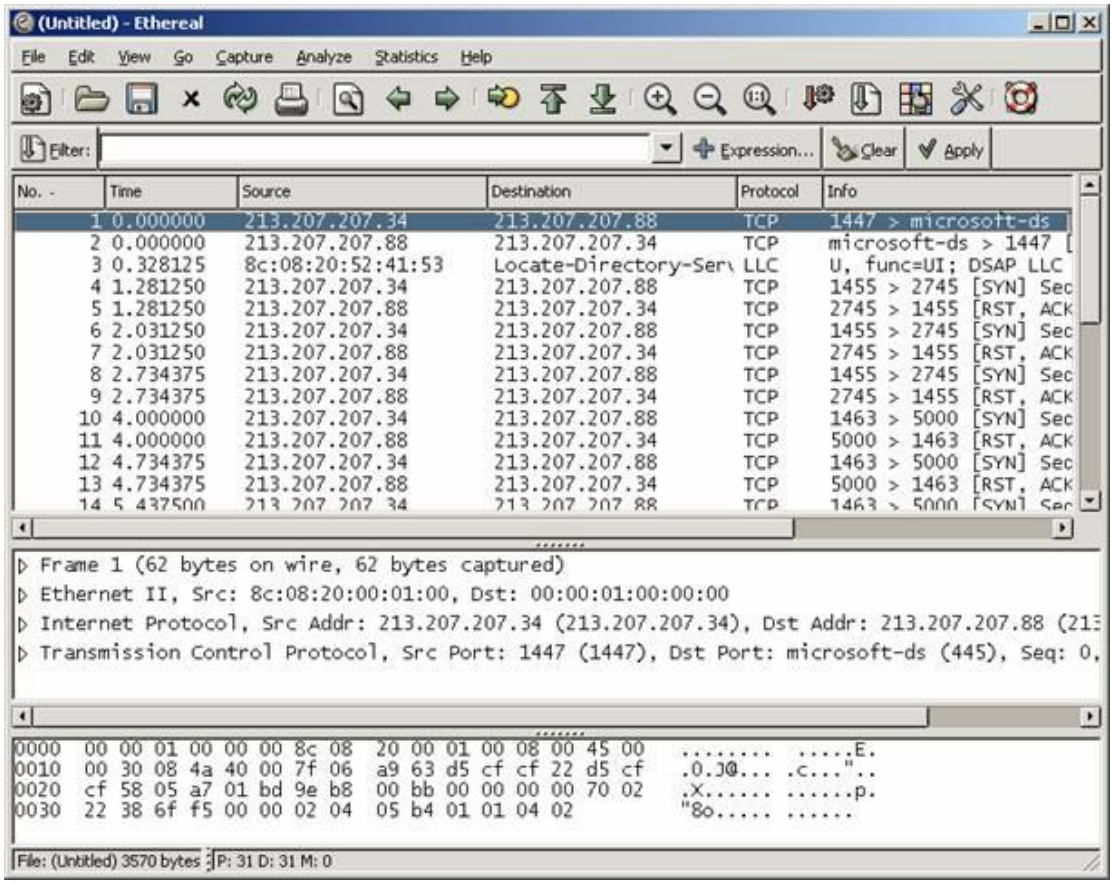
در قسمت بالا، رابط شبکه‌یی که عملیات دریافت بسته‌ها بر روی آن انجام می‌گیرد مشخص می‌شود. این رابط شبکه می‌تواند به ارتباط مودم ما با اینترنت نیز اشاره کند. به عبارت دیگر توسط چنین نرم‌افزارهایی، می‌توان به بررسی وضعیت ارسال و دریافت بسته‌ها و تحلیل آن‌ها در ارتباطات میان مودم‌ها و ارایه‌کننده‌گان سرویس اینترنت نیز پرداخت. خروجی این عملیات می‌تواند اطلاعات مفیدی از حملات احتمالی در حال انجام به سیستم ما را نشان دهد.

قسمت‌های دیگر این صفحه شامل تعیین نام فایلی که بسته‌های دریافت شده در آن‌ها قرار می‌گیرد و همچنین شرایط که در صورت حصول آن‌ها عمل Capture خاتمه می‌پذیرد. سمت راست این صفحه نیز یکی از ویژه‌گی‌های مهم عمل Capture را تعیین می‌کند که تعیین نام مترادف آدرس‌ها در شبکه است. این عمل، ضمن آن‌که اطلاعات جامع و مفیدی را در اختیار ما قرار می‌دهد، عمل دریافت و جمع‌آوری بسته‌ها را کند می‌کند.

شکل زیر، وضعیت پس از آغاز عملیات Capture را نشان می‌دهد. رابط شبکه‌ی مورد استفاده، ارتباط PPP برقرار شده است :

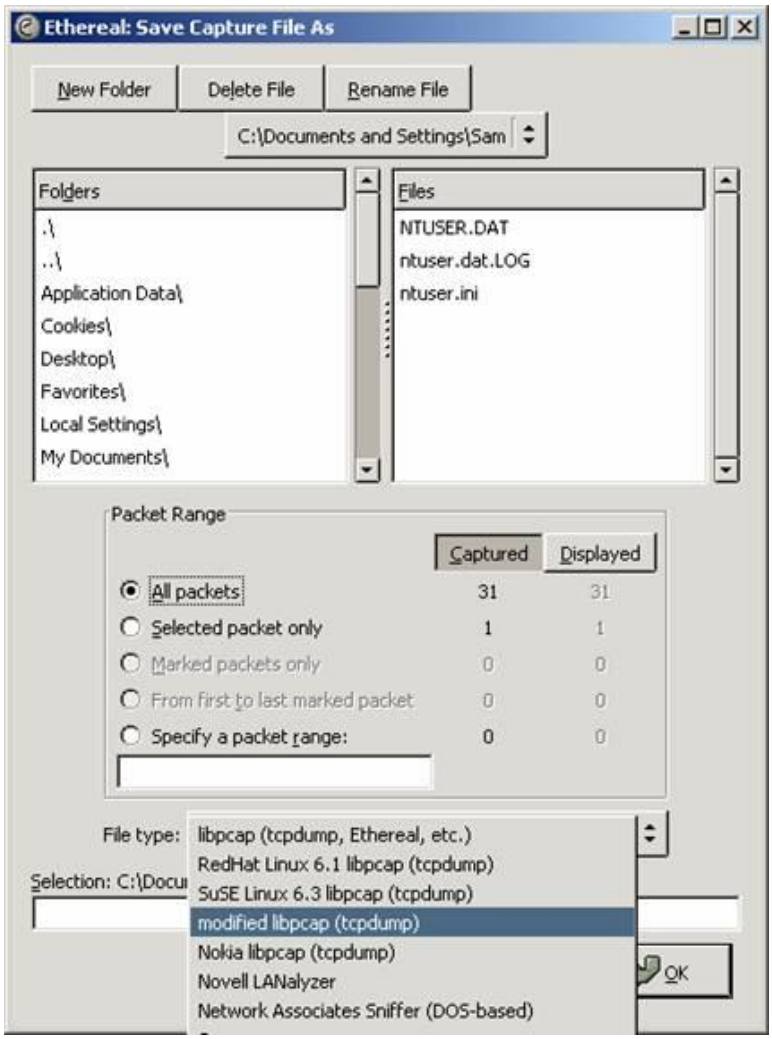
همان‌گونه که در شکل نیز مشخص است، انواع پروتکل‌ها در خروجی مورد نظر دسته‌بندی شده‌اند و در مقابل نام آنها تعداد دریافت شده از آن پروتکل درج می‌شود.

پس از قطع عمل Capture، فهرستی از بسته‌های دریافت شده در پنجره‌ی اصلی نمایش داده می‌شود :



بسته‌های دریافت شده، به ترتیب و بر اساس زمان دریافت مرتب شده‌اند. این فهرست شامل شماره‌ی بسته، زمان دریافت/ارسال آن، آدرس‌های مبدأ و مقصد و نوع بسته نمایش داده شده است. در قسمت پایین‌تر، نوع بسته و اطلاعاتی که از ابتدای بسته استخراج شده‌اند، مانند مبدأ و مقصد، پورت و دیگر اطلاعات درج می‌شود و در قسمت پایین پنجره‌ی اصلی محتوای خام بسته نمایش داده شده است.

خروجی به دست آمده را می‌توان با تعیین قالب مورد نظر برای دسترسی‌های آتی ذخیره نمود. شکل زیر صفحه‌یی که در آن امکان ذخیره سازی پرونده با تعیین قالب مورد نظر وجود دارد را نشان می‌دهد :



شکل بالا، تعدادی از قالب‌های قابل استفاده برای ذخیره‌ی پرونده توسط این نرم‌افزار را نشان می‌دهد. انواع این قالب‌ها در قسمت اول از بررسی این نرم‌افزار معرفی شده‌اند.

در قسمت بعدی از بررسی این نرم‌افزار به روش تعریف فیلترها و چگونه‌گی جستجو و تحلیل در بسته‌های دریافت/ارسال شده، با استفاده از فایل‌های پیشین ذخیره شده، خواهیم پرداخت.

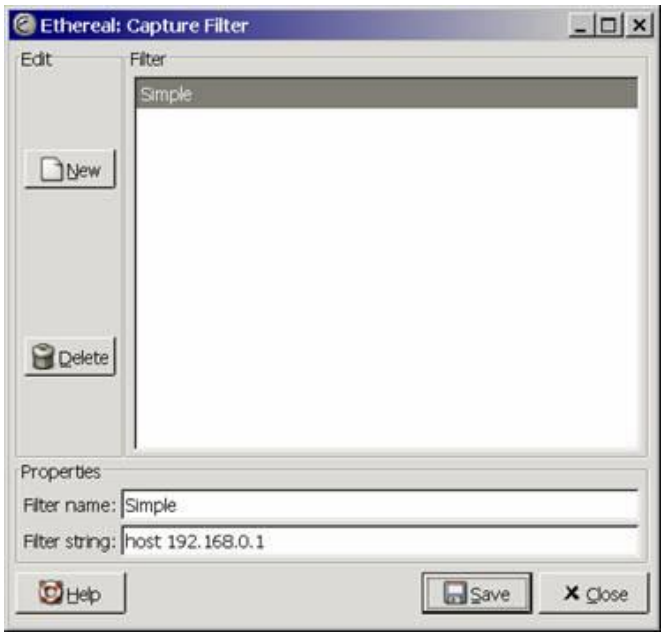
قسمت سوم

در دو قسمت پیشین، ضمن تعریف ابزارهای Sniffer، به معرفی یکی از متداول‌ترین آن‌ها، یعنی Ethereal پرداختیم. در این قسمت، به معرفی امکان استفاده از Filterهای این نرم‌افزار، و چگونه‌گی انجام تحلیل بر اساس خروجی‌های به‌دست آمده می‌پردازیم.

در این نرم‌افزار، عملاً سه نوع فیلتر قابل تعریف است:

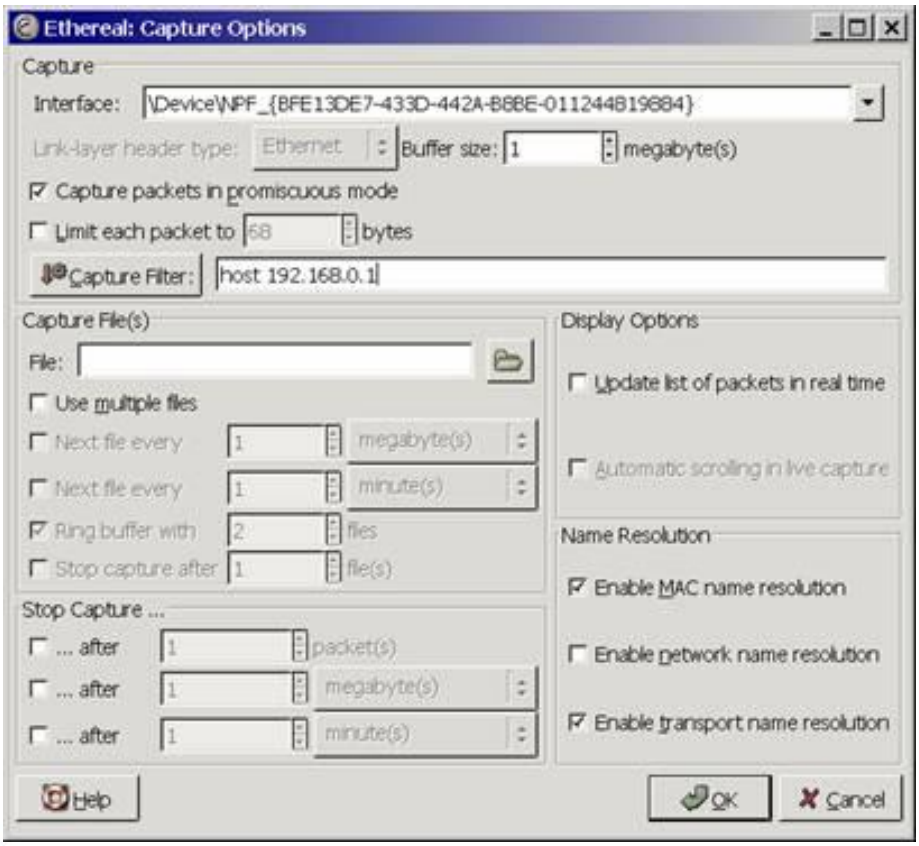
- فیلترهای Capture
- فیلترهای نمایش
- فیلترهای رنگی

برای استفاده از فیلترهای Capture، در منوی Capture، گزینه‌ی Capture Filters را انتخاب می‌کنیم. پنجره‌یی به شکل زیر باز می‌شود:



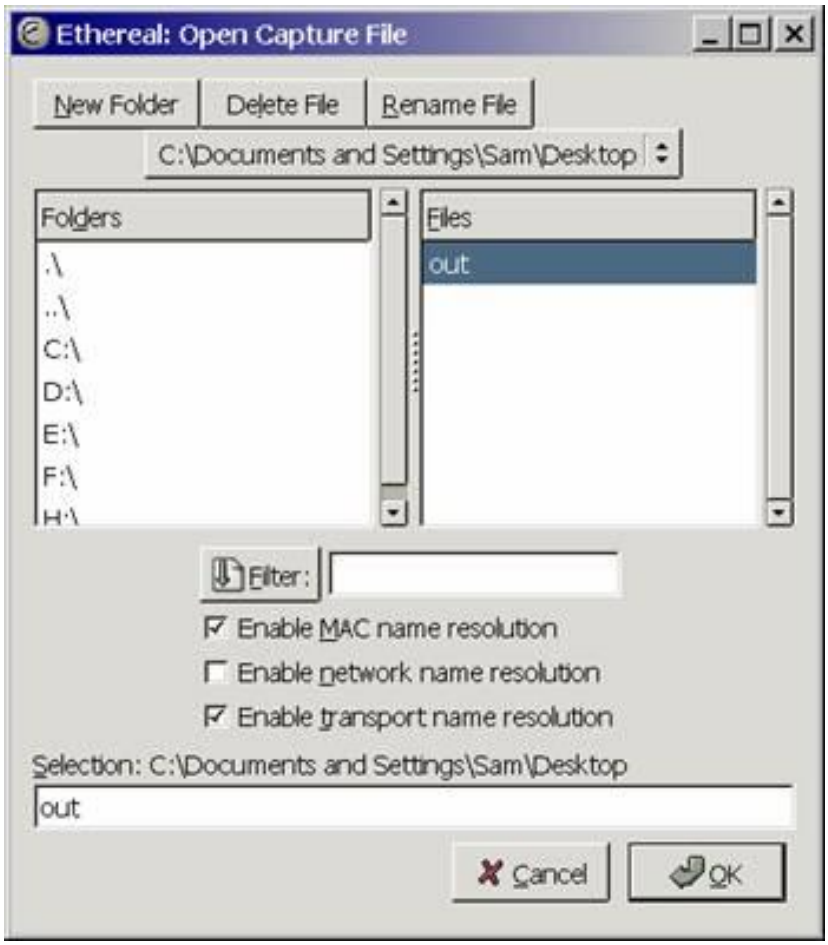
با انتخاب گزینه‌ی New، فیلتر جدیدی تعریف می‌کنیم.

این نرم‌افزار برای تعریف فیلتر رابط کاربری به‌صورت گرافیکی ندارد، لذا با استفاده از گزینه‌ی Help در پایین همین پنجره، می‌توان از روش تعریف فیلترها به‌صورت متنی آگاه شد. در این مثال، فیلتری به نام Simple تعریف می‌کنیم که توسط آن، Ethereal تنها به دریافت بسته‌هایی مبادرت می‌کند که آدرس فرستنده آن 192.168.0.1 باشد. فیلتر را ذخیره می‌کنیم پنجره را می‌بندیم. اکنون عمل Capture را آغاز می‌کنیم:

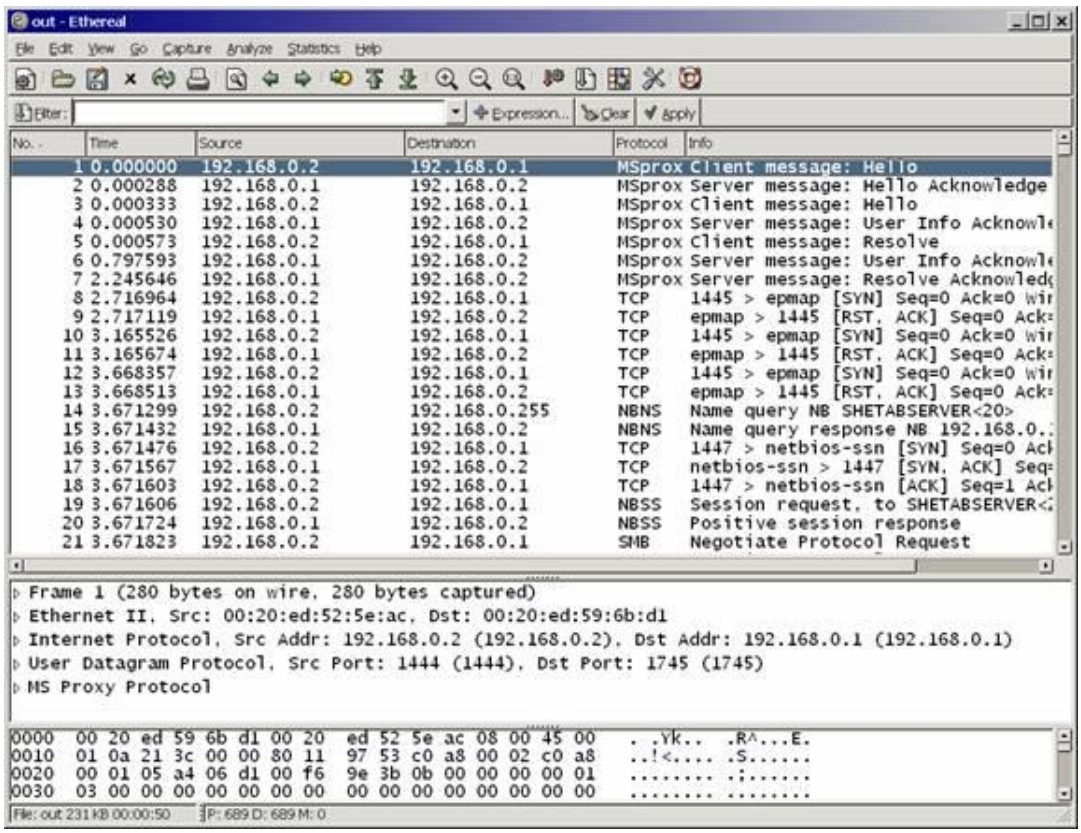


همان‌گونه در شکل بالا مشخص است، در قسمت Capture Filters می‌توان فیلتری را تعریف کرد و یا از فیلترهای تعریف شده‌ی پیشین استفاده کرد. پس از انجام عمل Capture، Ethereal تنها بسته‌هایی را دریافت خواهد کرد که آدرس مبدأ آنها 192.168.0.1 باشد.

برای استفاده از فیلترهای نمایشی، می‌توان از خروجی‌های پیشین و عملیات Capture قبلی استفاده کرد. به این منظور یکی از پرونده‌های قبلی را باز می‌کنیم:

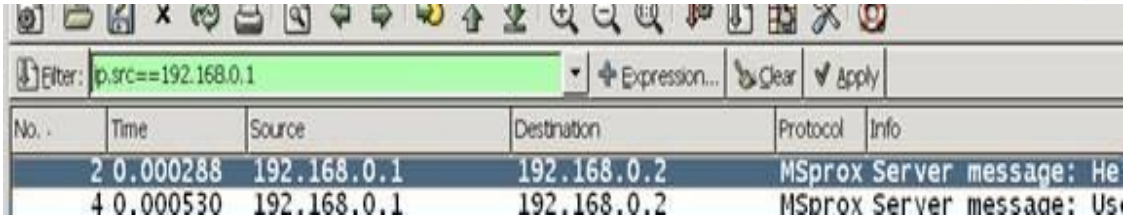


این پرونده به‌عنوان نمونه‌یی از عمل دریافت بسته‌ها تهیه شده است. پس از باز کردن این پرونده، بسته‌های موجود در آخرین عمل دریافت، در پنجره‌ی اصلی ظاهر خواهند شد:



طبیعی‌ست که برای دسته‌بندی بسته‌ها بر اساس یکی از پارامترهای زمان دریافت، آدرس مبدأ یا مقصد و نوع پروتکل می‌توان به کلیک کردن بر روی برچسب هریک از ستون‌ها، اطلاعات را بر حسب آن ستون مرتب‌کرد. عمل تعریف فیلتر و اعمال آن بر روی اطلاعات، متفاوت از این مرتب‌سازی است. به بیان دیگر، با استفاده از فیلتر می‌توان شروط پیچیده‌تری برای مشاهده‌ی بسته‌ها تعریف کرد.

اکنون می‌خواهیم با استفاده از تعریف فیلترها نمایش در این نرم‌افزار، بسته‌های مورد نظر خود را جدا کنیم. برای این‌کار می‌توان فیلتر را مستقیماً در قسمت **Filter**، پایین Toolbar اصلی، در پنجره‌ی اصلی تعریف کرد:

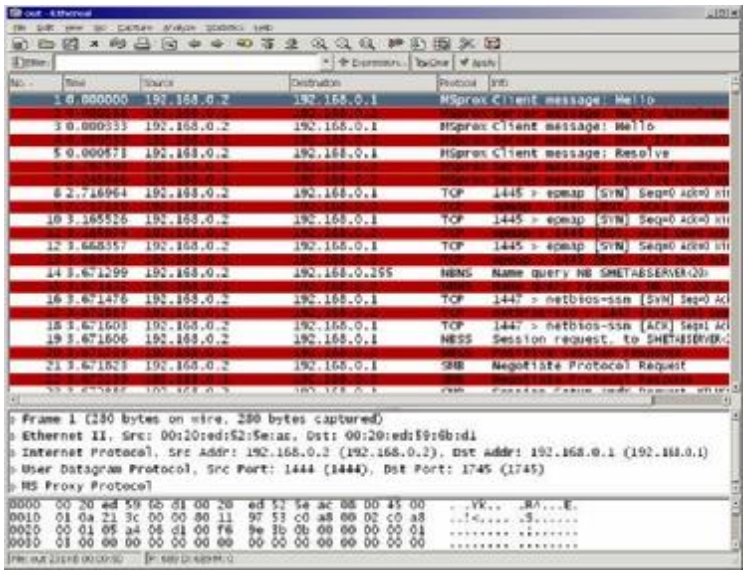


همان‌گونه که مشاهده می‌کنید، در این محل، برای تعریف فیلتری که تنها بسته‌هایی با مبدأ 192.168.0.1 را نمایش دهد از نوع دیگری از تعریف فیلتر استفاده می‌کنیم. به بیان دیگر، زبان تعریف فیلتر برای دو نوع Capture و نمایش (Analyze) با یکدیگر متفاوت است. با مراجعه به سایت این نرم‌افزار، می‌توانید با هر دو زبان آشنا شوید.

روش دیگر استفاده از فیلترهای نمایش استفاده از منوی Analyze و انتخاب Display Filters در این منو است. با این انتخاب پنجره‌ای مشابه پنجره‌ی Capture Filters نمایش داده می‌شود:

در مثال بالا، مجدداً فیلتری، از نوع نمایشی، با نام Simple تعریف کرده‌ایم که زبان تعریف آن همان زبان فیلترهای نمایش است. با فشار دکمه‌ی Apply، فیلتر مورد نظر اعمال می‌شود و شکل پنجره‌ی اصلی تنها بسته‌های با آدرس مبدأ 192.168.0.1 را نمایش می‌دهد. باید توجه داشت که بقیه‌ی بسته‌ها در این مرحله از میان نمی‌روند و استفاده از فیلترها تنها نمایش را به بازه‌ی مورد درخواست کاربر محدود می‌کند.

از دیگر قابلیت‌های مفید این نرم‌افزار، فیلترهای رنگی آن است. این فیلترها را می‌توان در منوی View با انتخاب Coloring Rules تعریف کرد. زبان و روش تعریف این فیلترها مشابه فیلترهای نمایش است. شکل زیر پنجره‌ی اصلی را پس از تعیین فیلتر رنگی ip.src=192.168.0.1 و تغییر رنگ بسته‌هایی که آدرس مبدأ آنها 192.168.0.1 است، نشان می‌دهد :



طبیعی است که می‌توان از چند فیلتر رنگی به‌طور هم‌زمان استفاده کرد.

با توجه به سه قسمت ارایه شده در باب معرفی این نرم‌افزار که حاکی از قابلیت‌ها متنوع آن است، Ethereal را می‌توان به جرأت قدرت‌مندترین نرم‌افزار از سری ابزارهای Sniffer به حساب آورد. لازم به ذکر است که این ابزار امکانات دیگری نیز دارد که با مراجعه به منوهای Analyze و Statistics می‌توانـــید از آن‌ها استفاده کنید.

Tools security

SuperScan

قسمت اول

یکی از اولین قدم ها برای تعیین میزان آسیب‌پذیری یک سیستم رایانه‌یی، استفاده از ابزارها و روش‌هایی است که به ما امکان می دهد خود به بررسی وضعیت امنیتی سیستم، از دید یک کاربر بیرونی، و در برخی شرایط از دید یک نفوذگر به شبکه و سیستم‌های رایانه‌یی، بپردازیم. به عبارت دیگر، چنانچه امکان بررسی وضعیت امنیتی سیستم مان، با چنین روش‌هایی وجود داشته باشد، چاره‌اندیشی برای مقابله با شرایط خطیر و برطرف نمودن ضعف‌های سیستم، آسان می‌شود.

در معرفی ابزارهای گوناگون در این بخش، جدا از معرفی ابزارهایی که به‌محافظت در برابر حملات احتمالی به سیستم‌مان به ما یاری می‌رسانند، تاکنون نرم‌افزارهایی را نیز معرفی کرده‌ایم که امکان بررسی وضعیت امنیتی سیستم مورد نظر را فراهم می‌کنند. در این دسته از نرم‌افزارها، پویش‌گرهای امنیتی، به عنوان راه‌کارهای جامعی که به کلیه‌ی ابعاد امنیتی یک سیستم می‌پردازند جای‌گاهی ویژه دارند. همان‌گونه که در مرورهای پیشین مشاهده کرده‌اید، هدف از استفاده از این پویش‌گرها، مجتمع‌سازی امکان بررسی امنیتی یک سیستم، بدون نیاز به استفاده از چند ابزار هم‌زمان است. در پویش‌گرهای امنیتی، وضعیت امنیتی سیستم از ابعاد مختلفی همچون پویش سیستم‌های موجود بر روی شبکه، تعیین سیستم‌های‌عامل موجود، وضعیت اصلاحیه‌های امنیتی، وضعیت درگاه‌های باز و غیره بررسی می‌گردد.

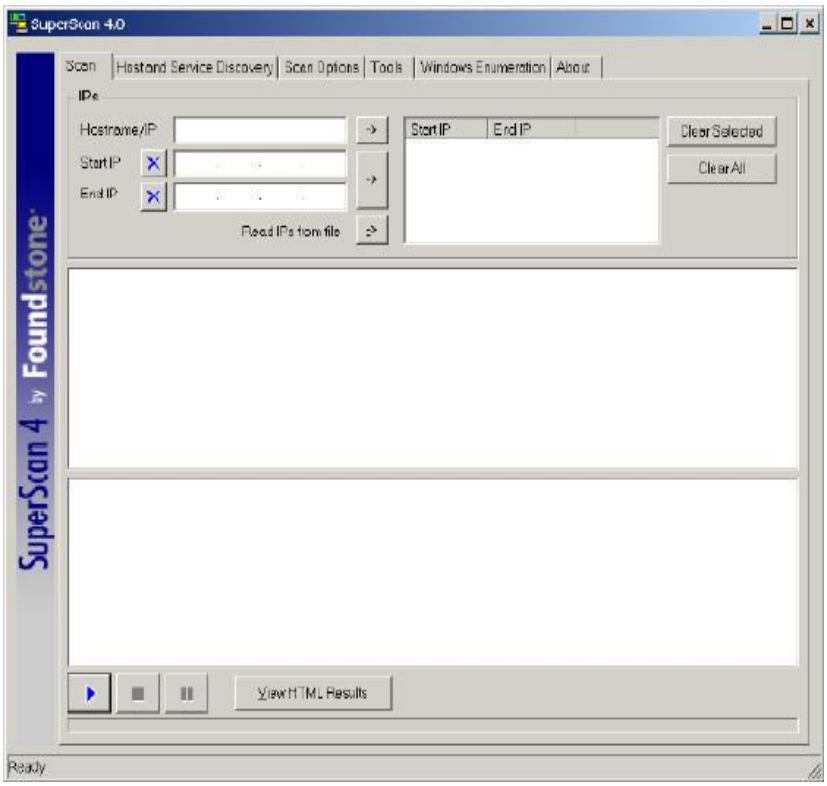
با وجود امکان استفاده از این دسته از پویش‌گرها امنیتی، در مواردی که تنها به پویش وضعیت امنیتی یک سیستم، از جنبه‌یی خاص، داریم، می‌توانیم تنها از دسته‌یی از نرم‌افزارها استفاده کنیم که بررسی امنیتی را به ابعادی خاص محدود می‌کنند. برای مثال یک پویش‌گر درگاه (که در این متن قصد معرفی یکی از متداول‌ترین نرم‌افزارهای این دسته ابزارها را داریم)، تنها به بررسی بازبودن درگاه‌های یک سیستم می‌پردازد.

پویش‌گرهای درگاه، به‌همراه پویش‌گرهای آدرس، دو دسته ابزاری هستند که اغلب توسط نفوذگران، برای بررسی اولیه‌ی وضعیت سیستم مورد نظر استفاده می‌گردند. از آن‌جایی که ارتباطات مبتنی بر پروتکل TCP/IP بر اساس شماره‌ی درگاه TCP/UDP مورد نظر انجام می‌گیرد، لذا هر درگاه عملاً نماینده‌ی نرم‌افزار خاصی است. برای مثال درگاه استاندارد Web Serverها درگاه شماره‌ی 80 است، لذا در صورتی که نفوذگر از باز بودن این درگاه مطلع شود، می‌تواند نوع Web Server را نیز مشخص کرده و با اطلاعاتی که در مورد ضعف‌های امنیتی آن دارد به حمله از طریق این درگاه مبادرت نماید. روند کار در مورد دیگر درگاه‌ها نیز مشابه است.

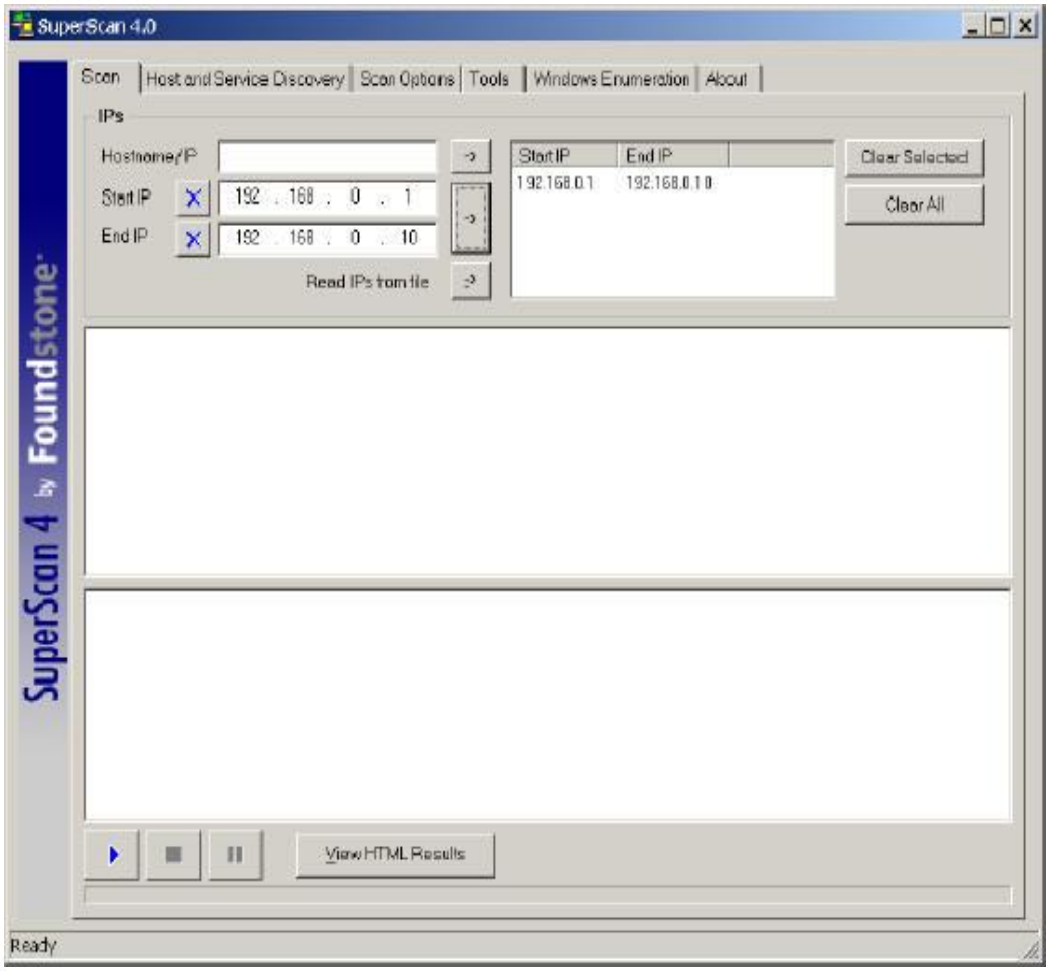
با توجه به اهمیتی که درگاه‌های باز روی سیستم در بالا رفتن خطر حملات دارند، یکی از قدم‌های اولیه برای تعیین میزان امنیت کنونی سیستم، اطلاع یافتن از درگاه‌های باز است. همان‌گونه که گفته شد، این نوع پویش قسمتی از وظایف پویش‌گرهای امنیت است و در صورت استفاده از آنها می‌توان برای اطلاع یافتن از وضعیت درگاه‌های باز، به گزارش‌های حاصل از پویش جزئی‌ی این نرم‌افزارهای رجوع کرد.

برای پویش درگاه‌های یک سیستم نرم‌افزارهای متعددی وجود دارند که نرم‌افزار SuperScan یکی از متداول‌ترین این ابزارهاست. این نرم‌افزار که محصول شرکت Foundstone است و امکان پویش آدرس‌های IP را نیز دارد،

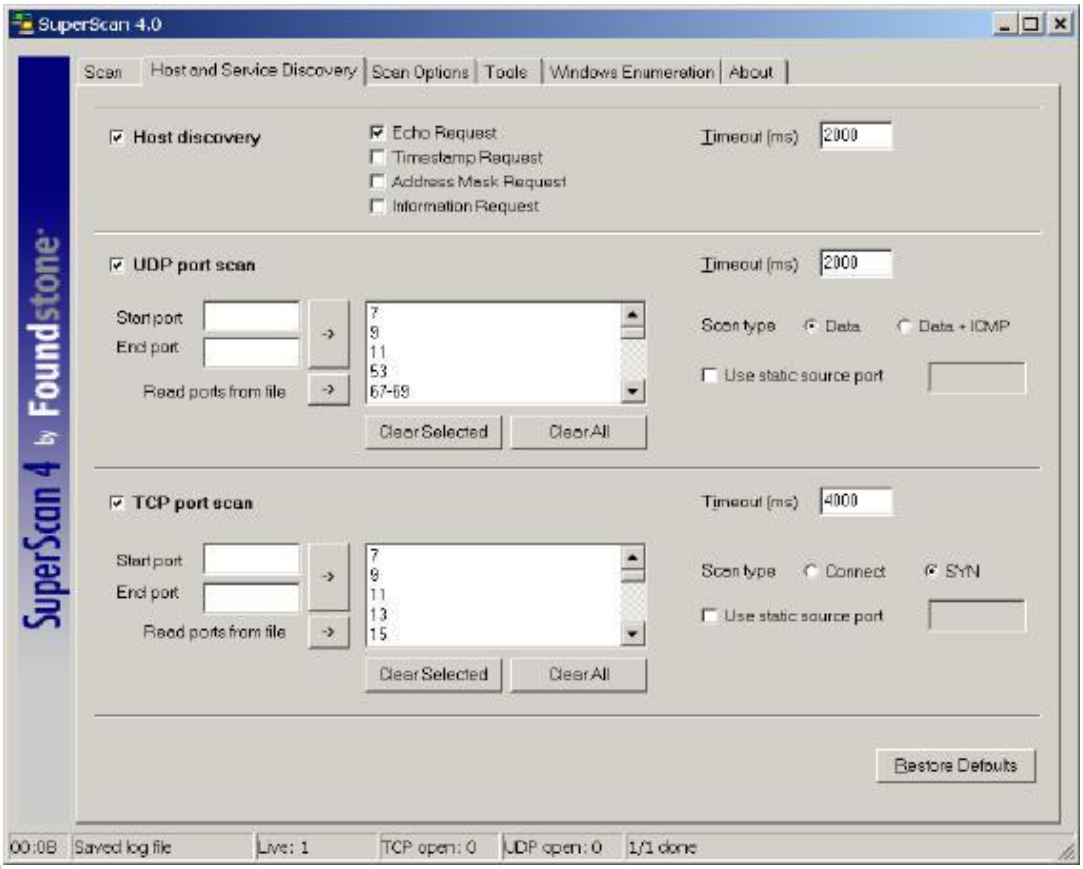
این نرم‌افزار که دارای حجم بسیار کمی است، تنها شامل یک فایل است و گزارش‌های خود را نیز در قالب HTML تولید می کند. شکل زیر صفحه‌ی اصلی این نرم‌افزار در ابتدای اجرا را نشان می‌دهد :



در قسمت اول، امکان ورود اسم یا آدرس IP یا بازه‌یی از آدرس‌های IP وجود دارد. در شکل زیر بازه‌یی از IPها برای عمل پویش تعیین شده‌اند:



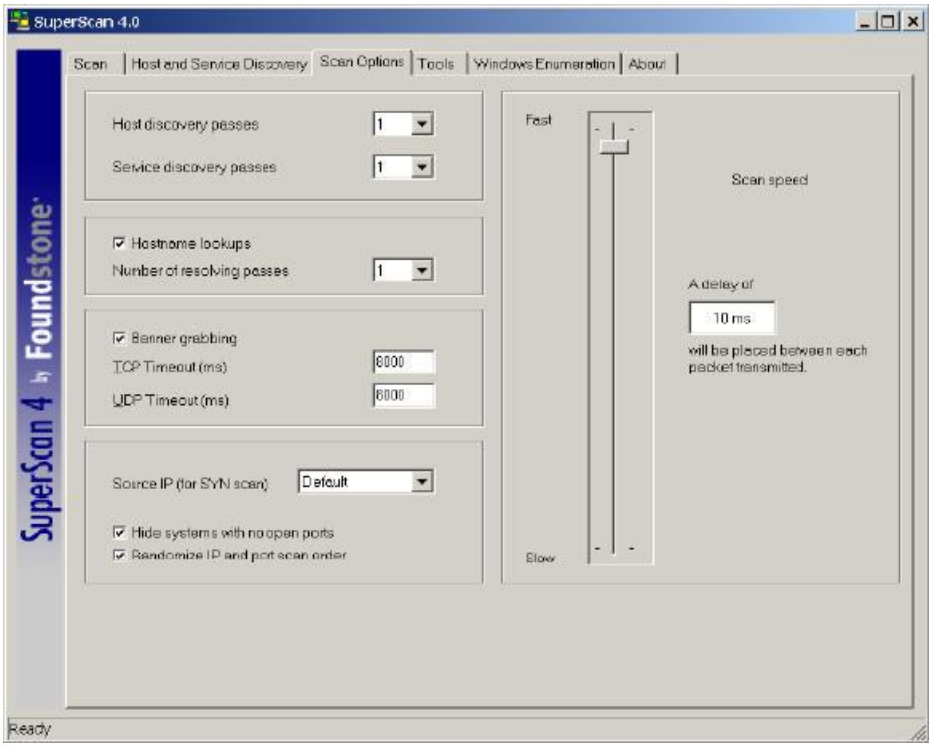
در قسمت دوم، امکان تعیین پارامتر برای تعیین نوع پویش وجود دارد. مقادیر پیش فرض در شکل زیر نمایش داده شده‌اند:



برای تعیین پارامترها، سه بخش مجزا وجود دارد که به عنوان سه وظیفه‌ی اصلی این ابزار است. در قسمت اول، امکان استفاده از این ابزار به عنوان یک پویش‌گر آدرس IP وجود دارد. در دو قسمت دیگر، پویش یا عدم پویش درگاه‌های پروتکل‌های TCP یا UDP و همچنین بازه‌ی درگاه‌های مورد نظر تعیین می‌گردد. بازه‌های تعیین شده به‌صورت پیش‌فرض، اختصاص به درگاه‌های متداول و مورد استفاده دارد. در صورت نیاز می‌توان به این بازه از درگاه‌ها، شماره‌های دیگری را نیز اضافه کرد. در قسمت درگاه‌های TCP/UDP، امکان تعیین درگاهی به عنوان درگاه مبدأ، به صورت ثابت، نیز وجود دارد.

در هریک از این سه بخش، زمانی که ابزار منتظر پاسخ از سوی سیستم مورد نظر می‌ماند، بر حسب میلی ثانیه، تعیین می‌شود. البته باید به‌خاطر داشت که این اعداد به‌معنای فاصله میان بسته‌های ارسالی نیست. این عدد در بخش دیگری قابل تنظیم است.

شکل زیر پنجره‌ی بعدی، یعنی Scan Options، برای تعیین پارامترهای دیگر این ابزار را نشان می‌دهد:



در این بخش امکان تعیین تعداد دفعاتی که پویش، چه برای آدرس و چه برای درگاه، انجام می‌گردد، وجود دارد. با تکرار پویش، نتایج دقت بیشتری می‌یابند، خصوصاً اگر در حال پویش بر روی شبکه‌یی با سرعت پایین هستیم.

پارامتر مهم دیگر در این میان امکان Banner Grabbing است که برای سرویس‌هایی که اصطلاحاً Banner نشان می‌دهند، همچون Web Serverها و FTP Server، کاربرد دارد. معمولاً با استفاده از Banner، می‌توان از نوع و سازنده‌ی Server مورد نظر آگاه شد.

در قسمت سمت راست، سرعت پویش تعیین می‌گردد. این سرعت که با تعیین فاصله‌ی میان بسته‌های تولیدی قابل تنظیم است، در صورتی که در حال پویش تعداد زیادی سیستم، بر روی شبکه‌یی گسترده با سرعتی قابل قبول هستیم، در کوتاه کردن زمان اجرای ابزار نقش به‌سزایی دارد.

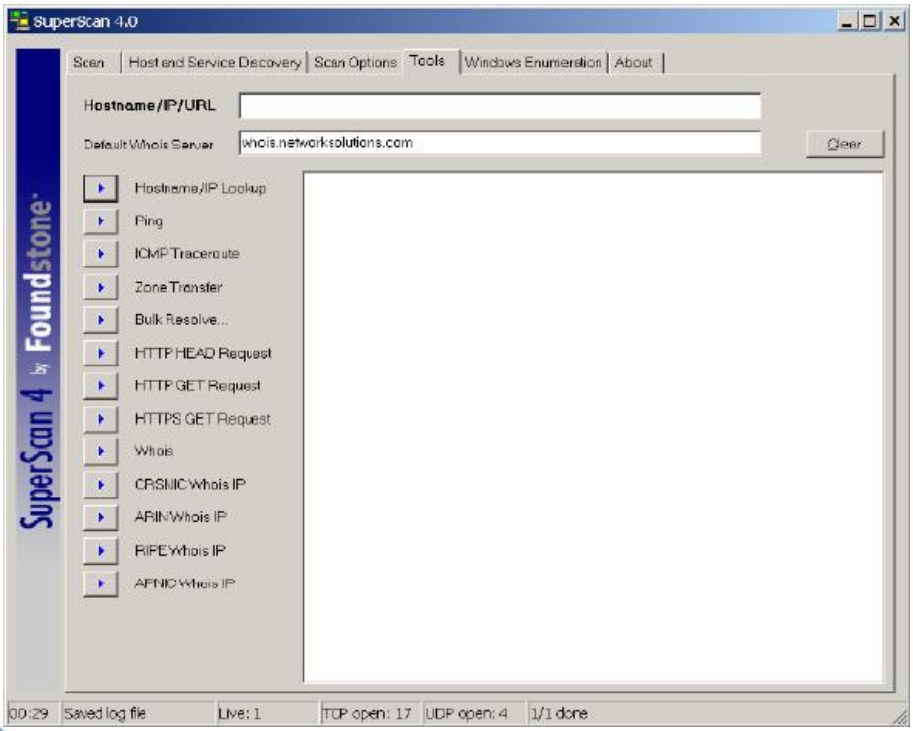
در قسمت بعدی از مرور این نرم‌افزار به امکانات دیگر آن خواهیم پرداخت.

SuperScan

قسمت دوم

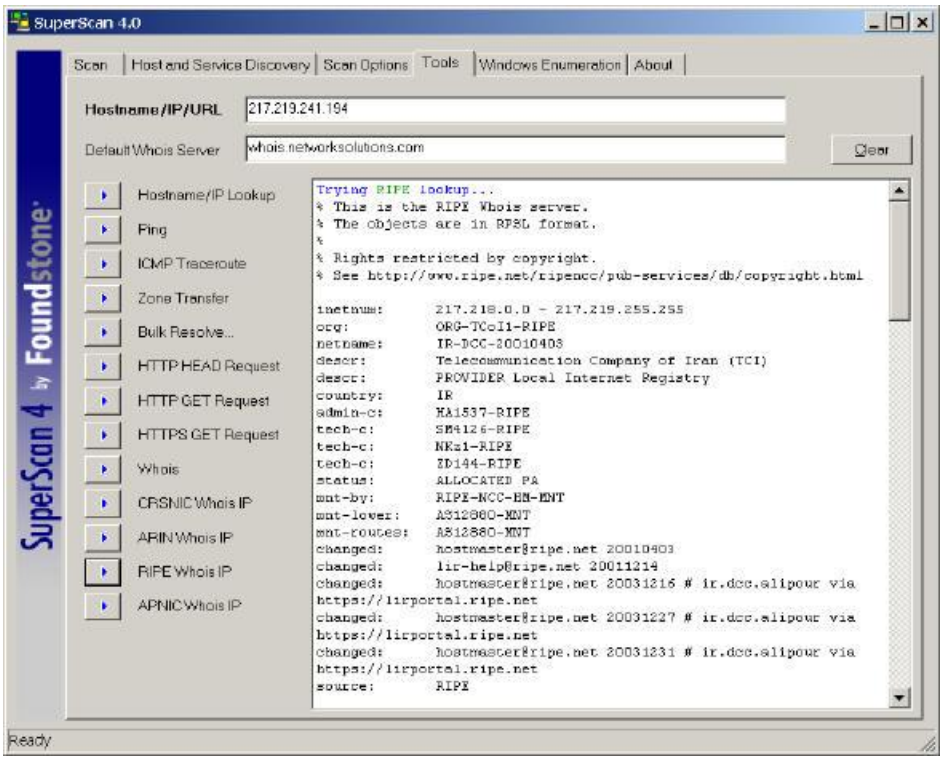
در ادامه‌ی قسمت پیشین، که در آن به معرفی متداول‌ترین دسته از نرم‌افزارهای بررسی امنیتی سیستم های رایانه‌یی، یعنی پویش‌گرهای آدرس و درگاه، پرداختیم، در این قسمت به ادامه‌ی معرفی امکانات ویژه‌ی این نرم‌افزار می‌پردازیم.

در پنجره‌ی زیر، بخش ابزارهای همراه با این نرم‌افزار را مشاهده می‌کنید:



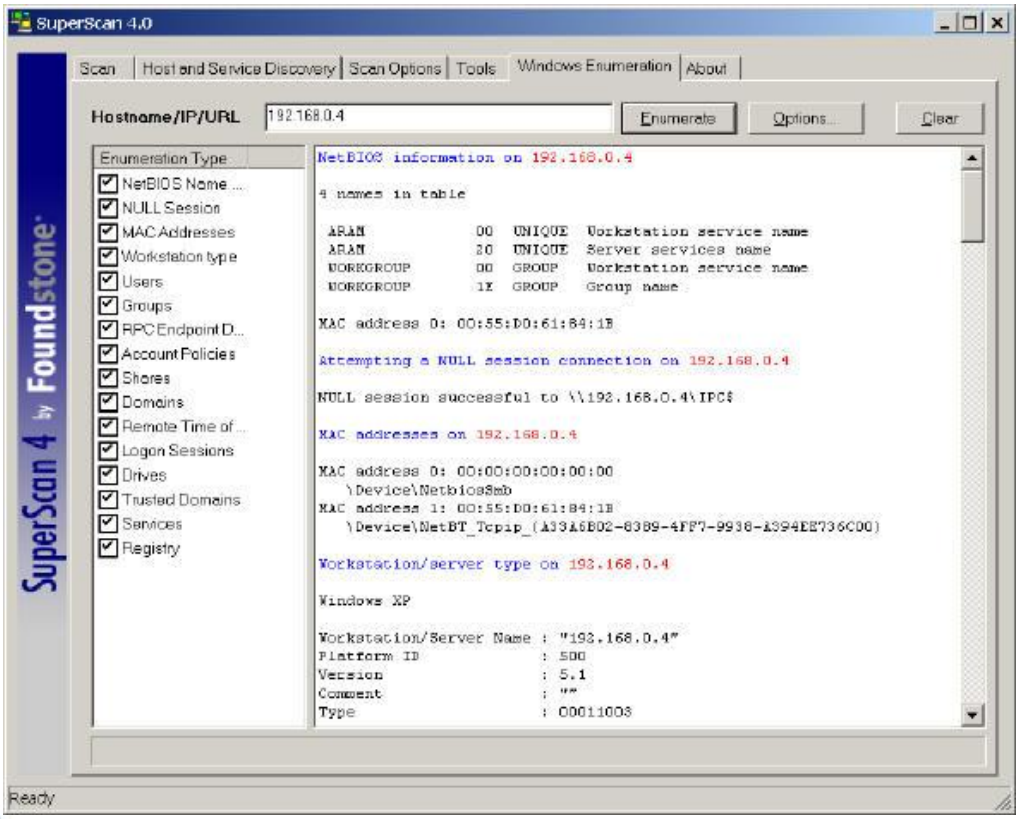
این نرم‌افزار، با در اختیار قراردادن ابزارهای کوچک و متداول، که در بررسی وضعیت شبکه‌ها استفاده می‌شود، عملاً امکانی مجتمع برای استفاده‌های متداول محسوب می‌گردد.

در این بخش امکان به دست آوردن آدرس IP از نام، Ping کردن یک ایستگاه، استفاده از امکانات HTTP، بررسی مالکیت یک دامنه‌ی اینترنتی و حتی بررسی مالکیت یک آدرس IP نیز وجود دارد. شکل زیر مثالی از اجرای RIPE Whois IP برای یکی از آدرس‌های متعلق به شرکت مخابرات ایران را نشان می دهد. خروجی این ابزار، اطلاعات جامعی در مورد آدرس IPی مورد نظر و مالک آن است:



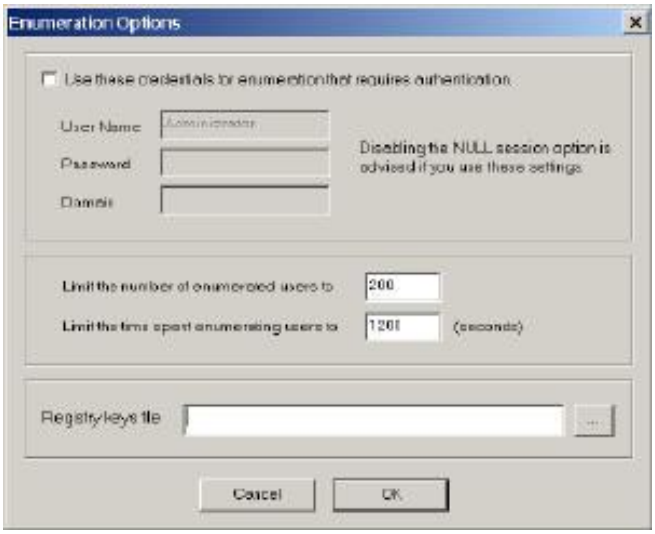
از دیگر امکانات ویژه‌ی این نرم‌افزار، امکان بررسی سیستم‌های مبتنی بر Windows است. بررسی‌هایی که در این راستا انجام می‌گیرد تمامی ابعاد معمول یک سیستم را در بر می‌گیرد، از جمله نام NetBIOS، گروه‌ها و کاربران آن سیستم، دامنه‌های محلی‌یی که سیستم به آن متصل است، منابع به اشتراک گذارده شده و دیگر ابعاد.

شکل زیر صفحه‌یی نمونه از اجرای آزمایشی این بررسی بر روی یک سیستم نمونه با آدرس IP محلی 192.168.0.4 را نشان می‌دهد:



در سمت چپ این پنجره، امکان تعیین بررسی‌های ویژه‌یی که مد نظر است نیز امکان‌پذیر است. برای مثال می توان تنها به بررسی نام NetBIOS و یا تنها گروه‌ها و کاربران پرداخت.

در همین قسمت، امکان تعیین پارامترهایی، مجزا از نوع عمل‌کرد ابزار وجود دارد. با انتخاب گزینه‌ی Options، می‌توان آن‌ها را تعیین کرد:



مهم‌ترین پارامتر قابل تعیین در این میان، تعیین نام کاربری است که برای بررسی یک سیستم مبتنی بر سیستم عامل خانواده‌ی Windows به‌کار می‌رود. به‌عبارت دیگر با تعیین کاربری که اختیارات کاملی دارد، مانند Administrator، می‌توان تمامی اطلاعات مورد نظر درباره‌ی سیستم راه دور را به‌دست آورد. نکته‌یی که در این میان اهمیت دارد این است که در اغلب موارد، بررسی انجام شده توسط کاربر Administrator یا کاربران دیگری که اختیار تام در سیستم مورد نظر دارند، هدف نیست. به‌بیان دیگر هدف اصلی از استفاده از این امکان ویژه، بررسی امکان دسترسی به اطلاعات سیستم توسط یک **کاربر نوعی بدون داشتن دسترسی‌های ویژه** است. در واقع وجود امکان دسترسی به اطلاعات حیاتی در مورد سیستم، برای کاربران متفرقه است که امکان وجود خطر حملات به سیستم را بالا می‌برد و نه امکان دسترسی برای کابران در سطوح مدیریتی.

امکان فوق را، با توجه به سبکی این نرم‌افزار از نظر حجمی، و ساده‌گی آن از نظر استفاده، می‌توان به‌نوعی یک امکان پویش امنیتی به‌حساب آورد. استفاده‌ی اغلب کاربران

خانه‌گی از سیستم‌های عامل سری Windows نیز به اهمیت این امکان ویژه افزوده و آن را بیش‌تر به عنوان یک پویش‌گر امنیتی ساده مطرح می‌کند.

WinDump

قسمت اول : Snifferها

این ابزارWinDump که نسخه‌ی تحت Windows نرم‌افزار قدیمی و مشهور tcpdump تحت سیستم‌های عامل خانواده‌ی Unix می‌باشد، عملاً یک تحلیل‌گر ترافیک شبکه است. از آن‌جاکه اغلب استفاده کننده‌گان سیستم‌های کامپیوتری خانه‌گی در کشورمان را کاربران سیستم‌های عامل خانواده‌یWindows تشکیل می‌دهند، معرفی WinDump را به بررسی tcpdump ترجیح داده‌ایم.

یک تحلیل‌گر ترافیک شبکه، که عموماً با نام Sniffer از آن یاد می‌گردد، وظیفه‌ی بررسی بسته‌های رد و بدل شده بر روی شبکه را برعهده دارد که نرم‌افزار Ethereal نمونه‌ی متداول و پرطرفداری از یک Sniffer است. از آن‌جاکه در معرفی نرم‌افزار پیشین بصورت اجمالی به این دسته از ابزارها پرداخته بودیم، در معرفی WinDump نیاز به ذکر مقدمات بیش‌تری از Snifferها داریم.

با استفاده از یک Sniffer، با تعیین یک رابط شبکه‌ی خاص، می‌توان به پایش و تحلیل بسته‌های اطلاعاتی رد و بدل شده بر روی شبکه‌یی که رابط شبکه‌ی مورد نظر به آن متصل است پرداخت. به عبارت دیگر یک Sniffer را می‌توان به یک سیستم پایش تشبیه کرد که تمامی اطلاعات منتقل شده بر روی بستر فیزیکی را بررسی و ذخیره می‌کند. در نهایت با به دست آوردن این اطلاعات دو عمل می‌توان بر روی محتوای بسته‌های بررسی شده انجام داد:

- **تحلیل کلی ترافیک شبکه**

این عمل توسط تحلیل‌گر انجام می‌گردد و از آن‌جاکه حجم اطلاعات رد و بدل شده بر روی شبکه بسیار زیاد است، تحلیل‌گر باید توانایی تمیز دادن اطلاعات مربوط به پروتکل‌های مختلف با مبدأ و مقصدهای مختلف را داشته باشد.

- فیلتر کردن بسته‌هایی با محتوایی خاص

با فیلترکردن بسته‌هایی خاص و نمایش اختصاصی آن‌ها توسط Sniffer، می‌توان تمیزدادن بسته‌های مربوط به یک پروتکل خاص، از/به مبدأ/مقصد خاص، با محتوایی از رشته‌یی تعیین شده و دیگر ویژه‌گی‌ها را به نرم‌افزار Sniffer سپرد. پس از به دست آوردن خروجی دل‌خواه تحلیل آن بسیار آسان‌تر است.

قابلیت پایش بسته‌های رد و بدل شده بر روی شبکه، قابلیتی مختص سخت‌افزار است. به عبارت دیگر رابط شبکه در حالتی خاص قرار می‌گیرد که تمامی بسته‌هایی که مقصد آدرس فیزیکی آن‌ها رابط مورد نظر نیست نیز مانند بسته‌های مربوط دریافت شده و محتوای آنها را می‌توان ذخیره کرد. در حالت عادی، سخت‌افزار و لایه‌ی Datalink بسته‌هایی که به رابط مورد نظر با آدرس فیزیکی خاص، ارتباطی ندارند را از روی شبکه بر نمی‌دارد.

با این وجود، از آن‌جاکه هدف از استفاده از Snifferها بررسی تمامی ترافیک شبکه، با استفاده از پایش تمامی بسته‌هایی که از مبدآهای مختلف به مقاصد دیگر ارسال می‌شوند می‌باشد، لذا پیش‌نیاز استفاده از این دسته از ابزارها اساساً وجود نسخه‌یی از تمامی ترافیک شبکه بر روی بستر متصل به رابط شبکه‌ی مورد نظر است.

این پیش‌نیاز، پیش‌نیازی سخت‌افزاری را به استفاده کننده از Sniffer تحمیل می‌کند، زیرا با استفاده از سوییچ‌ها، که در حال حاضر تقریباً در تمامی موارد جای Hubها را گرفته‌اند، ترافیکی که بر روی هریک از درگاه‌های سوییچ به سمت سیستم مورد نظر فرستاده می‌شود، تنها مختص آن سیستم است و ترافیک دیگر گره‌های شبکه بر روی آن قرار ندارد. لذا در شبکه‌یی که بر اساس سوییچ عمل می‌کند، عملاً امکان استفاده از Sniffer در شرایط معمول وجود ندارد.

با این‌وجود بسیاری از سوپیچ‌ها با هدف در اختیار گذاردن درگاهی خاص، امکان قرار دادن تمامی ترافیک شبکه بر روی یک کانال را فراهم می‌کنند و سیستمی که به این درگاه متصل باشد می‌تواند به پایش ترافیک شبکه بپردازد. امکان استفاده از این قبیل درگاه‌ها بر روی سوییچ‌ها، در صورت وجود، محدود بوده و تنها مختص مدیران شبکه می‌باشد. این امکان تنها برای جامه‌ی عمل پوشانیدن به یکی از اهدف استفاده از Snifferها، یعنی استفاده توسط مدیران شبکه برای تحلیل ترافیک فعال، در برخی از سوییچ‌ها وجود دارد.

در استفاده از این دسته از Snifferها دو کاربرد خاص مد نظر بوده است:

- استفاده توسط مدیران و تحلیل‌گران شبکه برای عیب‌یابی و رفع کاستی‌های شبکه
- استفاده توسط نفوذگران به شبکه‌ها و سیستم‌ها
- شناسایی تلاش‌ها برای نفوذ

هدف اول، عمل‌کردی است که در مورد آن صحبت شد. کاربرد بعدی، استفاده از قابلیت این دسته از نرم‌افزارها توسط نفوذگران به شبکه‌ها است. نفوذگران با پایش داده‌ها، به تلاش برای تحلیل داده‌های شبکه و به‌دست‌آوردن اطلاعاتی هرچه بیشتر در مورد شبکه

می‌پردازند. دسته‌ی مهمی از این اطلاعات کدهای کاربری و کلمات عبور نرم‌افزارهای مختلفی است که به‌صورت رمزنشده بر روی شبکه در حال انتقال هستند. یک نفوذگر، با تحلیل ترافیک، ابتدا به نوع نرم‌افزارهای فعال بر روی شبکه پی‌برده و سپس در پی شناخت بیش‌تر یک نرم‌افزار نمونه و تشخیص حفره‌های امنیتی موجود در آن، به فیلترکردن بسته‌های مختص آن نرم‌افزار پرداخته و سعی در گردآوری اطلاعات بیش‌تر در مورد آن می‌کند. با به دست آوردن اطلاعات مورد نظر، اقدامات بعدی برای حمله، توسط اطلاعات حیاتی به دست آمده، انجام می‌گیرد.

استفاده از سوییچ‌ها، علاوه بر بالابردن کارایی استفاده از سخت‌افزار و بستر شبکه، به بالابردن امنیت موجود نیز کمک شایانی کرده و احتمال پایش ترافیک توسط نفوذگران، بر روی سیستم‌های متفرقه‌ی موجود بر روی شبکه را پایین می‌آورد. **هرچند که باید به خاطر داشت که روش‌هایی نیز وجود دارد که می‌توان این امکان سوییچ‌ها را غیرفعال کرد و یا سوییچ را مجبور ساخت که کلیه‌ی ترافیک را به یک درگاه خاص بفرستد.** لذا استفاده از سوییچ تضمین قطعی جلوگیری از پایش ناخواسته‌ی ترافیک نیست.

هدف دیگری که می‌توان برای استفاده از Snifferها متصور بود امکان تشخیص تلاش‌های در حال انجام برای نفوذ است. تلاش‌هایی از قبیل حمله به آدرس یا درگاه خاص بر روی یک پروتکل خاص، و یا حمله به یک نرم‌افزار خاص، توسط یک تحلیل‌گر شبکه‌ی ماهر و با استفاده از یک Sniffer، قابل تشخیص است. با در نظر گرفتن این هدف، از Snifferها می‌توان بر روی یک سیستم منفرد، به منظور پایش ارتباطات انجام گرفته با سیستم، و تشخیص حملات احتمالی در حال انجام، استفاده کرد، هرچند که در این قبیل موارد استفاده از دیوارهای آتش، حتی انواع شخصی آن، کمک شایانی به کاربر می‌کنند.

با توجه به آن‌چه به‌صورت پراکنده درخلال متن گفته شد، راه‌های مقابله با Snifferها را می‌توان به سه دسته تقسیم نمود :

- استفاده از ابزارهای رمزنگاری داده‌ها
- استفاده از سوییچ در شبکه به جای Hub
- استفاده از ابزارهای ضد Sniff که امکان تشخیص رابط‌های شبکه‌یی که در حال Sniff قرار دارند را به وجود می‌آورد.

WinDump

قسمت دوم

در قسمت پیش، مقدمه‌یی درباره‌ی Snifferها، که ابزارهایی برای تحلیل ترافیک شبکه هستند، بیان شد. در آن بخش، پس از تعریف این دسته از نرم‌افزارها، فواید استفاده از این ابزارها، برای تحلیل ترافیک شبکه مورد بررسی قرار گرفت. در ادامه، همچنین به روش‌هایی که با استفاده از آن‌ها نفوذگران دست به حمله به سیستم‌ها و شبکه‌های رایانه‌یی می‌زنند پرداخته شد و در انتها برخی از روش‌های مقابله با این قبیل نفوذها را ذکر کردیم.

در قسمت دوم و پایانی از این بررسی، به نرم‌افزار WinDump، که نمونه‌یی مرسوم از این ابزارها است می‌پردازیم. این نرم‌افزار عملاً نسخه‌ی تحت سیستم‌های‌عامل سری Windows ابزار tcpdump است. tcpdump که نرم‌افزاری قدیمی و متداول تحت سیستم‌عامل خانواده‌ی Unix می‌باشد، جزو اولین و ساده‌ترین Snifferها است.

دریافت و نصب نرم‌افزار

برای دسترسی به این نرم‌افزار و دریافت آن می‌توانید به آدرس http://windump.polito.it مراجعه کنید. این نرم‌افزار از کتابخانه‌یی سازگار با libpcab استفاده می‌کند که نگارش تحت Windows آن به WinPcap موسوم است. این نرم‌افزار را می‌توانید از همان سایت دریافت کنید. پس از نصب آخرین نگارش WinPcap، نرم افزار WinDump عملیاتی می شود. نکته‌یی که باید به‌خاطر داشته باشید این است که برای آنکه این نرم‌افزار تمامی و یا اغلب بسته‌های در حال انتقال بر روی شبکه را شناسایی و دریافت کند، باید از آخرین نگارش آن استفاده کنید، هرچند که

این نرم‌افزار مدت‌هاست که به روز نشده، با این وجود اگر به‌طریقی نگارشی دیگر و قدیمی از این نرم‌افزار را به دست آوردید، برای کارایی بهتر، نسخه‌ی جدیدتر را دریافت کنید.

قابلیت‌های WinDump

محیط استفاده از این نرم‌افزار، محیطی ساده و متنی است. در واقع وجود این محیط به‌منظور سادگی بیشتر و تشابه هرچه بیش‌تر آن با نرم افزار tcpdump است. با وجود این سادگی، WinDump دارای قابلیت‌های متنوعی است.

پس از اجرای این نرم‌افزار، با تعیین رابط شبکه‌یی که WinDump می‌باید به‌دریافت بسته‌های رد و بدل شده بر روی شبکه‌ی مرتبط با رابط مورد نظر بپردازد، این نرم‌افزار، Header تمامی بسته‌های دریافت شده را بر روی صفحه‌ی نمایش داده و زمان و تاریخ هریک را نیز نشان می‌دهد.

شناسایی و تعیین پروتکل‌ها

WinDump، بسیاری از پروتکل‌ها را شناسایی می‌کند و در این صورت نام پروتکل مورد نظر را بر روی صفحه نشان می‌دهد. با این وجود این امکان وجود دارد که تنها پروتکلی خاص برای تحلیل و شناسایی مورد نظر قرار گیرد و WinDump تنها بسته‌های پروتکل تعیین شده را در گزارش نشان دهد.

از سوی دیگر، این نرم‌افزار امکان شناسایی بسته‌هایی با انواع خاص، مانند بسته‌هایی متعلق به VLANهای تعریف شده بر روی شبکه، یا بسته‌های متعلق به ارتباطات VPN را دارد. در مورد بسته‌های متعلق به VPN، امکان رمزگشایی آنها با تعیین الگوریتم رمزنگاری و تعیین کلید مربوطه نیز وجود دارد.

- **تعیین مبدأ و مقصد خاص**

در صورت نیاز، با استفاده از کلیدهایی، می‌توان بسته‌هایی را مشاهده کرد که از مبدأ(هایی) به مقصد(هایی) خاص در حال گذر هستند.

خروجی‌های مختلف

این نرم‌افزار، بر اساس پروتکل‌های مختلف خروجی‌های مختلفی را نشان می‌دهد. به‌عبارت دیگر، برای هر بسته، بر اساس اینکه متعلق به چه نوع پروتکلی است، نوع خروجی، یا خط گزارش مورد نظر، مستقل از زمان و تاریخ دریافت بسته، متفاوت است. هرچند که برای اکثر آنها، نام یا آدرس و شماره‌ی پورت مورد نظر بسته، نمایش داده می‌شود.

در صورت نیاز و به منظور بالاتر رفتن سرعت پردازش WinDump، می‌توان قابلیت استخراج اسامی سیستم‌ها در قالب مبدأ و مقصد را، حذف نمود و تنها به مشاهده‌ی آدرس اکتفا کرد. در این صورت، تأخیری که صرف به دست آوردن نام سیستم مبدأ یا مقصد می‌شود از بین می‌رود.

فیلترهای متنوع خروجی

یکی از قابلیت‌های خاص این نرم‌افزار، امکان استفاده از فیلترهای مختلف برای تعیین خروجی و بررسی بسته‌های ویژه است. برای تعیین نوع گزارش، می‌توان پارامترهای مختلفی را تعیین نمود که بر اساس آنها، WinDump گزارش بسته‌های خاصی را نمایش می‌دهد و بسته‌های دیگر را نادیده می گیرد.

نمونه‌یی از این فیلترها، فیلتر اندازه‌ی بسته و یا نوع بسته در قالب یک پروتکل واحد است. به عبارت دیگر، توسط این فیلترها، می‌توان بسته‌هایی با اندازه‌هایی خاص را مورد نظر قرار داد و یا برای مثال می‌توان بسته‌های خاصی از پروتکل TCP را بررسی کرد و دیگر بسته‌ها را نادیده گرفت.

برای تعیین فیلترها، علاوه بر عباراتی که به‌صورت پیش‌فرض در این نرم‌افزار قابل دسترسی هستند، عباراتی جدید را نیز با ترکیب عبارات ساده می‌توان به‌دست آورد. عبارات پایه، برای تعیین پارامترهای ابتدایی مانند مبدأ، مقصد، پورت، پروتکل و دیگر پارامترها هستند.

ذخیره‌ی گزارش

این نرم‌افزار قابلیت ذخیره‌ی گزارش مورد نظر به صورت یک پرونده را نیز دارد. پرونده به‌صورت خام و پردازش نشده ذخیره می‌شود و برای پردازش بر روی آن، می‌توان از همین نرم‌افزار، با تعیین از پارامتری خاص، استفاده نمود که در آن صورت عملاً گزارش اولیه تولید می‌شود.

با توجه به قابلیت‌هایی که در مورد این نرم‌افزار، به‌اختصار، مورد اشاره قرار گرفت، این ابزار را می‌توان ابزاری قوی برای کاربرانی که به ابزار متداول و قدیمی tcpdump عادت داشته‌اند دانست. با این وجود از آنجاکه روش کار با آن برای کاربران عادی، به دلیل نبود رابط کاربری گرافیکی مناسب، کمی خسته کننده است، می‌توان از Snifferهای دیگری همچون نرم‌افزار Ethereal استفاده کرد، که با استفاده از رابط کاربری آنها، تحلیل و تعیین روش کار به‌راحتی صورت گرفته، و خروجی تولید شده خوانایی بیش‌تری دارد.

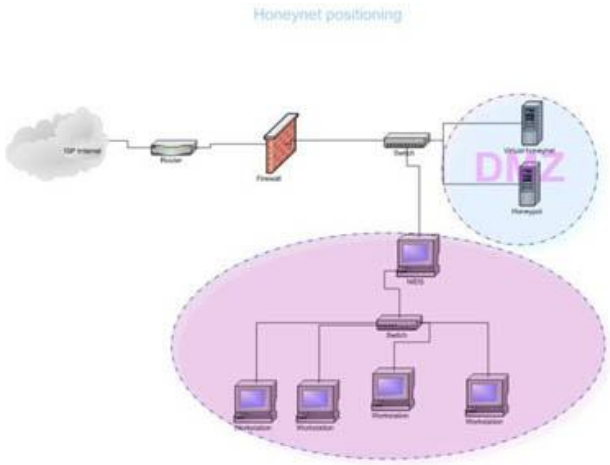
نکته‌یی که علاوه بر ذکر در بخش اول در این‌جا نیز مجدداً بر روی آن تأکید می‌کنیم این است که تقریباً در **تمامی موارد، Snifferها تنها در شرایطی کاربرد دارند که در شبکه‌ی مورد نظر از سوییچ استفاده نشده باشد یا در صورت استفاده از سوییچ، درگاهی خاص برای تحلیل تمامی ترافیک در حال پردازش توسط سوییچ بر روی درگاه‌های دیگر، قابل تعریف باشد.**

Honeypot قسمت اول

Honeypot ها یک تکنولوژی جدید می باشند که قابلیتهای فراوانی برای جامعه امنیتی دارند. البته مفهوم آن در ابتدا به صورتهای مختلفی تعریف شده بود به خصوص توسط Cliff Stoll در کتاب « The Cuckoos Egg » . از آنجا به بعد بود که Honeypot ها شروع به رشد کردند و به وسیله ابزارهای امنیتی قوی توسعه یافتند و رشد آنها تا به امروز ادامه داشته است. هدف این مقاله تعریف و شرح واقعی Honeypot می باشد و بیان منفعت ها و مضرات آنها و اینکه آنها در امنیت چه ارزشی برای ما دارند.

تعریف

قدم اول در فهم اینکه Honeypot چه می باشند بیان تعریفی جامع از آن است. تعریف Honeypot می تواند سخت تر از آنچه که به نظر می رسد باشد. Honeypot ها از این جهت که هیچ مشکلی را برای ما حل نمی کنند شبیه دیواره های آتش و یا سیستمهای تشخیص دخول سرزده نمی باشند. در عوض آنها یک ابزار قابل انعطافی می باشند که به شکلهای مختلفی قابل استفاده هستند.آنها هر کاری را می توانند انجام دهند از کشف حملات پنهانی در شبکه های IPv6 تا ضبط آخرین کارت اعتباری جعل شده! و همین انعطاف پذیریها باعث شده است که Honeypot ها ابزارهایی قوی به نظر برسند و از جهتی نیز غیر قابل تعریف و غیر قابل فهم!!



Honeypot ا

یک Honeypot یک منبع سیستم اطلاعاتی می باشد که با استفاده از ارزش کاذب خود اطلاعاتی از فعالیتهای بی مجوز و نا مشروع جمع آوری می کند.

البته این یک تعریف کلی می باشد که تمامی گونه های مختلف Honeypot ها را در نظر گرفته است. ما در ادامه مثالهای مختلفی برای Honeypot ها و ارزش امنیتی آنها خواهیم آورد. همه آنها در تعریفی که ما در بالا آورده ایم می گنجند ، ارزش دروغین آنها برای اشخاص بدی که با آنها در تماسند. به صورت کلی تمامی Honeypot ها به همین صورت کار می کنند. آنها یک منبعی از فعالیتها بدون مجوز می باشند. به صورت تئوری یک Honeypot نباید هیچ ترافیکی از شبکه ما را اشغال کند زیرا آنها هیچ فعالیت قانونی ندارند. این بدان معنی است که تراکنش های با یک Honeypot تقریبا تراکنش های بی مجوز و یا فعالیتهای بد اندیشانه می باشد. یعنی هر ارتباط با یک Honeypot می تواند یک دزدی ، حمله و یا یک تصفیه حساب می باشد. حال آنکه مفهوم آن ساده به نظر می رسد (و همین طور هم است) و همین سادگی باعث این هم موارد استفاده شگفت انگیز از Honeypot ها شده است

فواید Honeypot ها

Honeypot مفهوم بسیار ساده ای دارد ولی دارای توانایی های قدرتمندی می باشد.

۱. داده های کوچک دارای ارزش فراوان: Honeypot ها یک حجم کوچکی ار داده ها را جمع آوری می کنند. به جای اینکه ما در یک روز چندین گیگابایت اطلاعات را در فایلهای ثبت رویدادها ذخیره کنیم توسط Honeypot فقط در حد چندین مگابایت باید ذخیره کنیم. به جای تولید ۱۰۰۰۰ زنگ خطر در یک روز آنها فقط ۱ زنگ خطر را تولید می کنند. یادتان باشد که Honeypot ها فقط فعالیتهای ناجور را ثبت می کنند و هر ارتباطی با Honeypot می تواند یک فعالیت بدون مجوز و یا بداندیشانه باشد. و به همین دلیل می باشد که اطلاعات هر چند کوچک Honeypot ها دارای ارزش زیادی می باشد زیرا که آنها توسط افراد بد ذات تولید شده و توسط Honeypot ضبط شده است. این بدان معنا می باشد که تجزیه و تحلیل اطلاعات یک Honeypot آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد.

۲. ابزار و تاکتیکی جدید : Honeypot برای این طراحی شده اند که هر چیزی که به سمت آنها جذب می شود را ذخیره کنند. با ابزارها و تاکتیکهای جدیدی که قبلا دیده نشده اند.

۳. کمترین احتیاجات: Honeypot ها به کمترین احتیاجات نیاز دارند زیرا که آنها فقط فعالیتهای ناجور را به ثبت می رسانند. بنابراین با یک پنتیوم قدیمی و با ۱۲۸ مگابایت RAM و یک شبکه با رنج B به راحتی می توان آن را پیاده سازی کرد.

٤. رمز کردن یا IPv6 : بر خلاف برخی تکنولوژیهای امنیتی (مانند IDS ها) Honeypot خیلی خوب با محیطهای رمز شده و یا IPv6 کار می کنند. این مساله

مهم نیست که یک فرد ناجور چگونه در یک Honeypot گرفتار می شود زیرا Honeypot ها خود می توانند آنها را شناخته و فعالیتهای آنان را ثبت کنند.

مضرات Honeypot ها

شبیه تمامی تکنولوژیها ، Honeypot ها نیز دارای نقاط ضعفی می باشند. این بدان علت می باشد که Honeypot ها جایگزین تکنولوژی دیگری نمی شوند بلکه در کنار تکنولوژیهای دیگر کار می کنند.

۱- محدودیت دید : Honeypot ها فقط فعایتهایی را می توانند پیگیری و ثبت کنند که به صورت مستقیم با آنها در ارتباط باشند. Honeypot حملاتی که بر علیه سیستمهای دیگر در حال انجام است را نمی توانند ثبت کنند به جز اینکه نفوذگر و یا آن تهدید فعل و انفعالی را با Honeypot داشته باشد.

۲- ریسک : همه تکنولوژیهای امنیتی دارای ریسک می باشند. دیوارهای آتش ریسک نفوذ و یا رخنه کردن در آن را دارند. رمزنگاری ریسک شکستن رمز را دارد، IDS ها ممکن است نتوانند یک حمله را تشخیص دهند. Honeypot ها مجزای از اینها نیستند. آنها نیز دارای ریسک می باشند. به خصوص اینکه Honeypot ها ممکن است که ریسک به دست گرفتن کنترل سیستم توسط یک فرد هکر و صدمه زدن به سیستمهای دیگر را داشته باشند. البته این ریسکها برای انواع مختلف Honeypot ها فرق می کند و بسته به اینکه چه نوعی از Honeypot را استفاده می کنید نوع و اندازه ریسک شما نیز متفاوت می باشد.ممکن است استفاده از یک نوع آن، ریسکی کمتر از IDS ها داشته باشد و استفاده از نوعی دیگر ریسک بسیار زیادی را در پی داشته باشد.ما در ادامه مشخص خواهیم کرد که چه نوعی از Honeypot ها دارای چه سطحی از ریسک می باشند. چگونگی و شیوه به کار بردن Honeypot ها می باشد که ارزش و فواید و مضرات آنها را مشخص می کند. در ادامه بیشتر روی آن بحث خواهد شد.

Honeypot قسمت دوم

در قسمت اول، تعریفی از Honeypot ها ارائه دادیم و فواید و مضرات آنها را بیان کردیم. در این قسمت درباره انواع آنها بحث خواهیم کرد

انوع Honeypot ها

Honeypot ها در اندازه و شکلهای مختلفی هستند و همین امر باعث شده است که فهم آنها کمی مشکل شود. برای اینکه بتوان بهتر آنها را فهمید همه انواع مختلف آنها را در دو زیر مجموعه آورده ایم:

۱- Honeypot های کم واکنش

۲- Honeypot های پرواکنش

این تقسیم بندی به ما کمک می کند که چگونگی رفتار آنها را بهتر درک کنیم. و بتوانیم به راحتی نقاط ضعف و قدرت آنها و توانایی ها یشان را روشن تر کنیم. واکنش در اصل نوع ارتباطی که یک نفوذگر با Honeypot دارد را مشخص می کند.

Honeypot های کم واکنش دارای ارتباط و فعالیتی محدود می باشند.آنها معمولا با سرویسها و سیستم های عامل را شبیه سازی شده کار می کنند. سطح فعالیت یک نفوذگر با سطحی از برنامه های شبیه سازی شده محدود شده است. به عنوان مثال یک سرویس FTP شبیه سازی شده که به پورت ۲۱ گوش می کند ممکن است فقط یک صفحه login و یا حداکثر تعدادی از دستورات FTP را شبیه سازی کرده باشد . یکی از فواید این دسته از Honeypot های کم واکنش سادگی آنها می باشد.

نگهداری Honeypot های کم واکنش بسیار راحت و آسان است و خیلی راحت می توان آنها را گسترش داد و ریسک بسیار کمی دارند. آنها بیشتر درگیر این هستند که

چه نرم افزارهایی باید روی چه سیستم عاملی نصب شود و همچنین می خواهید چه سرویسهایی را برای آن شبیه سازی و دیده بانی (Monitor) کنید.

همین رهیافت خودکار و ساده آنها است که توسعه آن را برای بسیاری از شرکت ها راحت می کند. البته لازم به ذکر است که همین سرویسهای شبـــیه سازی شده باعث می شود که فعالیت های فرد نفوذگر محدود شود و همـــین امر باعث کاهش ریسک می گردد. به این معنی که نفوذگر نمی تواند هیچگاه به سیستم عامل دسترسی پیدا کند و به وسیله آن به سیستم های دیگر آسیب برساند.

یکی از اصلی ترین مضرات Honeypot های کم واکنش این است که آنها فقط اطلاعات محدودی را می توانند ثبت کنند و آنها طراحی می شوند که فقط اطلاعاتی راجع به حملات شناخته شده را به ثبت برسانند.همچنین شناختن یک Honeypot کم واکنش برای یک نفوذگر بسیار راحت می باشد. نگران این نباشید که شبیه سازی شما چه اندازه خوب بوده است زیرا که نفوذگران حرفه ای به سرعت یک Honeypot کم واکنش را از یک سیستم واقعی تشخیص می دهند. از Honeypot های کم واکنش می توان Honeyd , Spector و KFSensor را نام برد.

Honeypot های پر واکنش متفاتند. آنها معمولا از راه حل های پیچیده تری استفاده می کنند زیرا که آنها از سیستم عاملها و سرویسهای واقعی استفاده می کنند. هیچ چیزی شبیه سازی شده نیست و ما یک سیستم واقعی را در اختیار نفوذگر می گذاریم.

اگر شما می خواهید که یک Honeypot لینوکس سرور FTP داشته باشید شما باید یک لینوکس واقعی به همراه یک سرویس FTP نصب کنید. فایده این نوع Honeypot دو چیز است. شما می توانید یک حجم زیادی از اطلاعات را به دست آورید. با دادن یک سیستم واقعی به فرد نفوذگر شما می توانید تمامی رفتار او از rootkit های جدید گرفته تا یک نشست IRC را زیر نظر بگیرید.

دومین فایده Honeypot های پرواکنش این است که دیگر جای هیچ فرضیه ای روی رفتار نفوذگر باقی نمی گذارد و یک محیط باز به او می دهد و تمامی فعالیتهای او را زیر نظر می گیرد. همین امر باعث می شود که Honeypot های پرواکنش رفتارهایی از فرد نفوذگر را به ما نشان دهند که ما انتظار نداشته ایم و یا نمی توانسته ایم حدس بزنیم!!

بهترین جا برای استفاده از این نوع Honeypot ها زمانی است که قصد داریم دستورات رمز شده یک در پشتی را روی یک شبکه غیر استاندارد IP به دست بیاریم. به هر حال همین امور است که ریسک اینگونه Honeypot ها را افزایش می دهد زیرا که نفوذگر یک سیستم عامل واقعی را در اختیار دارد و ممکن است به سیستم های اصلی شبکه صدمه بزند. به طور کلی یک Honeypot پرواکنش می تواند علاوه بر کارهای یک Honeypot کم واکنش کارهای خیلی بیشتری را انجام دهد.

برای فهم بهتر اینکه Honeypot کم واکنش و پرواکنش چگونه کار می کنند بهتر است دو مثال واقعی در این زمینه بیاوریم. با Honeypot های کم واکنش شروع می کنیم.

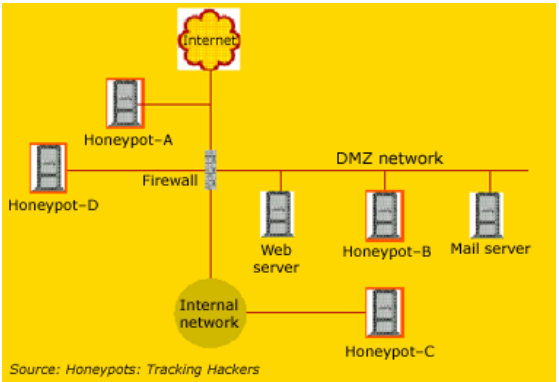


Figure 1. Honeypots can be deployed from a variety of locations. This diagram shows four different possible locations. The optimum location for deployment depends on an array of factors, such as the type of information the organization is interested in gathering, and the level of risk that organization can tolerate to obtain the maximum amount of data.

Honeyd : یک Honeypot کم واکنش

Honeyd یک Honeypot کم واکنش است که توسط Provos Niels ساخته شده است. Honeyd به صورت کد باز می باشد و برای مجموعه سیستم عاملهای یونیکس ساخته شده است.(فکر کنم روی ویندوز هم برده شده است). Honeyd بر اساس زیر نظر گرفتن IP های غیر قابل استفاده بنا شده است. هر چیزی که قصد داشته باشد با یک IP غیر قابل استفاده با شبکه ارتباط برقرار کند ارتباطش را با شبکه اصلی قطع کرده و با نفوذگر ارتباط برقرار می کند و خودش را جای قربانی جا می زند.

به صورت پیش فرض Honeyd تمامی پورتها TCP و یا UDP را زیر نظر گرفته و تمامی درخواستهای آنها را ثبت می کند. همچنین برای زیر نظر گرفتن یک پورت خاص شما می توانید سرویس شبیه سازی شده مورد نظر را پیکربندی کنید مانند شبیه سازی یک سرور FTP که روی پروتکل TCP پورت ۲۱ کار می کند.وقتی که نفوذگر با یک سرویس شبیه سازی شده ارتباط برقرار می کند تمامی فعالیتهای او را با سرویسهای شبیه سازی شده دیگر ثبت کرده و زیر نظر می گیرد. مثلا در سرویس FTP شبیه سازی شده ما می توانیم نام کاربری و کلمه های رمزی که نفوذگر برای شکستن FTP سرور استفاده می کند و یا دستوراتی که صادر می کند را به دست آوریم و شاید حتی پی ببریم که او به دنبال چه چیزی می گردد و هویت او چیست!

همه اینها به سطحی از شبیه سازی بر می گردد که Honeypot در اختیار ما گذاشته است. بیشتر سرویسهای شبیه سازی شده به یک صورت کار می کنند. آنها منتظر نوع خاصی از رفتارهای هستند و طبق راههایی که قبلا تعیین کرده اند به این رفتارهای واکنش نشان می دهند.

اگر حمله A این را انجام داد از این طریق واکنش نشان بده و اگر حمله B این کار را کرد از این راه واکنش نشان بده!

محدودیت این برنامه ها در این است که اگر نفوذگر دستوراتی را وارد کند که هیچ پاسخی برای آنها شبیه سازی نشده باشد. بنابراین آنها نمی دانند که چه پاسخی را باید برای نفوذگر ارسال کنند. بیشتر Honeypot های کم واکنش – مانند Honeyd – یک پیغام خطا نشان می دهند. شما می توانید از کد برنامه Honeyd کل دستوراتی که برای FTP شبیه سازی کرده است را مشاهده کنید.

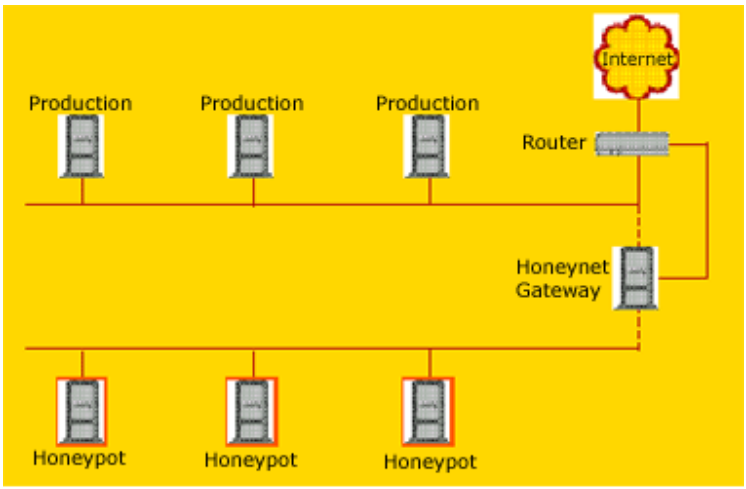


Figure 2. In this Honeynet (a research honeypot used to gather information), the Honeynet Gateway is a Layer 2 bridge that isolates the Honeynet from the rest of the production network. The bridge controls inbound and outbound traffic. Systems are placed in the Honeynet as intended targets for attackers to break into and interact with.

Honeynet ها : یک Honeypot پر واکنش

Honeynet یک مثال بدیهی برای Honeypot های پرواکنش می باشد. Honeynet ها یک محصول نمی باشند. آنها یک راه حل نرم افزاری که بتوان روی یک کامپیوتر نصب شوند نمی باشد. Honeynet ها یک معماری می باشند. یک شبکه بی عیب از کامپیوترهایی که طراحی شده اند برای حملاتی که روی آنها انجام می گیرد. طبق این نظریه ما باید یک معماری داشته باشیم که یک کنترل بالایی را روی شبکه ایجاد کند تا تمامی ارتباطات با شبکه را بتوان کنترل کرد و زیر نظر گرفت.

درون این شبکه ما چندین قربانی خیالی در نظر می گیریم البته با کامپیوترهایی که برنامه های واقعی را اجرا می کنند. فرد هکر این سیستم ها را پیدا کرده و به آنها حمله می کند و در آنها نفوذ می کند اما طبق ابتکار و راهکارهای ما ! یعنی همه چیز در کنترل ما می باشد. البته وقتی آنها این کارها را انجام می دهند نمی دانند که در یک Honeynet گرفتار شده اند. تمامی فعالیت های فرد نفوذگر از نشست های رمز شده SSH گرفته تا ایمیل ها و فایلهایی که در سیستم ها قرار می دهند همه و همه بدون آنکه آنها متوجه شوند زیر نظر گرفته و ثبت می شود. در همان زمان نیز Honeynet تمامی کارهای نفوذگر را کنترل می کند. Honeynet ها این کارها را توسط دروازه ای به نام Honeywall انجام می دهند. این دروازه به تمامی ترافیک ورودی اجازه می دهد که به سمت سیستم های قربانی ما هدایت شوند ولی ترافیک خروجی باید از سیستم های مجهز به IDS عبور کند. این کار به نفوذگر این امکان را می دهد که بتواند ارتباط قابل انعطاف تری با سیستم های قربانی داشته باشد اما در کنار آن اجازه داده نمی شود که نفوذگر با استفاده از این سیستم ها به سیستم های اصلی صدمه وارد کند.

Keylogger ابزاری برای جاسوسی

Keylogger ابزاری است که دنباله کلیدهایی که کاربر بر روی صفحه‌کلید کامپیوتر می‌فشارد، را ثبت می‌کند. این ابزار که به صورت‌های سخت‌افزاری و نرم‌افزاری تولید شده و در دسترس است در موارد متنوع و با کاربردهای مختلف به کار می‌رود. نمونه‌های مختلف Keylogger مقدار کمی از منابع سیستم شامل حافظه و پردازنده را مورد استفاده قرار می‌دهند. علاوه بر این در Task manager و لیست فرایندهای سیستم هم ظاهر نمی‌شوند، بنابراین تشخیص آنها بر روی دستگاه به سادگی امکان‌پذیر نیست.

علی رغم اهمیت زیادی که این ابزار در از بین رفتن حریم شخصی افراد و سرقت اطلاعات آنها دارد، توجه زیادی به این ابزار و تهدیدات ناشی از آن نمی‌شود. شاید دلیل این امرشهرت بیشتر ویروس‌ها، اسب‌های تروا و کرم‌ها و شناخت بیشتر نسبت به آنهاست. با توجه به سادگی انتشار این ابزار و تهدیدات ناشی از آن در این مقاله به معرفی keylogger و روش‌های مقابله با آن پرداخته است.

قابلیت‌های Keylogger ها

قابلیت Keylogger ها در این است که هر کلیدی که فشرده شود را ذخیره نموده، لیستی از حروف تایپ شده بر روی کامپیوتر را تولید می‌کنند. این لیست سپس در اختیار فردی که برنامه را بر روی دستگاه نصب کرده قرار می‌گیرد. بعضی از Keylogger ها این امکان را دارند که گزارش حروف تایپ شده را به کامپیوتری دیگر بر روی شبکه ارسال کنند. امکان ارسال اطلاعات ذخیره شده از طریق e-mail هم وجود دارد.

علاوه بر ذخیره حروف تایپ شده، بعضی از Keylogger ها اطلاعات خاصی را به صورت جدای از سایرین ثبت و گزارش آنها را تولید می‌کنند. لیست URLهایی که توسط کاربر دستگاه مشاهده شده و یا پیام‌هایی که در جریان Chat بین کاربر و دیگران رد و بدل می‌شود، جزء این گروه از اطلاعات می‌باشند.

قابلیت جالبی که تعدادی از Keylogger ها دارند گرفتن عکس از صفحه کامپیوتر در فواصل زمانی قابل تنظیم است. به این ترتیب مشخص می‌شود که چه برنامه‌هایی بر روی کامپیوتر نصب و در حال اجرا می‌باشند، چه فایل‌هایی بر روی DeskTop دستگاه قرار دارد و چه فعالیت‌هایی بر روی دستگاه انجام می‌شود.

انواع Keylogger ها

شرکت‌های مختلف تولید کننده Keylogger محصولات خود را به دو صورت سخت‌افزاری و نرم‌افزاری ارائه می‌نمایند. نرم‌افزارهای Keylogger به صورت بسته‌های نرم‌افزاری توسط شرکت‌های مختلفی توسعه داده شده، با قابلیت‌های مختلف به صورت‌های تجاری و یا مجانی عرضه می‌گردند. با یک جستجوی ساده بر روی کلمه KeyLogger در یکی از موتورهای جستجو نمونه‌های زیادی از این ابزار یافته می‌شود که بعضی از آنها به صورت مجانی قابل دریافت می‌باشد. نکته‌ای که در همه نرم‌افزارهای Keylogger وجود دارد این است که هیچ یک از آنها در Task Manager و لیست فرایندهای دستگاه ظاهر نمی‌شوند. علاوه بر این فایلی که نرم‌افزار برای ثبت اطلاعات از آن بهره می‌گیرد نیز مخفی بوده و به سادگی قابل تشخیص نیست.

برای استفاده از قابلیت‌های keylogger باید یک نمونه از نرم‌افزار بر روی دستگاه مورد نظر نصب شود. این کار با داشتن مجوزهای مدیر سیستم امکان‌پذیر است. در این صورت حتی از راه دور هم می‌توان برنامه را نصب نمود. انتقال Keylogger از طریق e-mail هم ممکن است. در این روش نرم‌افزار به همراه با یک فایل پیوست برای قربانی ارسال می‌گردد. باز کردن نامه و گرفتن پیوست آن منجر به نصب و فعال شدن keylogger بر روی دستگاه می‌شود.

نمونه‌های سخت‌افزاری این ابزار که بین صفحه‌کلید و درگاه کامپیوتر وصل می‌شوند معمولا مشابه کابل اتصال می‌باشند. با توجه به اینکه اتصال این ابزار از پشت دستگاه انجام می‌شود لذا در معرض دید نبوده و احتمال اینکه کاربر به سرعت وجود آن را کشف کند پایین است. علاوه بر این نمونه‌هایی از Keylogger ها داخل خود صفحه کلید قرار می‌گیرند و امکان شناسایی شدن آن به سادگی وجود ندارد.

نمونه‌ای از Keylogger سخت‌افزاری

کاربردهای Keylogger

پس از آشنایی با مشخصات و قابلیت‌های Keylogger اولین چیزی که به ذهن هر کسی می‌رسد استفاده از آن برای یافتن کلمات عبور دیگران می‌باشد. با استفاده از این ابزار امکان دزدیدن شناسه‌های کاربری، کلمات عبور، شماره کارت اعتباری و ... بوجود

می‌آید. از جمله مواردی که Keylogger ها در کاربردهای منفی مورد استفاده قرار گرفته‌اند می‌توان به دو مورد زیر اشاره نمود:

در فوریه ۲۰۰۳ دیوید بودرو که دانشجوی دانشگاه بوستون بود اقدام به نصب Keylogger بر روی بیش از ۱۰۰ دستگاه کامپیوتر دانشگاه نمود. او با استفاده از اطلاعاتی که به این ترتیب در مورد اساتید، دانشجویان و کارکنان دانشگاه به دست آورد، توانست بیش از ۲۰۰۰ دلار به دست آورد. مورد دیگر مربوط به جولای ۲۰۰۳ است که در آن جوجو جیانگ اعتراف نمود بر روی کامپیوترهای بیست فروشگاه در نیویورک Keylogger نصب نموده و به مدت دو سال شناسه‌های کاربری و کلمات عبور کاربران را از این طریق سرقت می‌کرده است.

در کنار این کاربردها که همگی منفی بوده و به نوعی سوء استفاده از قابلیت‌های یک ابزار محسوب می‌شوند کاربردهای دیگری نیز برای این ابزار وجود دارد. بسیاری از والدین همواره نگران نحوه استفاده فرزندان خود از اینترنت هستند. با توجه به وجود انواع سایت‌ها و مراکز اطلاع رسانی، این والدین دوست دارند که کنترل بیشتری بر استفاده از اینترنت داشته باشند. حداقل خواسته آنها این است که بدانند فرزندانشان چه سایت‌هایی را مشاهده می‌نمایند و یا با چه کسانی چت می‌کنند. در چنین مواردی استفاده از این ابزار می‌تواند کمکی باشد برای والدینی که نگران سلامت روانی فرزندان خود بوده و نسبت به تربیت آنها دغدغه‌های خاص خود را دارند.

Anti- Keylogger

این نرم‌افزارها با هدف شناسایی و ردیابی Keylogger ها تولید می‌شوند. با توجه به اینکه Keylogger ها روش‌های مختلفی برای کار و مخفی کردن خود دارند شناسایی آنها به سادگی امکان پذیر نیست. نمونه‌هایی از این نرم‌افزارها از طریق جستجو در

اینترنت قابل دریافت می‌باشند. ولی واقعیتی که در رابطه با همه این نرم‌افزارها وجود دارد عدم کارآیی آنها در مواجه با Keylogger های متنوع است.

تولیدکنندگان Keylogger، عموما ابزارهایی هم برای ردیابی Keyloggerهای خود به مشتریان عرضه می‌کنند. این ابزارها جامع نیستند و با توجه به اینکه روش‌های مختلفی برای ثبت کلیدهای فشرده شده وجود دارد، نمی‌توانند همه Keylogger ها را شناسایی نمایند.

روش‌های مقابله

متاسفانه ردیابی Keylogger ها بر روی دستگاه بسیار دشوار بوده و anti Keylogger ها هم کارایی مطلوبی ندارند. تنها راهی که برای مقابله با این ابزارها و جلوگیری از دزدی اطلاعات و نقض حریم شخصی می‌توان پیشنهاد داد بهره گرفتن از روش‌های پیش‌گیرانه است. موارد زیر به کاربران کامپیوترهای متصل به شبکه و مدیران سیستم توصیه می‌شود:

۱. کاربران عادی کامپیوتر باید با اختیارات عادی به کامپیوتر وصل شده و مجوز نصب برنامه نداشته باشند.
۲. تعداد اعضای گروه مدیران سیستم باید محدود بوده و سیاست‌های دقیقی بر فرایند انتخاب و محافظت از کلمات عبور حاکم باشد.
۳. هیچ‌گاه نباید با شناسه کاربری مدیر سیستم به اینترنت (و حتی شبکه محلی) وصل شد. ممکن است در همین زمان هکرها به سیستم نفوذ کرده و با استفاده از اختیارات مدیران سیستم اقدام به نصب نرم‌افزار keylogger بر روی دستگاه نمایند.
٤. پورت صفحه‌کلید کامپیوتر باید هر چند وقت یکبار مورد بازرسی قرار گیرد و سخت‌افزارهای مشکوک بررسی شوند.

یکی از روش‌های انتقال keyloggerها از طریق e-mail است. لذا باید نکات امنیتی لازم رعایت شده، از باز کردن نامه‌های مشکوک اجتناب شود.

آشنایی با PGP

با استفاده از PGP (Pretty Good Privacy) شما می‌توانید محرمانگی پیغامها و فایلهایتان را حفظ کنید بطوریکه فقط دریافت‌کنندگان مورد نظر شما بتوانند آنها را بخوانند. بعلاوه می‌توانید پیامها و فایلهایتان را امضای دیجیتال کنید تا دریافت‌کنندگان از تعلق آنها به شما مطمئن شوید. یک پیام امضاءشده، عدم تغییر محتویات آن را نیز تایید می‌کند. البته PGP تنها نرم‌افزار ارسال و دریافت ایمیلهای امن نیست اما کاربرد آن در این زمینه نسبتا زیاد است.

PGP براساس رمزنگاری کلید عمومی عمل می‌کند که در آن از یک جفت کلید برای برقراری ارتباط امن استفاده می‌شود. برای ارسال ایمیل خصوصی به یک نفر، از کپی کلید عمومی آن شخص برای رمزنگاری اطلاعات استفاده می‌کنید و به این ترتیب تنها آن فرد می‌تواند با استفاده از کلید خصوصی خود ایمیل را رمزگشایی کند. بالعکس، چنانچه شخصی بخواهد برای شما ایمیل امن ارسال کند، از کلید عمومی شما برای رمز کردن متن نامه استفاده می‌کند و تنها شمایید که می‌توانید آن متن را با استفاده از کلید خصوصی خود رمزگشایی کنید. بنابراین شما دیگران را از کلید عمومی خودتان مطلع می‌کنید اما از کلید خصوصی خودتان، خیر!!!

همچنین از کلید خصوصی خود برای امضای ایمیلی که قصد ارسال آنرا دارید استفاده می‌کنید. دریافت‌کنندگان می‌توانند از کلید عمومی شما برای تعیین اینکه آیا واقعا خود شما آنرا ارسال کرده‌اید و آیا متن نامه در طول ارسال تغییر نکرده است، استفاده کنند. شما هم برای تایید امضای دیگران از کلید عمومی آنها برای رمزگشایی متن دریافت‌شده استفاده می‌کنید.

در ادامه به نحوه کار با نرم‌افزار PGP اشاره می‌شود،

۱- PGP را روی کامپیوتر خود نصب کنید:

با مراجعه به راهنمای نصب PGP که معمولا همراه این نرم‌افزار است با نحوه نصب آن آشنا خواهید شد. در صورت نبود این راهنما، خودتان دست بکار شوید. چندان مشکل نیست.

۲- یک جفت کلید خصوصی و عمومی ایجاد کنید:

قبل از اینکه بتوانید استفاده از PGP را آغاز کنید، نیاز به تولید یک جفت کلید دارید. می‌توانید اینکار را در طول نصب PGP انجام دهید یا زمان دیگری که این نرم‌افزار را اجرا می‌کنید. شما به جفت کلید برای موارد زیر نیاز دارید:

- رمزنگاری اطلاعات
- رمزگشایی اطلاعاتی که با کلید شما رمز شده‌اند.
- امضاء کردن اطلاعات

۳- مبادله کلیدهای عمومی با دیگران:

بعد از اینکه جفت‌کلید را ایجاد کردید، می‌توانید مکاتبه با دیگر استفاده‌کنندگان PGP را آغاز کنید. شما به یک کپی از کلید عمومی دیگران نیاز دارید. کلید عمومی شما بصورت بلوکی از متن است، بنابراین تبادل کلید با شخص دیگر آسان است. می‌توانید کلید عمومی خود را در ایمیل قرار دهید، آنرا در فایل کپی کنید یا آنرا به یک سرویس‌دهنده کلید ارسال کنید تا هرکسی بتواند به کپی آن در صورت نیاز دسترسی داشته باشد. (مراقب باشید که کلید خصوصی خود را برای دیگران ارسال نکنید، در ضمن مطمئن باشید که از کلید عمومی یک نفر نمی‌توان به کلید خصوصی وی پی برد)

۴- از اعتبار کلید عمومی دیگران مطلع شوید:

هنگامی که شما یک کپی از کلید عمومی شخصی را دارید، می‌توانید آنرا به جاکلیدی خود اضافه کنید. بعد از آن می‌توانید نسبت به تعلق این کلید به شخص مورد نظر اطمینان حاصل کنید و اینکه این کلید تغییر نکرده است. اینکار با مقایسه اثرانگشت

(fingerprint) یکتا که در کنار کپی کلید عمومی آن شخص دارید با اثرانگشت کلید اصلی که در اختیار صاحب اصلی کلید است، انجام می‌پذیرد. هنگامی که مطمئن شدید که کلید عمومی معتبری از آن شخص در اختیار دارید، به آن کلید نشانه معتبر بودن اضافه می‌کنید.

۵- امن‌کردن ایمیلها و فایلهایتان را آغاز کنید:

بعد از اینکه جفت کلیدهایتان را تولید کردید و کلیدهای عمومی را مبادله کردید، می‌توانید دست به کار رمزنگاری، امضاء، رمزگشایی و تایید ایمیلها و فایلها شوید. برای انجام یک عمل PGP باید فایل یا پیامی را که می‌خواهید امن کنید انتخاب کنید و سپس عمل مورد نظر خود را «رمزنگاری (Encrypt)، امضاء (Sign)، رمزگشایی (Decrypt) یا تایید (Verify) » از طریق منوی PGP انتخاب کنید. منوهای PGP از چند طریق در دسترس هستند؛ مثلا در Windows Explorer شما می‌توانید روی فایل مورد نظر کلیک راست کنید و سپس عمل مناسب را در قسمت PGP انتخاب کنید.

۶- فایلهای مورد نظر را پاک کنید.

هنگامی که احتیاج به پاک کردن دائمی یک فایل دارید، می‌توانید با استفاده از ویژگی Wipe این عمل را انجام دهید تا مطمئن شوید که فایل قابل بازیابی نیست. فورا در محل ذخیره فایل اطلاعاتی نوشته می‌شود تا نتوان فایل را با استفاده از نرم‌افزارهای بازیابی دیسک حاصل کرد.

ضمنا نرم‌افزار PGP به شما امکان رمزکردن، رمزگشایی و سایر اعمال را روی اطلاعاتی که روی clipboard قرار دارد، می‌دهد. سپس اطلاعات تغییریافته را روی همان clipboard قرار میدهد. حتما می‌دانید که با انتخاب گزینه copy ، متن انتخاب شده به clipboard و با انتخاب گزینه paste متن موجود در clipboard به پنجره فعال شما منتقل می‌شود.

Nessus : پویش‌گری ساده و قدرتمند

معرفی نرم افزاری قدرتمند با نام Nessus محصولی کد باز و رایگان که با قابلیت‌های ویژه‌اش خود را مبدل به یکی از به‌ترین ابزارها در سال‌های اخیر ساخته است، می‌رسد.

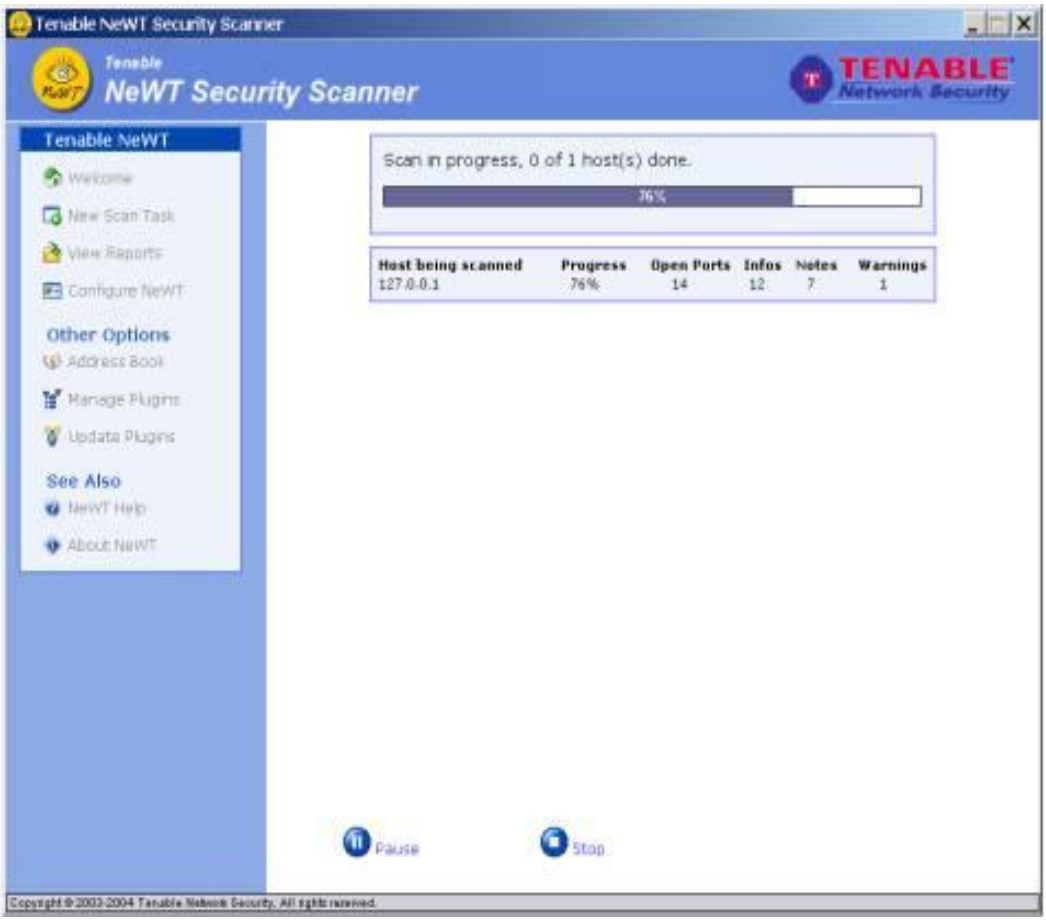
هرچند که این نرم‌افزار در واقع تنها برای محیط‌های Linux، BSD، Solaris و دیگر محیط‌های مشابه Unix نوشته شده است و در پایگاه www.nessus.org قابل دریافت است، ولی نگارشی از آن برای سیستم‌های عامل سری Windows با نام NeWT محصول Inc Tenable Network Security. نیز موجود است که با مراجعه به پایگاه این شرکت، www.tenablesecurity.com، قابل دریافت است. مبنای این معرفی بر پایه‌ی نسخه‌ی تحت Windows این ابزار، یعنی NeWT، می‌باشد.

شکل زیر صفحه‌ی آغازین این نرم‌افزار را نشان می‌دهد :

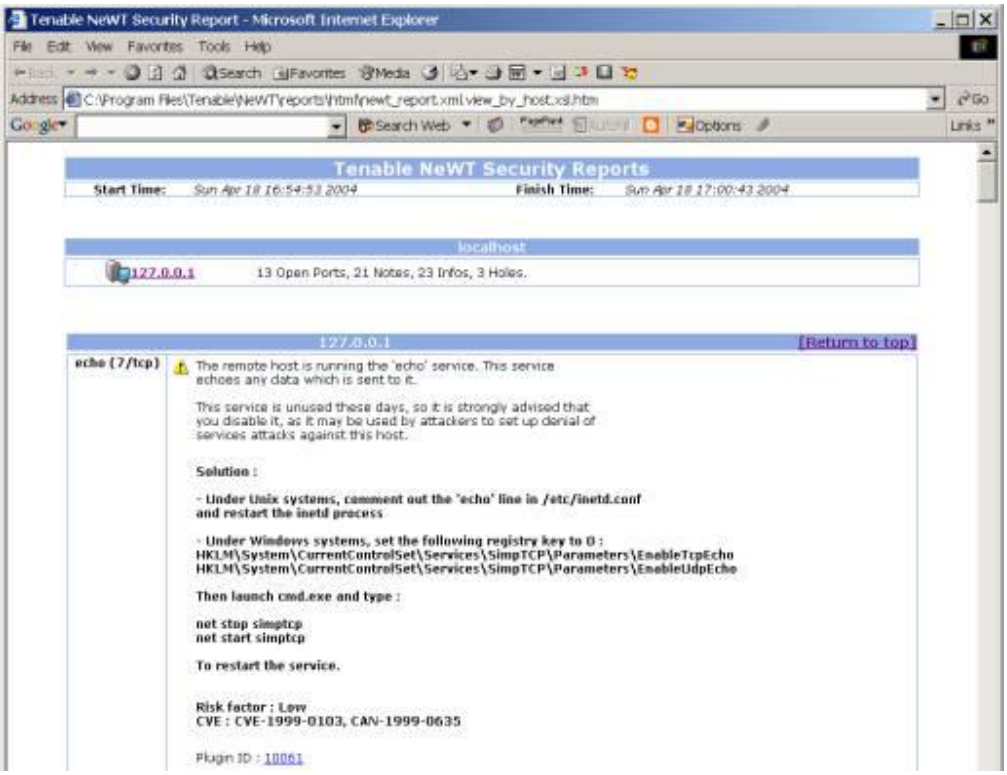
با انتخاب پویش جدید، نرم‌افزار آدرس یا آدرس‌های سیستم‌های مورد نظر برای پویش را به عنوان ورودی دریافت می‌کند. این آدرس‌ها می‌توانند در یک بازه‌ی آدرس نیز نباشند و در این صورت تک تک آنها به صورت مجزا باید ذکر شوند.

پیش از شروع پویش، از آن‌جاکه برخی از عملیاتی که در حین پویش توسط نرم‌افزار انجام می‌گیرد باعث ایجاد آسیب‌های امنیتی به سیستم مورد نظر می‌شوند، امکان تعیین زیربرنامه‌هایی که برای بررسی امنیت مورد استفاده قرار خواهند گرفت نیز وجود دارد.

پس از انتخاب حالت مورد نظر، که همان‌گونه که نرم‌افزار نیز پیش‌نهاد کرده است حالت اول امن‌ترین حالت برای پویش است، نرم‌افزار شروع به پویش کرده و در حین پویش اطلاعاتی همچون درصد پیشرفت پویش، تعداد پورت‌های باز، اخطارهای امنیتی و شکاف‌های موجود در سیستم مورد نظر ارایه می‌دهد. شکل زیر خروجی نرم‌افزار در حین پویش را نمایش می‌دهد.



پس از اتمام عمل پویش، نرم‌افزار گزارشی به‌صورت HTML تولید کرده و توسط مرورگر نمایش می‌دهد. شکل زیر نمونه‌ای از این گزارش را نشان می‌دهد.



در هر بخش از گزارش‌های ارایه شده توسط این نرم‌افزار، ضمن درج آسیب‌های امنیتی محتمل، آدرسی برای دریافت اطلاعات بیشتر در مورد ضعف امنیتی به‌همراه روش رفع آن نیز ذکر می‌شود.

همان‌گونه که در تصویر اول نیز مشاهده می‌شود، در این نرم‌افزار امکان مدیریت زیربرنامه‌هایی که توسط آن‌ها پویش انجام می‌گیرد نیز وجود دارد. از سوی دیگر در قسمت پیکربندی نیز می‌توان جزئیات پویش را نیز تعیین کرد. در این قسمت امکان تعیین کدهای کاربری به همراه رمز عبور برای پویش سرویس‌هایی که نیاز به احراز هویت دارند نیز فراهم شده است.

نرم‌افزار Nessus، و نسخه‌ی تحت Windows آن یعنی NeWT، با توجه به بازه‌ی نستباً وسیعی از سرویس‌ها و جوانب امنیتی که مد نظر قرار داده است، یکی از قوی‌ترین نرم‌افزارها در میان ابزارهای مشابه است. از آن‌جاکه رایگان بودن و راحتی استفاده از آن، به همراه گزارش نسبتاً مفصل و جامع پس از پویش، به جذابیت‌های آن افزوده است، یکی از ابزارهای مناسب برای کاربران مبتدی، متوسط و حتی پیشرفته محسوب شده و استفاده از آن به همه توصیه می‌گردد.

یک نرم‌افزار تشخیص نفوذ به‌صورت کدباز است که بر روی محیط‌های Linux و Windows عرضه می‌گردد و با توجه به رایگان بودن آن، به یکی از متداول‌ترین سیستم‌های تشخیص نفوذ شبکه‌های رایانه‌یی مبدل شده است. از آن‌جاکه برای معرفی آن نیاز به معرفی کوتاه این دسته از ابزارها داریم، ابتدا به مفاهیمی اولیه درباره‌ی ابزارهای تشخیص نفوذ می‌پردازیم، به عبارت دیگر معرفی این نرم‌افزار بهانه‌یی است برای ذکر مقدمه‌یی در باب سیستم‌های تشخیص نفوذ.

Intrusion Detection System (IDS) یا سیستم تشخیص نفوذ به سخت‌افزار، نرم‌افزار یا تلفیقی از هر دو اطلاق می‌گردد که در یک سیستم رایانه‌یی که می‌تواند یک شبکه‌ی محلی یا گسترده باشد، وظیفه‌ی شناسایی تلاش‌هایی که برای حمله به شبکه صورت می‌گیرد و ایجاد اخطار احتمالی متعاقب حملات، را بر عهده دارد.

IDSها عملاً سه وظیفه‌ی کلی را برعهده دارند: پایش، تشخیص، واکنش. هرچند که واکنش در مورد IDSها عموماً به ایجاد اخطار، در قالب‌های مختلف، محدود می‌گردد. هرچند دسته‌یی مشابه از ابزارهای امنیتی به نام Intrusion Prevention System (IPS) وجود دارند که پس از پایش و تشخیص، بسته‌های حمله‌های احتمالی را حذف می‌کنند. نکته‌یی که در این میان باید متذکر شد، تفاوت و تقابل میان Firewallها و IDSها است. از آن‌جاکه ماهیت عمل‌کرد این دو ابزار با یکدیگر به کلی متفاوت است، هیچ‌یک از این دو ابزار وظیفه‌ی دیگری را به طور کامل برعهده نمی‌گیرد، لذا تلفیقی از استفاده از هردو ابزار می‌تواند امنیت کلی سیستم را بالا ببرد.

در حالت کلی IDSها را می‌توان به دو دسته‌ی کلی تقسیم‌بندی نمود :

- Network IDS (NIDS)
- Host IDS (HIDS)

HIDSها، اولین سیستم IDSی هستند که در یک سیستم رایانه‌ای باید پیاده‌سازی شود. معیار تشخیص حملات در این سیستم‌ها، اطلاعات جمع‌آوری شده بر روی خادم‌های مختلف شبکه است. برای مثال این سیستم با تحلیل صورت عملیات انجام شده، ذخیره شده در پرونده‌هایی خاص، سعی در تشخیص تلاش‌هایی که برای نفوذ به خادم مذکورد انجام شده است دارد. این تحلیل‌ها می‌تواند به صورت محلی بر روی خود خادم انجام گردد یا به سیستم تحلیل‌گر دیگری برای بررسی ارسال شود. یک **HIDS** می‌تواند تحلیل اطلاعات بیش از یک خادم را بر عهده بگیرد.

با این وجود، اگر نفوذگر جمع‌آوری صورت عملیات انجام‌شده بر روی هریک از خادم‌های مورد نظر را به نحوی متوقف کند، HIDS در تشخیص نفوذ ناموفق خواهد بود و این بزرگ‌ترین ضعف HIDS است.

NIDSها، به عنوان دومین نوع IDSها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌گیرد می‌پردازند. به عبارت دیگر معیار NIDSها، تنها بسته‌هایی است که بر روی شبکه‌ها رد و بدل می‌گردد. از آن‌جایی‌که NIDSها تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گسترده‌گی بیش‌تری داشته و فرایند تشخیص را به صورت توزیع‌شده انجام می‌دهند. با این وجود این سیستم‌ها در رویایی با بسته‌های رمزشده و یا شبکه‌هایی با سرعت و ترافیک بالا کارایی خود را از دست می‌دهند.

با معرفی انجام شده در مورد دو نوع اصلی IDSها و ضعف‌های عنوان شده برای هریک، واضح است که برای رسیدن به یک سیستم تشخیص نفوذ کامل، بهترین راه استفاده‌ی همزمان از هر دو نوع این ابزارهاست.

Snort، در کامل‌ترین حالت نمونه‌یی از یک NIDS است. این نرم‌افزار در سه حالت قابل برنامه‌ریزی می‌باشد :

- حالت **Sniffer**

در این حالت، این نرم‌افزار تنها یک Sniffer ساده است و محتوای بسته‌های ردوبدل شده بر روی شبکه را بر روی کنسول نمایش می‌دهد.

- حالت ثبت‌کننده‌ی بسته‌ها

Snortدر این وضعیت، اطلاعات بسته‌های شبکه را در پرونده‌یی که مشخص می‌شود ذخیره می‌کند.

- سیستم تشخیص نفوذ

در این پیکربندی، بر اساس دو قابلیت پیشین و با استفاده از قابلیت تحلیل بسته‌ها و قوانینی که تعیین می‌گردد، Snort امکان پایش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را به‌روز می‌دهد.

حالت پیش‌فرض خروجی این ابزار فایلی متنی است که می‌تواند در آن ابتدای بسته‌ها را نیز درج کند. با این وجود در صورتی‌که این ابزار در حال فعالیت بر روی ارتباطات شبکه‌یی با سرعت بالا می‌باشد به‌ترین راه استفاده از خروجی خام باینری و استفاده از ابزاری ثانویه برای تحلیل و تبدیل اطلاعات خروجی است.

بُعد دیگر از پیکربندی Snort به عنوان یک سیستم تشخیص نفوذ، استفاده از قوانین برای ایجاد معیار نفوذ برای Snort است. برای مثال می‌توان با قانونی، Snort را مکلف

ساخت که نسبت به دسترسی‌های انجام شده مبتنی بر پروتکلی تعیین شده از/ به یک پورت خاص و از/ به یک مقصد معین با محتوایی شامل رشته‌یی خاص، اخطاری یا واکنشی ویژه را اعمال کند.

نکته‌یی که باید در نظر داشت این است که از آن‌جاکه Snort را می‌توان به گونه‌یی پیکربندی نمود که قابلیت تشخیص حمله توسط ابزارهای پویش پورت را نیز داشته باشد، لذا با وجود استفاده از Snort نیازی به استفاده از ابزاری ثانویه برای تشخیص پویش‌گرهای پورت وجود ندارد.

همان‌گونه که گفته شد، Snort با قابلیت‌های نسبتاً کاملی که در خود جای داده‌است، به همراه رایگان بودن آن و قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متدوال، به یکی از معمول‌ترین IDSهای کنونی مبدل شده است. برای دریافت این نرم‌افزار و همچنین اطلاعات جامعی در مورد آن می‌توانید به پایگاه اصلی آن، www.snort.org، مراجعه کنید.

Retina Network Security Scanner

این نرم‌افزار که محصولی از شرکت eEye Digital Security است، کاربردی مشابه Scanner LANGuard Security دارد. از آنجاکه در این پایگاه مقدمه‌یی از نرم‌افزار LANGuard، به عنوان آشنایی با نرم‌افزارهای پویش امنیت در شبکه قرار گرفته است، در این متن ضمن معرفی Retina به مقایسه مختصر و اجمالی میان این دو محصول، که تحت Windows رقبای یکدیگر محسوب می‌شوند، نیز پرداخته خواهد شد.

پویش‌گر امنیت شبکه‌ی Retina، یکی از قوی‌ترین نرم‌افزارها در این دسته از محصولات به شمار می‌آید. امکانات و قابلیت‌های متنوع، به همراه امکان پویش در شبکه‌هایی که از سیستم‌های عامل متنوعی، همچون Windows و خانوادهی Linux و Unix استفاده می‌کنند، و همچنین امکان نصب اصلاحیه‌های امنیتی ویژه ضعف‌های امنیتی یافت شده که به‌صورت خودکار توسط **Retina** انجام می‌گیرد، این نرم‌افزار را به محصولی خاص و قدرتمند تبدیل می‌کند، تا حدی که اغلب مجلات و منابعی که در زمینه‌ی بررسی چنین نرم‌افزارهایی از اعتباری بالا برخوردارند، آن‌را به عنوان محصولی برتر معرفی می‌کنند.

از امکانات ویژه و منحصربه‌فرد این نرم‌افزار، که در دیگر پویش‌گرهای امنیت شبکه‌ی مشابه یافت نمی‌شود، می توان به امکان Auditing آن اشاره کرد. توسط Auditing Tool این نرم‌افزار می‌توان در زمان پویش، دسته‌یی خاص از ضعف‌های امنیتی را برای تعدادی از ایستگاه‌های کاری یا خادم‌های تعیین شده اعمال کرد. همچنین در این ابزار امکان اضافه نمودن ضعفی جدید، به صورت دستی، توسط مدیر شبکه نیز وجود دارد. به عبارت دیگر، می‌توان گزارشی از وضعیت تعدادی رایانه‌ی خاص در برابر ضعف‌هایی معین، تهیه نمود و در صورت نیاز اقدام به نصب خودکار اصلاحیه‌های امنیتی نمود.

این پویش‌گر، با استفاده از بازه‌یی از آدرس‌های IP به پویش شبکه می‌پردازد و ضعف‌های امنیتی را بر اساس بحرانی‌بودن آن‌ها مرتب می‌کند. همان‌گونه که گفته شد می‌توان بررسی امنیتی شبکه را محدود به دسته‌ی خاصی از ضعف‌های، نرم‌افزارها و یا جنبه‌های امنیتی نمود. در این میان شاید تنها ایرادی، آن هم از بعد گزارش‌گیری و رابط کاربری، می‌توان به این نرم‌افزار وارد دانست، نبود امکان مرتب‌سازی ایستگاه‌های پویش‌شده بر اساس نوع سیستم‌عامل آن‌هاست.

در هنگام نصب، پویش‌گر، اقدام به اتصال به پایگاه داده‌ی اصلی شرکت سازنده کرده و به به‌روز سازی ضعف‌های امنیتی شناخته شده می‌پردازد. این اقدام با هدف کاهش احتمال نادیده انگاشتن ضعف‌های نوین امنیتی صورت می‌گیرد.

حفاظ شخصی Zone Alarm

استفاده از حفاظ‌های شخصی، در دنیای کنونی که اغلب حملات امنیتی و ویروس‌ها، کاربران عادی خانه‌گی را هدف قرار داده‌اند، اهمیتی ویژه یافته است.

شرکت ZoneLabs با ارایه‌ی این نرم‌افزار، عملاً خود را در بازار این دسته از نرم‌افزارها مبدل به حریفی بی‌رقیب نموده است. رقبای دیگر این نرم‌افزار محصولات مشابه دیگری از McAfee و Norton هستند.

مهم‌ترین امکانات و قابلیت‌های این نرم‌افزار را می‌توان به‌صورت زیر برشمرد:

- محدود ساختن دسترسی نرم‌افزارهای مختلف بر روی رایانه

این نرم‌افزار قابلیت بررسی وضعیت ارتباط نرم‌افزارهای نصب شده بر روی سیستم با شبکه را داراست. لذا در صورتی‌که نرم‌افزاری ناشناس سعی در تماس به شبکه داشته باشد، می‌توان این دسترسی را محدود ساخت.

- محدودیت بر روی آدرس‌ها، پورت‌ها و پروتکل‌ها

توسط این امکان می‌توان از دسترسی‌هایی که از بیرون از رایانه‌مان صورت می‌گیرد، در قالب آدرس IP، پورت و پروتکل مورد نظر آگاهی یافت و در

صورت نیاز این دسترسی را بست. از سوی دیگر می‌توان آدرس‌ها، پورت‌ها و پروتکل‌هایی که دسترسی از طریق آن‌ها به سیستم مانعی ندارد را مشخص نمود.

- **امکان حفاظت از اطلاعات شخصی**

توسط این امکان، و با پاک کردن Cacheهای مختلف پرونده‌ها، آدرس‌ها، Cookieها و دیگر اطلاعات شخصی حساس مشابه، می‌توان از درز کردن اطلاعات شخصی مهمی از این قبیل به شبکه جلوگیری نمود.

- **سیستم محافظت از سرویس پست الکترونیک**

توسط این امکان، نامه‌های ورودی به سیستم، که احتمال آلوده‌گی آن‌ها وجود دارد را مسدود ساخت. از سوی دیگر در صورت آلوده بودن سیستم به ویروس‌هایی که خود را از طریق ارسال نامه به دریافت‌کننده‌گانی که آدرس آنها در فهرست آدرس برنامه‌ی ارسال پست‌الکترونیک موجود است، منتشر می‌کنند، می‌توان جلو این انتشار را با مسدود ساختن نامه‌های ارسالی گرفت.

- **صدور اخطارهای امنیتی**

جدا از گزارش حملات احتمالی، درصورتی‌که قصد ارسال اطلاعات به شبکه را داشته باشیم، هشدارهای امنیتی از سوی این نرم‌افزار توجه استفاده کننده را به دقت بیشتر در این زمینه جلب می‌کند.

- **تغییر سطح امنیت به صورت خودکار**

در صورت بروز حملات متعدد امنیتی، نرم‌افزار به طور خودکار سطح حفاظت را بالاتر می‌برد. این امکان احتمال دفع حملات را بالا می‌برد.

آخرین نگارش این نرم‌افزار نسخه‌ی ۴ است که کماکان بیشترین اقبال را در میان این دسته از نرم‌افزارها به خود جلب کرده، و بیشترین محبوبیت و کارایی را در میان کاربران عادی یافته است.

مقدمه‌ای بر SSH

SSH که مخفف Secure Shell می‌باشد، به‌طور عمومی به برنامه‌یی اطلاق می‌گردد که برای دسترسی امن به رایانه‌یی از راه دور، برای اجرای فرامین یا انتقال پرونده‌ها، مورد استفاده قرار می‌گیرد. علت اهمیت چنین روش‌هایی، اقدامات معمول نفوذگران در قالب پویش شبکه برای آگاهی از محتوای بسته‌ها، استفاده از IPهای جعلی و سرقت آدرس‌های IP، تهدیدات سرویس‌های DNS و دیگر روش‌های حمله است. عملاً با رمزکردن کانال ارتباطی میان کاربر و خادم، احتمال هریک از این حملات در پی اقدامات نفوذگران به حداقل می‌رسد.

با وجود آن‌که SSH به برنامه‌یی که این وظیفه را بر عهده دارد اطلاق می‌گردد، ولی تمامی این برنامه‌ها از استاندارد واحدی تبعیت می‌کنند. در نگارش جدید آن به نام SSH2، نرم‌افزاری به نام sftp برای برعهده‌گرفتن وظیفه‌ی FTP Clientها نیز وجود دارد. طبق آمارهای تقریبی ارایه شده، قریب به ۲ میلیون کاربر از نسخه‌های مختلف برنامه‌های متنوع SSH تحت سیستم‌های عامل مختلف استفاده می‌کنند.

نکته‌یی که لازم به گفتن است، تفاوت میان پروتکل‌های استفاده شده در SSH1 و SSH2 است. به بیان دیگر این دو استاندارد با یکدیگر سازگاری ندارند. استانداردی که SSH1 بر مبنای آن است را می‌توان از آدرس

http://www.tigerlair.com/ssh/faq/ssh1-draft.txt به‌دست آورد و

برای آگاهی از استاندارد SSH2 می‌توانید به آدرس

http://www.ietf.org/ids.by.wg/secsh.html مراجعه کنید. در حال حاضر، پشتیبان این استاندارد IETF است. با این وجود تعداد زیادی از شرکت‌ها نرم‌افزارهایی بر اساس این استاندارد تولید می‌کنند که برخی رایگان و برخی تجاری است.

برای استفاده از SSH، نیاز به سرویس و نرم‌افزاری داریم که در سوی خادم نصب می‌گردد. پس از آن نرم‌افزاری به عنوان مخدوم، کانال ارتباطی را ایجاد کرده و ارتباط امن برقرار می‌گردد. در حال حاضر سرویس‌ها و نرم‌افزارهای مخدوم برای سیستم‌های عامل مختلفی از جمله Windows، Macintosh، خانواده‌ی Unix، PalmOS، OS/2 و سیستم‌های عامل کم استفاده‌یی همچون VMS موجود است.

نکته‌یی که در این میان اهمیتی خاص دارد، مقایسه‌ی میان SSH1 و SSH2 است و اینکه باید از کدام یک از این استانداردها و نرم‌افزارهای مبتنی بر آن‌ها استفاده کرد؟ پاسخ به این سؤال چندان ساده نیست زیرا کماکان نرم‌افزارهای بسیاری وجود دارند که بر مبنای SSH1 هستند و عملاً این استاندارد SSH1 است که برای تمامی سیستم‌های عامل و محیط‌ها توسعه یافته و نرم‌افزارهایی بر مبنای آن تولید شده‌اند. با این وجود عملاً توسعه‌ی SSH1 متوقف شده است و تولیدکننده‌گان نرم‌افزار تنها بر روی SSH2 تمرکز کرده‌اند. از علل این تغییر می‌توان به ضعف‌های امنیتی موجود در ساختار SSH1، امکان حملات شناخته شده‌یی مانند نوع man-in-the-middle در مورد آن و احتمال رخداد حملات پیش‌بینی‌نشده، اشاره کرد.

Windows XP Service Pack 2

هدف اصلی SP2، بهبود امنیت کاربران ویندوز XP است که این کار را با ٤ رویکرد انجام می دهد:

- محافظت بهتر از شبکه
- بهبود حفاظت از حافظه
- ایمن سازی امور مربوط به E-Mail
- امنیت در مرور اینترنت (توسط Internet Explorer)

محافظت از شبکه با فایروال پیشرفت کرده ویندوز است (که قبلا تحت عنوان Internet Firewall Connection وجود داشت) که به صورت پیش فرض فعال می باشد. این فایروال در مراحل اولیه بوت شدن ویندوز، قبل از اینکه Network Stack فعال شود، شروع به کار می کند و نفوذ گر در مراحل اولیه بالا آمدن سیستم هم نمی تواند آن را مورد حمله قرار دهد. همچنین هنگام خاموش شدن سیستم نیز، این فایروال بسیار دیر خاموش می شود و بعد از اینکه لایه های شبکه غیر فعال شدند، این فایروال کار خود را پایان می دهد. این فایروال دارای واسط کاربری قابل قبولی برای مدیریت آن می باشد و قابل مدیریت و اعمال سیاست از سوی مدیر شبکه یا همان Domain Administrator می باشد. همچنین از IPv6 که در این نسخه از ویندوز ارائه شده است نیز پشتیبانی می کند.

RPC که در دو سال گذشته، هدف حملات اصلی کرم های اینترنتی بود نیز در این نسخه از ویندوز بهبود یافته است. آسیب پذیری کمتر، سطوح دسترسی بیشتر و همچنین

امکان استفاده از آن در شبکه های محدود و مدیریت آن برای جلوگیری از حملات خارج از شبکه از بهبودهایی است که در RPC صورت گرفته است.

مدیریت دسترسی بیشتر روی DCOM [3] برای پایین آوردن احتمال حمله از این طریق، از ویژگی های دیگر SP2 است. در این نسخه، تنها مدیران تایید هویت شده حق اتصال و فعال کردن از راه دور اجزا COM را دارند و تنها کاربران تأئید هویت شده می توانند به صورت از راه دور، COMها را صدا(Call) کنند.

ویژگی امنیتی قابل توجه دیگر در SP2، حمایت و پشتیبانی از پردازنده های با تکنولوژی NX است. در این مدل، ویندوز صفحه های حافظه که مربوط به Data هستند را برچسب غیر اجرایی (non-executable) می زند و بدین طریق، از بسیاری از حملات Buffer Overflow که با فرستادن Data به صورت خاص، ویندوز را وادار به اجرای آن می کردند، جلوگیری می شود. شایان ذکر است که در حال حاضر، تنها پردازنده هایی که NX را پشتیبانی می کنند، پردازنده های ٦٤ بیتی AMD K8 و Intel Itanium هستند که مایکروسافت امیدوار است سایر پردازنده های ٣٢ و ٦٤ بیتی به زودی از این تکنولوژی استفاده کنند و این امنیت سخت افزاری را برای کاربران فراهم آورند.

در زمینه جلوگیری از Buffer Overflow، علاوه بر پشتیبانی از NX، ویژگی دیگری موسوم به Sandboxing را نیز در ویندوز پیاده سازی کرده اند که طی آن، کلیه کدهای باینری قبل از اجرا، دوباره کامپایل می شوند و ویژگیهای امنیت بافر در آن فعال می شود تا runtime libraryهایی بتوانند در حال اجرا، حملات مبتنی بر Buffer overflow را تشخیص دهند و از آن جلوگیری کنند و Cookieهایی به heap افزوده می شود تا بتواند حملات heap buffer overflow رانیز محافظت کند.

با ارائه نسخه جدیدی از Outlook Express در SP2، از عکسها و کلیه محتوای خارجی جلوگیری می شود، در مورد سایر برنامه ها که قصد فرستادن E-Mail

را دارند، هشدار داده می شود و روی باز کردن و ذخیره کردن ضمیمه نامه ها(Email Attachments) نیز کنترل صورت می گیرد.

برای کنترل اجرای ضمیمه های آسیب رسان، از سرویس دیگری به نام Application New Execution Servic استفاده می شود. همچنین کاربران این امکان را دارند تا همه نامه ها را به صورت Plain Text یا متنی مشاهده کنند و بدین وسیله از حملاتی که بالقوه ممکن است در HTML صورت پذیرد، جلوگیری کنند. Windows Messenger و Messenger MSN نیز از بهبودهای Attachment استفاده می کنند. بهبود امنیت Internet Explorer از دغدغه های اصلی SP2 است. مدیریت add-onها و تشخیص توقف سیستم (Crash) مربوط به آنها، کنترل اینکه آیا اطلاعات باینری اجازه اجرا دارند یا خیر، به کار بردن محدودیت های امنیتی برای همه URL Objectها که قبلا تنها در مورد ActiveXها وجود داشت و کنترل روی اجرای همه نوع محتوا (Content) از ویژگی های SP2 هستند. SP2 IE به صورت جدی، امکانات Local Machine Zone را محدود کرده است تا از حملاتی که از این ناحیه امنیتی برای اجرای HTMLهای مخرب استفاده می کردند، جلوگیری کند. همچنین IE بر سازگاری اطلاعات همه انواع فایلها که از طرف سرورها فرستاده می شود، نظارت می کند که اطلاعاتی که برای یک نوع فایل خاص فرستاده می شود از همه نظر مطابق آنچه مورد انتظار است باشد؛ همچنین فایلها را sniff می کند تا کدهای مخرب را درون فایلهای ظاهرا بی خطر شناسایی کند.IE SP2 از دسترسی به cached scriptable object جلوگیری می کند، یعنی صفحه های HTML تنها به اشیاء مربوط به خود دسترسی دارند و بدین وسیله، از حملاتی که روی مدل cross-domain security model انجام می شوند تا حد زیادی جلوگیری می کند، به scriptها اجازه نمی دهد که به رخدادها

(events) و محتوای سایر فریم ها گوش دهند و مثلا از دزدیده شدن اطلاعات مربوط به Credit Card در یک فرم دیگر جلوگیری می کند. از ویژگی های دیگر IE، قابلیت جلوگیری از پنجره های pop-up ناخواسته است و کاربر می تواند به دلخواه خود، pop-upها را مدیریت کند. IE همچنین از اطلاعات امضا شده توسط منبع غیر مطمئن جلوگیری می کند، کد های امضا شده با امضای الکترونیکی غیر معتبر را به صورت پیش فرض مانع می شود. همچنین IE از کدهای مربوط به تغییر اندازه پنجره ها و تغییر status bar محافظت می کند.

در SP2، با استفاده از DirectX 9 و Windows Media Player 9، ویژگی های امنیتی، سرعت و کارایی آنها را افزایش داده است. با افزودن امکاناتی به سیستم Update ویندوز، به روز رسانی و نصب patchها را سریع، ساده، اتوماتیک و امن تر کرده است و حجم این Patchها از این پس، بسیار کمتر خواهد بود و بخش عمده کار به عهده Installer خواهد بود. با استفاده از Windows Installer ۳،۰، امکانات زیادی در زمینه امنیت در نصب برنامه ها افزوده شده است و سیستم مدیریت patchها و حجم کمتر patchها را با استفاده از تکنولوژی Delta Compression فراهم کرده است و patch removal را نیز قابل اطمینان تر کرده است. وجود Windows Security Center از امکانات جدید ویندوز SP2 است که با فراهم کردن یک محیط user friendly و ثابت برای کاربر، امکان مدیریت امنیتی متمرکز ویندوز را برای کاربران فراهم می کند. مدیریت فایروال ویندوز، به روز رسانی ویندوز، گزینه های امنیتی اینترنت و محافظت در مقابل ویروسها از امکانات این محیط است. این امکان وجود دارد تا در این محیط از فایروال خود ویندوز استفاده شود و یا تولید کنندگان دیگر فایروال شخصی، محصولات خود را برای این محیط سازگار کنند. درمورد Anti-Virus این امکان در Security Center قرار داده شده تا سایر شرکتهای تولید کننده Anti-Virus خود را با این محیط مطابقت دهند و هنوز مایکروسافت راه حل مستقلی در این زمینه ندارد.

نرم افزارهای ضدویروس

با استفاده از نرم افزارهای ضد ویروس، امکان شناسائی و بلاک نمودن ویروس ها قبل از آسیب رساندن به سیستم شما، فراهم می گردد. با نصب این نوع نرم افزارها بر روی سیستم خود یک سطح حفاظتی مناسب در خصوص ایمن سازی کامپیوتر و اطلاعات موجود بر روی آن ایجاد خواهد شد. به منظور استمرار سطح حفاظتی ایجاد شده، می بایست نرم افزارهای ضدویروس بطور دائم بهنگام شده تا امکان شناسائی ویروس های جدید، وجود داشته باشد.

نرم افزارهای ضد ویروس، چه کار می کنند ؟

جزئیات عملکرد هر یک از برنامه های ضد ویروس با توجه به نوع هر یک از نرم افزارهای موجود، متفاوت است. اینگونه نرم افزارها فایل های موجود بر روی کامپیوتر و یا حافظه کامپیوتر شما را به منظور وجود الگوهائی خاص که می تواند باعث ایجاد آلودگی گردند را پویش می نمایند. برنامه های ضد ویروس بدنبال الگوهائی مبتنی بر علائم خاص، تعاریفی خاص و یا ویروس های شناخته شده، می گردند. نویسندگان ویروس های کامپیوتری همواره اقدام به نوشتن ویروس های جدید نموده و ویروس های نوشته شده قبلی خود را بهنگام می نمایند. بنابراین لازم است که همواره بانک اطلاعاتی شامل تعاریف و الگوهای ویروس های کامپیوتری مربوط به نرم افزار، بهنگام گردد. پس از نصب یک نرم افزار آنتی ویروس بر روی کامپیوتر خود، می توان عملیات پویش و بررسی سیستم به منظور آگاهی از وجود ویروس را در مقاطع زمانی مشخص و بصورت ادواری انجام داد. در این رابطه می توان از دو گزینه متفاوت استفاده نمود:

- **پویش اتوماتیک** : برخی از برنامه های ضد ویروس دارای پتانسلی به منظور پویش اتوماتیک فایل ها و یا فولدرهائی خاص و در یک محدوده زمانی مشخص شده ، می باشند.

- **پویش دستی** : پیشنهاد می گردد، پس از دریافت هرگونه فایلی از منابع خارجی و قبل از فعال نمودن و استفاده از آن، عملیات بررسی و پویش آن به منظور شناسائی ویروس صورت پذیرد. بدین منظور عملیات زیر توصیه می گردد:

– ذخیره و پویش ضمائم نامه های الکترونیکی و یا نرم افزارهائی که از طریق اینترنت Download می نمائید(هرگز ضمائم نامه های الکترونیکی را مستقیما" و بدون بررسی آن توسط یک برنامه ضد ویروس، فعال ننمائید).

– بررسی فلاپی دیسک ها، CD و یا DVD به منظور یافتن ویروس بر روی آنان قبل از باز نمودن هر گونه فایلی

نحوه برخورد نرم افزار ضدویروس با یک ویروس

نرم افزارهای ضد ویروس به منظور برخورد با یک ویروس از روش های متفاوتی استفاده می نمایند. روش استفاده شده می تواند با توجه به مکانیزم پویش (دستی و یا اتوماتیک) نیز متفاوت باشد. در برخی موارد ممکن است نرم افزار مربوطه با ارائه یک جعبه محاوره ای، یافتن یک ویروس را به اطلاع شما رسانده و به منظور برخورد با آن از شما کسب تکلیف نماید . در برخی حالات دیگر، نرم افزار ضدویروس ممکن است بدون اعلام به شما اقدام به حذف ویروس نماید. در زمان انتخاب یک نرم افزار ضد ویروس، لازم است به ویژگی های ارائه شده و میزان انطباق آنان با انتظارات موجود، بررسی کارشناسی صورت پذیرد.

از کدام نرم افزار می بایست استفاده نمود ؟

تولید کنندگان متعددی اقدام به طراحی و پیاده سازی نرم افزارهای آنتی ویروس می نمایند. عملکرد این نوع نرم افزارها مشابه یکدیگر می باشد. به منظور انتخاب یک نرم افزار ضد ویروس می توان پارامترهای متعددی نظیر ویژگی های ارائه شده توسط نرم افزار، قیمت و میزان انطباق آنان با خواسته های موجود را بررسی نمود.

نصب هر نوع نرم افزار ضد ویروس (صرفنظر از نرم افزاری انتخاب شده)، باعث افزایش حفاظت شما در مقابل ویروس ها می گردد. برخی از پیام های ارسالی که ادعا می نمایند شامل نرم افزارهای ضدویروس بوده و یا اینگونه نرم افزارها را به شما معرفی می نمایند، خود به منزله یک ویروس بوده و می بایست دقت لازم در خصوص بازنمودن آنان و ضمائم مربوطه را داشته باشیم.

چگونه می توان از آخرین اخبار و اطلاعات مربوط به ویروس ها، آگاهی یافت ؟

فرآیند بهنگام سازی در هر نرم افزار ضدویروس متفاوت بوده و می بایست در زمان انتخاب اینگونه نرم افزارها، پتانسیل آنان در خصوص بهنگام سازی بانک اطلاعاتی تعاریف الگوها، بررسی گردد. تعداد زیادی از نرم افزاری ضد ویروس دارای گزینه ای به منظور بهنگام سازی اتوماتیک، می باشند. استفاده از پتانسیل فوق با توجه ایجاد ویروس های جدید، امری لازم و اجتناب ناپذیر است. نصب یک نرم افزار ضد ویروس، یکی از ساده ترین و در عین حال موثرترین روش های حفاظت از کامپیوتر است. آیا صرفا" با یک نصب همه چیز تمام شده و ما همواره دارای ایمنی لازم و حفاظت مطلوب خواهیم بود؟ پاسخ به سوال فوق قطعا" منفی بوده و این نوع نرم افزارها دارای محدودیت های خاص خود نیز می باشند. نرم افزارهای ضد ویروس به منظور شناسائی و برخورد با ویروس ها از الگوهای شناخته شده، استفاده می نمایند. بنابراین طبیعی است که اینگونه نرم افزارها صرفا" قادر به شناسائی و برخورد با ویروس هائی می باشند که قبلا" الگوی آنان برای نرم افزار معرفی شده باشد. به منظور حفظ اقتدار نرم افزارهای ضد ویروس و کمک به آنان در جهت شناسائی و برخورد با ویروس های جدید، می بایست فرآیند بهنگام سازی آنان بطور مداوم و در محدوده های زمانی مشخص، تکرار گردد.

قابلیت‌های نرم‌افزارهای ضدویروس

قابلیت‌های نرم‌افزارهای ضدویروس وتفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهای e-mail، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد.

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می‌کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

حافظت e-mail

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است. تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند.

از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای e-mail با برنامه‌های اداری باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و W32.Klez به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانند Fat16، Fat32، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همه e-mailها از دست بروند. به عنوان مثال کرم W32.Klez که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail

داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌های Microsoft Outlook Express، Microsoft Outlook، Netscape Messenger، Netscape، Eudora Pro و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس‌گیرنده‌های POP3 و MAPI را مطرح می‌کنند.

بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصـــص زیاد نیست.

تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است. شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند.

طرز کار برنامه های ضد ویروس

ضد ویروس اصطلاحی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند. مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن (Scanning engine) آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلوده به ویروس را با استفاده از فایل امضای ویروس ها بر عهده دارند. فایل امضای ویروس یک رشته بایت است که با استفاده از آن می توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسان ها می باشد. ضد ویروس متن فایل های موجود در کامپیوتر را با نشانه های ویروس های شناخته شده مقایسه می نماید. در بیشتر موارد در صورتی که فایل آلوده باشد برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد و حتی می توان تنظیمات ضدویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.

بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جدیدی که هنوز فایل امضای آنها ارائه نشده از روش های جستجوی ابتکاری استفاده می کنند. به این ترتیب

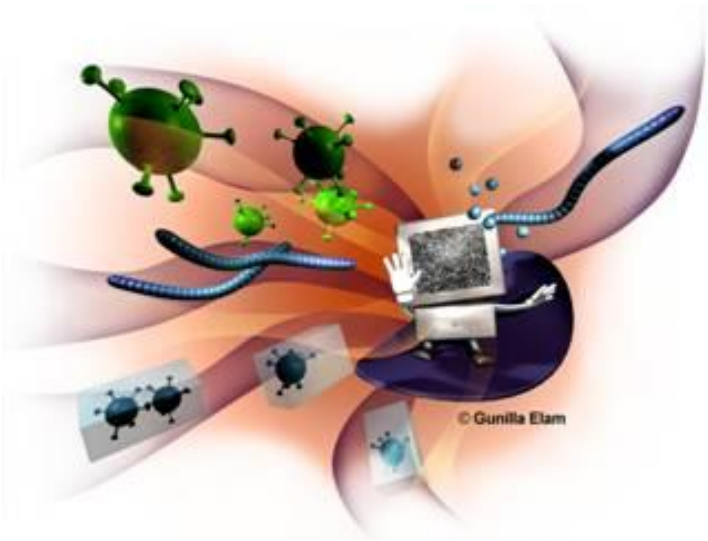
داده های مشکوک در فایل های موجود در سیستم و یا فعالیت های مشکوک مشابه رفتار ویروس ها (حتی در صورتی که تعریف ویروسی منطبق با آنچه که در فایل مشکوک یافت شده موجود نباشد) علامت گذاری می شوند. اگر ضد ویروس فعالیت مشکوکی را مشاهده نماید، برنامه ای که فعالیت مشکوک انجام داده را قرنطینه نموده و به کاربر در مورد آن اعلام خطر می کند (به عنوان مثال اعلام می شود که برنامه مشکوک مایل به تغییر Windows Registry می باشد). دقت این روش پایین است و در بسیاری از مواقع در شناخت فایل های مشکوک به ویروس اشتباهاتی رخ می دهد.

در چنین مواقعی فایل قرنطینه شده برای شرکت های سازنده ضد ویروس ها ارسال می شود که پس از تحقیق و آزمایش آن، در صورتی که واقعا فایل آلوده به ویروس باشد نام، امضاء و مشخصات آن مشخص شده و پادزهر آن ارائه می گردد. در این صورت کد مشکوک تبدیل به یک ویروس شناخته شده می شود.

قابلیت های نرم افزار های ضدویروس

سطح محافظت نرم افزار بسته به جدید و بروز بودن آن متغیر است. محصولات جدیدتر قابلیت های مانند بروز رسانی خودکار، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های

کاربردی اینترنتی مانند برنامه های e-mail و مرورگرهای وب را دارند. نسخه های قدیمی تر نرم افزارهای ضدویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند. همه نرم افزار های ضدویروس در صورتی که به صورت منظم به روز رسانی شده و عملیات اسکن بر روی دیسک های سخت، تجهیزات قابل انتقال (مانند فلاپی و Zip disk) انجام شود می توانند دستگاه کامپیوتر را در برابر ویروس ها مقاوم کنند. در واقع نقطه برتری محصولات جدید ضد ویروس در قابلیت های آنها برای محافظت از سیستم در مواقعی است که کاربر دانش و یا دقت لازم برای به کارگیری آن را ندارد.



حداقل توقعی که از یک برنامه ضد ویروس خوب می توان داشت این است که در برابر ویروس های boot-sector، ماکرو، اسب های تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد. از محصولات جدیدتر می توان انتظار محافظت در برابر صفحات وب، اسکریپت ها، کنترل های ActiveX و اپلت های جاوای خطرناک، همچنین کرم های e-mail را داشت.

امید است مطالب ارائه شده در این کتاب، برای همکاران فنی، مفید وقابل استفاده واقع شود. در همین جا بر خود لازم می دانم از مدرس محترم دوره **MCSE** ، جناب آقای مهدی ساسانی وهمکارانی که درتهیه این کتاب بنده را یاری کـــرده اند، آقایان اصغرکشاورز مهدی شیبانی، بابک محمودی خانمها قریشی، انصاری و نوروزی تشکر و قدردانی بعمل آورم. لازم بذکر میباشد تنظیم این مجموعه حدوداً ۹ ماه به طول انجامیده است.

(التماس دعا)

آشنایی با تعاریف سیستم های
نرم افزاری و شبکه
تحقیق و گردآوری : غلامرضا امیریان
shihanamirian@gmail.com