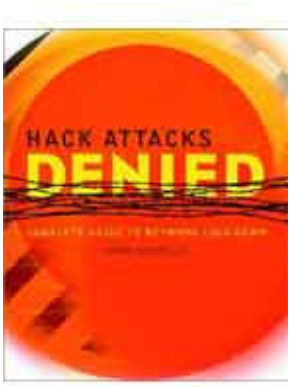
انواع حملات در شبکه های کامپیوتری



امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله موضوعاتی است که این روزها در کانون توجه تمامی سازمان ها و موسسات قرار گرفته شده است . در یک شبکه کامپیوتری به منظور ارائه خدمات به کاربران ، سرویس ها و پروتکل های متعددی نصب و پیکربندی می گردد. برخی از سرویس ها دارای استعداد لازم برای انواع حملات بوده و لازم است در مرحله اول و در زمان نصب و پیکربندی آنان ، دقت لازم در خصوص رعایت مسائل ایمنی انجام و در مرحله دوم سعی گردد که از نصب سرویس ها و پروتکل های غیرضروری ، اجتناب گردد . در این مقاله قصد داریم از این زاویه به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری پرداخته و در ادامه با انواع حملاتی که امروزه متوجه شبکه های کامپیوتری است ، بیشتر آشنا شویم . قطعا" شناسائی سرویس های غیرضروری و انواع حملاتی که مهاجمان با استفاده از آنان شبکه های کامپیوتری را هدف قرار می دهند ، زمینه برپاسازی و نگهداری شبکه های کامپیوتری ایمن و مطمئن را بهتر فراهم می نماید .

مقدمه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس ها ی فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطمینان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین) . در زمان ارائه سرویس دهندگان ، مجموعه ای از سرویس ها و پروتکل ها به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال شده اند.این موضوع ارتباط مستقیمی با سیاست های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهائی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند.

اولین مرحله در خصوص ایمن سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص ایمن سازی شبکه را شامل می شود . هر نوع برنامه ریزی در این رابطه مستلزم توجه به موارد زیر است :

- بررسی نقش هر سرویس دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- انطباق سرویس ها ، پروتکل ها و برنامه های نصب شده با خواسته ها ی یک سازمان
- بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس ها و پروتکل های غیرضروری ، تنظیم دقیق امنیتی سرویس ها و پروتکل های فعال) .

تعلل و یا نادیده گرفتن فاز برنامه ریزی می تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد . متاسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری ها به سرعت و به صورت مستمر در حال تغییر بوده و می بایست متناسب با فن آوری های جدید ، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس دهندگان و کاهش نقاط آسیب پذیر آنان با جدیت دنبال شود . نشستن پشت یک سرویس دهنده و پیکربندی آن بدون وجود یک برنامه مدون و مشخص ، امری بسیار خطرناک بوده که بستر لازم برای بسیاری از حملاتی که در آینده اتفاق خواهند افتاد را فراهم می نماید . هر سیستم عامل دارای مجموعه ای از سرویس ها ، پروتکل ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل های آنان در جهت افزایش کارائی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنان با توجه به شرایط موجود و فن آوری های جدید ارائه شده ، اعمال گردد . فراموش نکنیم که حتی راه حل های انتخاب شده فعلی که دارای عملکردی موفقیت آمیز می باشند ، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح ، نباشند .

وظیفه یک سرویس دهنده

پس از شناسائی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس ها و پروتکل های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم گیری نمود . برخی از سرویس دهندگان به همراه وظیفه آنان در یک شبکه کامپیوتری به شرح زیر می باشد :

Logon Server : این نوع سرویس دهندگان مسئولیت شناسائی و تائید کاربران در زمان ورود به شبکه را برعهده دارند . سرویس دهندگان فوق می توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس دهندگان نیز انجام دهند .

Network Services Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن سـرویس های مورد نیاز شبکه را برعهده دارند . این سرویس ها عبارتند از :

- DHCP Dynamic Host Configuration (Protocol)
- DNS (Domain Name System)
- WINS Windows Internet Name (Service)
- SNMP (Simple Network Management Protocol)

Application Server : این نـوع از سـرویس دهنـدگان مسـئولیت میزبـان نمـودن برنامـه هـا ی کاربردی نظیر بسته نرم افزاری Accounting و سایر نرم افزارهای مورد نیاز در سازمان را برعهده دارند .

File Server : از این نوع سرویس دهندگان به منظور دستیابی به فایل ها و دایرکتوری ها ی کاربران ، استفاده می گردد .

Print Server: از این نوع سرویس دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشـته شـده در شبکه ، استفاده می شود.

Web Server: این نوع سرویس دهندگان مسئولیت میزبان نمودن برنامه هـای وب و وب سـایت هـای داخلی و یا خارجی را برعهده دارند.

FTP Server: این نـوع سـرویس دهنـدگان مسـئولیت ذخیـره سـازی فایـل هـا بـرای انجـام عملیـات Downloading و Uploading را برعهده دارند. سرویس دهندگان فوق می توانند به صورت داخلی و یا خارجی استفاده گردند .

Email Server: این نوع سرویس دهندگان مسئولیت ارائه سرویس پست الکترونیکی را برعهده داشـته و می توان از آنان به منظور میزبان نمودن فولدرهای عمومی و برنامه های Groupware ، نیز استفاده نمود.

News/Usenet (NNTP) Server: این نوع سرویس دهندگان به عنوان یک سرویس دهنده newsgroup بوده و کاربران می توانند اقدام به ارسال و دریافت پیام هائی بر روی آنان نمایند .

به منظور شناسائی سرویس ها و پروتکل های مورد نیاز بر روی هر یک از سرویس دهندگان ، می بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنان به چه صورت است ؟ : شبکه داخلی ، شبکه جهانی و یا هر دو مورد . پاسخ به سوال فوق زمینه نصب و پیکربندی سرویس ها و پروتکل های ضروری و حذف و غیر فعال نمودن سرویس ها و پروتکل های غیرضروری در ارتباط با هر یک از سرویس دهندگان موجود در یک شبکه کامپیوتری را فراهم می نماید .

سرویس های حیاتی و موردنیاز

هر سیستم عامل به منظور ارائه خدمات و انجام عملیات مربوطه ، نیازمند استفاده از سرویس های متفاوتی است . در حالت ایده آل ، عملیات نصب و پیکربندی یک سرویس دهنده می بایست صرفا" شامل سرویس ها و پروتکل های ضروری و مورد نیاز به منظور انجام وظایف هر سرویس دهنده باشد. معمولا" تولید کنندگان سیستم های عامل در مستندات مربوطه به این سرویس ها اشاره می نمایند. استفاده از مستندات و پیروی از روش های استاندارد ارائه شده برای پیکربندی و آماده سازی سرویس دهندگان ،زمینه نصب و پیکربندی مطمئن با رعایت مسائل ایمنی را بهتر فراهم می نماید .

زمانی که کامپیوتری در اختیار شما گذاشته می شود ، معمولا" بر روی آن نرم افزارهای متعددی نصب و پیکربندی های خاصی نیز در ارتباط با آن اعمال شده است . یکی از مطمئن ترین روش ها به منظور آگاهی از این موضوع که سیستم فوق انتظارات شما را متناسب با برنامه تدوین شده ، تامین می نماید ، انجام یک نصب Clean با استفاده از سیاست ها و لیست ها ی از قبل مشخص شده است . بدین ترتیب در صورت بروز اشکال می توان به سرعت از این امر آگاهی و هر مشکل را در محدوده خاص خود بررسی و برای آن راه حلی انتخاب نمود. (شعاع عملیات نصب و پیکربندی را به تدریج افزایش دهیم) .

مشخص نمودن پروتکل های مورد نیاز

برخی از مدیران شبکه عادت دارند که پروتکل های غیرضروری را نیز بر روی سیستم نصب نمایند ، یکی از علل این موضوع ، عدم آشنائی دقیق آنان با نقش و عملکرد هریک از پروتکل ها در شبکه بوده و در برخی موارد نیز بر این اعتقاد هستند که شاید این پروتکل ها در آینده مورد نیاز خواهد بود. پروتکل ها همانند سرویس ها ، تا زمانی که به وجود آنان نیاز نمی باشد ، نمی بایست نصب گردند . با بررسی یک محیط شبکه با سوالات متعددی در خصوص پروتکل های مورد نیاز برخورد نموده که پاسخ به آنان امکان شناسائی و نصب پروتکل های مورد نیاز را فراهم نماید .

- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) با سـرویس دهنـدگان ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس دهنده با سرویس دهنده ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) از راه دور بـا سـرویس دهندگان ، نیاز می باشد ؟
- آیا پروتکل و یا پروتکل های انتخاب شده ما را ملزم به نصب سرویس های اضافه ای می نمایند ؟
- آیا پروتکل های انتخاب شده دارای مسائل امنیتی خاصی بوده که می بایست مورد توجه و بررسی قرار گیرد ؟

در تعداد زیادی از شبکه های کامپیوتری ،از چندین سیستم عامل نظیر ویندوز ، یونیکس و یا لینوکس ، اسـتفاده می گردد . در چنین مواردی می توان از پروتکل TCP/IP به عنوان فصل مشترک بین آنان استفاده نمـود. در ادامه می بایست در خصوص فرآیند اختصاص آدرس های IP تصیم گیری نمود (به صورت ایستا و یا پویا و به کمک DHCP) . در صورتی که تصمیم گرفته شود که فرآیند اختصاص آدرس های IP به صورت پویـا و بـه کمک DHCP ، انجام شود، به یک سرویس اضافه و با نام DHCP نیاز خواهیم داشت . با این که استفاده از DHCP مدیریت شبکه را آسانتر می نماید ولی از لحاظ امنیتی دارای درجه پائین تـری نسـبت بـه اختصـاص ایستای آدرس های IP ، می باشد چراکه کاربران ناشناس و گمنـام مـی تواننـد پـس از اتصـال بـه شـبکه ، بلافاصله از منبع صادرکننده آدرس های IP ، یک آدرس IP را دریافت و به عنـوان یـک سـرویس گیرنـده در شبکه ایفای وظیفه نمایند. این وضعیت در ارتباط با شبکه های بدون کابل غیرایمن نیز صدق می نماید. مـثلا" یک فرد می تواند با استقرار در پارکینگ یک ساختمان و به کمک یک Laptop به شبکه شما بـا اسـتفاده از یک اتصال بدون کابل ، متصل گردد. پروتکل TCP/IP ، بـرای "معـادل سـازی نـام بـه آدرس " از یـک سرویس دهنده DNS نیز استفاده می نماید . در شبکه های ترکیبی شامل چندین سیستم عامل نظیر وینـدوز و یونیکس و با توجه به این که ویندوز NT 4.0 و یـا ۲۰۰۰ شـده اسـت ، عـلاوه بـر DNS بـه سـرویس WINS نیز نیاز می باشد . همزمان با انتخاب پروتکل ها و سرویس های مورد نیاز آنان ، می بایست بررسـی لازم در خصوص چالش های امنیتی هر یک از آنان نیز بررسی و اطلاعات مربوطه مستند گردند(مستندسازی ، ارج نهادن به زمان خود و دیگران است) . راه حل انتخابی ، می بایست کاهش تهدیدات مرتبط بـا هـر یـک از سرویس ها و پروتکل ها را در یک شبکه به دنبال داشته باشد .

مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری

استفاده عملیاتی از یک سرویس دهنده بدون بررسی دقیق سرویس ها ، پروتکل ها و پیکربندی متناظر با هر یک از آنان زمینه بروز تهدیدات و حملات را در یک شبکه به دنبال خواهد داشت . فراموش نکنیم که مهاجمان همواره قربانیان خود را از بین سرویس دهندگانی که به درستی پیکربندی نشده اند ، انتخاب می نمایند. بنابراین می بایست به سرعت در خصوص سرویس هائی که قصد غیرفعال نمودن آنان را داریم ، تصمیم گیری شود . قطعا" نصب سرویس ها و یا پروتکل هائی که قصد استفاده از آنان وجود ندارد ، امری منطقی و قابل قبول نخواهد بود. در صورتی که این نوع از سرویس ها نصب و به درستی پیکربندی نگردند ، مهاجمان می توانند با استفاده از آنان ، آسیب های جدی را متوجه شبکه نمایند . تهدید فوق می تواند از درون شبکه و یا خارج از شبکه متوجه یک شبکه کامپیوتری گردد . بر اساس برخی آمارهای منتشر شده ، اغلب آسیب ها و تهدیدات در شبکه یک سازمان توسط کارکنان کنجکا و و یا ناراضی صورت می پذیرد تا از طریق مهاجمان خارج از شبکه .

بخاطر داشته باشید که ایمن سازی شبکه های کامپیوتری مستلزم اختصاص زمان لازم و کافی برای برنامه ریزی است . سازمان ها و موسسات علاقه مندند به موازات عرضه فن آوری های جدید ، به سرعت از آنان استفاده نموده تا بتوانند از مزایای آنان در جهت اهداف سازمانی خود استفاده نمایند. تعداد و تنوع گزینه های انتخابی در خصوص پیکربندی هر سیستم عامل ، به سرعت رشد می نماید . امروزه وجود توانائی لازم در جهت شناسائی و پیاده سازی سرویس ها و پروتکل های مورد نیاز در یک شبکه خود به یک مهارت ارزشمند تبدیل شده است. بنابراین لازم است کارشناسان فن آوری اطلاعات که مسئولیت شغلی آنان در ارتباط با شبکه و ایمن سازی اطلاعات است ، به صورت مستمر و با اعتقاد به اصل بسیار مهم " اشتراک دانش و تجارب " ، خود را بهنگام نمایند. اعتقاد عملی به اصل فوق ، زمینه کاهش حملات و تهدیدات را در هر شبکه کامپیوتری به دنبال خواهد داشت .

حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصا" اینترنت ،امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد.

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی زمان و موقعیت بروز یک تهاجم باشیم . به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه

خود آگاه می شویم ؟ چگونه با آن برخورد نموده و در سریعترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد ؟ شناسائی نوع حملات و نحوه پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است .شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویاروئی با آنان افزایش خواهد داد. بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم . جدول زیر برخی از حملات متداول را نشان می دهد :

انواع حملات	
Denial of Service (DoS) & Distributed Denial of Service (DDoS)	
Spoofing	Back Door
Replay	Man in the Middle
Weak Keys	TCP/IP Hijacking
Password Guessing	Mathematical
Dictionary	Brute Force
Software Exploitation	Birthday
Viruses	Malicious Code
Trojan Horses	Virus Hoaxes
Worms	Logic Bombs
Auditing	Social Engineering
	System Scanning