
بسم الله الرحمن الرحيم

دانشگاه آزاد اسلامی

واحد دزفول

مهندسی کامپیوتر

گرایش: نرم افزار

عنوان:

شبکه های کامپیوتری و راه های نفوذ به آن

استاد راهنما:

جناب آقای مهندس موجودی

نگارش:

نرگس ترنجی زاده

پاییز۱۳۹۱

تقدیم به:

***** همسر عزیزم علیرضا *****

با تقدیروسپاس از:

تمامی اساتید و مسئولین محترمی که در جهت ارتقاء و پیشرفت دانشجویان تلاش بعمل می‌آورند

فهرست مطالب:

فصل دوم : نفوذگری

فهرست شکلها

عناوین **شماره صفحه**

چکیده:

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده وسازمانها وموسسات اقدام به برپایی شبکه نموده‌اند. هر شبکه کامپیوتری باید با توجه به شرایط وسیاست های هر سازمان، طراحی وپیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساخت های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می‌آورند؛ در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه های زیادی به منظور نگهداری شبکه وتطبیق آن با خواسته‌های مورد نظر صرف شود.

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 می‌شویم؟ 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.

کلمات کلیدی: شبکه های کامپیوتری ، سیستم حفاظتی

مقدمه :

در این گزارش برآنیم تا ضمن مختصر توضیحی از شبکه های کامپیوتری، اصطلاحات رایج در شبکه، نحوه‌ی بهم‌بندی، ذکر اجزا و انواع شبکه ها به موضوع مهم و قابل توجه نفوذگری در شبکه‌های کامپیوتری بپردازیم. چرا که امروزه شبکه‌های کامپیوتری و اطلاعاتی که از طریق آنها به اشتراک گذاشته می‌شود از اهمیت زیادی برخوردارند.

در نتیجه با توجه به این موضوع اطلاع از نحوه-های متفاوت نفوذ به شبکه های کامپیوتری و راهکارهای مناسب جهت مقابله با آنها حائز اهمیت قرار می‌گیرد.

در ادامه می‌توان گفت، حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس-های فعال، پروتکل‌های استفاده شده و پورت های باز می‌باشد

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری،خصوصاً 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.

تاریخچه:

پس از پرتاب نخستین ماهواره اتحاد جماهیر شوروی به فضا و هنگامی که رقابت سختی از نظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد، وزارت دفاع آمریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیرنظامی که در امتداد دانشگاه ها بودند، تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود. در آن زمان کامپیوتر های Mainframe از طریق ترمینال ها به کاربران سرویس می‌دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها در MIT، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار شد. تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۶۷ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۶۷ نخستین نامه الکترونیکی از طریق شبکه منتقل شد. در این سال ها حرکتی غیرانتفاعی به نام MERIT که چندین دانشگاه بنیانگذار آن بوده‌اند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر DECPDP-۱۱ نخستین بستر اصلی یا Backdone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام PCP نقش میزبان را در شبکه ها ایفا می‌کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michnet نام داشت. از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته‌ای است. قبل از معرفی شدن این روش از سوئیچینگ مداری برای تعیین مسیر ارتباطی استفاده می‌شد اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP این پروتکل

جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل شد. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل شد.

نفوذگران، از دیروز تا امروز

فعالیت های مخرب نفوذگران، سابقه ای طولانی دارد، بر اساس آنچه که در اسناد و مدارک تاریخی مربوط به این قبیل فعالیت‌ها وجود دارد، اولین نمونه چنین اعمالی برای اولین بار در اواخر قرن نوزدهم اتفاق افتاد. جریان از این قرار بود که چند نوجوان باهوش به دلایل نامشخصی موفق شدند یک سیستم تلفنی کاملاً جدید را از کار بیندازند.

اولین قربانی: دومین حمله این افراد در دهه ۶۰ قرن بیستم و به یک آزمایشگاه مجهز به سیستم های رایانه‌ای در ماساچوست صورت گرفت.(تا پیش از این اتفاق واژه نفوذگر به کسانی اطلاق می‌شد که به دلیل مهارت‌های حرفه‌ای در استفاده از رایانه قادر به باز کردن قفل برنامه های رایانه‌ای بودند.

این افراد معمولا برای انجام امور خاصی توسط ماموران قانون به خدمت گرفته می شدند.) اما آزمایشگاه هوش مصنوعی ماساچوست برای اولین بار قربانی نفوذگرانی شد که برای آسیب رساندن و تخریب دست به این اعمال می‌زدند. در اوایل دهه ۷۰ شخصی به نام «جان دراپر» با نفوذ به سیستم امنیتی ارائه دهندگان خدمات تلفن راه دور، توانست به صورت رایگان و البته غیر قانونی از خدمات این مراکز استفاده نماید. او بعد ها از این طریق امرار معاش می کرد و بارها به جرم ایجاد اختلال در سیستم‌های تلفنی، با عنوان «کاپیتان کرانچ» بازداشت و روانه زندان شد.

پس از وی جنبش اجتماعی «هیپی ها » با مرکزی به نام YIPL/TAP کار خود را با عنوان حامی نفوذگران تلفنی آغاز کرد و به آنها کمک می کرد تا به استفاده رایگان از خدمات تلفنی راه دور بپردازند و متعاقب این جریان دو تن از اعضای باشگاه رایانه ای «هوم برو » جعبه‌های آبی رنگی را تولید و توزیع کردند که در آن شیوه اخلال و نفوذ در سیستم های تلفنی آموزش داده می شد. نکته جالب توجه اینجاست که این دو نفر که با نام های مستعار «برکلی بلو و تیوبارک»دست به این اقدامات می زدند، بعدها به چهره های شناخته شده صنعت رایانه مبدل شدند. این دو نفر«استیو جابز و استیو زنیاک» بودند که شرکت رایانه‌ای معروف «اپل مکینتاش»را تاسیس کردند!

یک دهه پس از این اتفاقات نویسنده‌ای به نام ویلیام گیبسون در کتاب علمی تخیلی خود(new romonser) برای اولین بار واژه «سایبر نتیک» را به کار برد و همزمان با انتشار این کتاب سازمان امنیت ایالات متحده اقدام به دستگیری گسترده نفوذگران و انهدام ۴۱۴ پایگاه آنها در میلواکی نمود. اعضای این پایگاه ها متهم به نفوذ در ۶۰ رایانه مربوط به مرکز سرطان سلوان کترینگ و آزمایشگاه ملی لوس آنجلس و دسترسی به اطلاعات آنها بودند. در همین زمان پارلمان آمریکا قانونی را به تصویب رساند که بر اساس آن تجاوز به محیط سایبر نتیک افراد حقیقی و حقوقی جرم و عمل جنایتکارانه تلقی می‌شد و متجاوزان را تحت پیگرد جدی قضایی قرار می-داد.

از دیگر رویدادهای قابل توجه در این دهه شکلگیری دو گروه از نفوذگران به نام‌های «هنگ مجازات » و «باشگاه هرج و مرج طلبان رایانه‌ایی» در کشور آلمان بود. همچنین در همین دوره در فصلنامه‌ای موسوم به ۲۶۰۰ که توسط گروهی از نفوذگران منتشر می‌شد اطلاعات محرمانه‌ای در مورد چگونگی نفوذ به سیستم های تلفن و رایانه به چاپ می‌رسید.

بغرنج شدن موضوع جرائم رایانه‌ای باعث شد تا در اواخر دهه ۸۰ گروهی با نام «پاسخگویان به فوریت های رایانه ای» که در دانشگاه کارنگی پیتزبورگ مستقر بودند، در دل تشکیلات دفاعی آمریکا شکل بگیرد. وظیفه این گروه تحقیق و بررسی روزانه حملات نفوذگران به شبکه های رایانه‌ای بود. با این حال اقدامات مخرب نفوذگران هر روز شدت و حدت بیشتری می یافت . «کوین میت نیک» ۲۵ ساله که یک از نفوذگران کهنه کار بود با نفوذ به شبکه پست الکترونیک شرکت «MSI» و تجهیزات دیجیتالی دفاتر محرمانه آنها خسارات سنگینی را به این شرکت وارد کرد و به همین دلیل نیز برای مدت یکسال پشت میله های زندان قرار گرفت.

متعاقب این ماجرا بانک ملی شیکاگو مورد حمله رایانه‌ای قرارگرفت و مبلغ ۷۰ میلیون دلار از آن به سرقت رفت. به فاصله کوتاهی از این سرقت جنجالی، یک نفوذگر ایتالیایی که خود را «YONG MAN» می‌نامید دستگیر شد و پس از او شخص دیگری در اتلانتا دستگیر شد که عضو گروه « هنگ مجازات » بود.

فصل اول:

تعاریف

شکل ۱. شبکه

۱-۱ برخی اصطلاحات شبکه های کامپیوتری:

• DTE (Data Terminal Equipment) : منبع و گیرنده داده‌ها را در شبکه‌های رایانه‌ای DTE می‌گویند

• DCE (Data Communication Equipment) : تجهیزاتی که مشخصات الکتریکی داده‌ها را با مشخصات کانال داده‌ها تطبیق می‌دهد. مانند مودم

• B.W (Band width) : پهنای باند یا محدوده‌ای که در آن امواج آنالوگ بدون هیچ افتی حرکت می‌کنند.

• Noise : نویز یا پارازیت به امواج الکتریکی مزاحم می‌گویند که موجب اختلال در انتقال داده-ها می‌شود

• Bps : سرعت انتقال داده ها یا بیت در ثانیه

• Network : شبکه

• Share : به اشتراک گذاری داده‌ها و منابع سخت افزاری برای استفاده همه کامپیوترهای موجود در شبکه

• Time Sharing : نوعی شبکه در قدیم که از یک Main Frame به عنوان سرور استفاده می-کردند.

• LAN (Local area network) : شبکه-های محلی و کوچک

• MAN (Metropolition area network : شبکه‌های شهری

• WAN (Wide area network) : شبکه-های گسترده همانند اینترنت

• Node : به هر کامپیوتر وصل به شبکه Node یا گره می گویند.

• Server : سرویس دهنده

• Client : سرویس گیرنده

• Peer - to - Peer : شبکه‌های نظیر به نظیر که در آن هر کامپیوتری هم سرویس دهنده هست و هم سرویس گیرنده

• Server – Based : شبکه‌های بر اساس سرویس دهنده که در آن یک یا چند کامپیوتر فقط سرویس دهنده و بقیه کامپیوترها سرویس گیرنده هستند.

• Topology : توپولوژی به طرح فیزیکی شبکه و نحوه آرایش رایانه‌ها در کنار یکدیگر می‌گویند.

• BUS : توپولوژی خطی که در آن رایانه‌ها در یک خط به هم وصل می‌شوند. در این توپولوژی رایانه اول و آخر به هم وصل نیستند.

- Ring : توپولوژی حلقوی که بصورت یک دایره رایانه‌ها به هم وصلند و در این توپولوژی رایانه اول و آخر به هم وصلند.
- STAR : توپولوژی ستاره ای که در آن از یک هاب به عنوان قطعه مرکزی استفاده می‌شود. و رایانه‌ها به آن وصل می‌شوند.
- Collision : برخورد یا لرزش سیگنال ها
- NIC : کارت شبکه

۱-۲ شبکه کامپیوتری چیست ؟

اساسا یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند این‌ها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار ونرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم افزاری موجود در شبکه منبع (Source) گویند.

در این تشریک مساعی با توجه به نوع پیکربندی کامپیوتر، هر کامپیوتر کاربر می‌تواند در آن واحد منابع خود را اعم از ابزارها وداده‌ها با کامپیوترهای دیگر همزمان بهره ببرد.

۱-۲-۱ دلایل استفاده از شبکه

۱. استفاده مشترک از منابع:

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه، بدون توجه به محل جغرافیایی هریک از منابع را استفاده از منابع مشترک گویند.

۲. کاهش هزینه:

متمرکز نمودن منابع واستفاده مشترک از آنها وپرهیز از پخش آنها در واحدهای مختلف واستفاده اختصاصی هر کاربر در یک سازمان کاهش هزینه را در پی خواهد داشت.

۳. قابلیت اطمینان:

این ویژگی در شبکه‌ها بوجود سرویس دهنده‌های پشتیبان در شبکه اشاره میکند، به این معنا که می-توان از منابع گوناگون اطلاعاتی وسیستم ها در شبکه نسخه های دوم وپشتیبان تهیه کرد ودر صورت عدم دسترسی به یکی از منابع اطلاعاتی در شبکه (به علت از کارافتادن سیستم) از نسخه-های پشتیبان استفاده کرد. پشتیبان از سرویس دهنده‌ها در شبکه، کارآیی، فعالیت وآمادگی دائمی سیستم را افزایش می‌دهد.

۴. کاهش زمان:

یکی دیگر از اهداف ایجاد شبکه‌های رایانه‌ای، ایجاد ارتباط قوی بین کاربران از راه دور است؛ یعنی بدون

محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می‌یابد.

۵. قابلیت توسعه:

یک شبکه محلی می‌تواند بدون تغییر در ساختار سیستم توسعه یابد وتبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات

وتجهیزات مورد نیاز برای گسترش شبکه مد نظر است.

۶. ارتباطات:

کاربران می‌توانند از طریق نوآوریهای موجود مانند پست الکترونیکی ویا دیگر سیستم‌های اطلاع رسانی پیغام هایشان را مبادله کنند؛ حتی امکان انتقال فایل نیز وجود دارد.

در طراحی شبکه مواردی که قبل از راه اندازی شبکه باید مد نظر قرار دهید شامل موارد ذیل هستند:

۱ – اندازه سازمان

۲ – سطح امنیت

۳ – نوع فعالیت

۴ – سطح مدیریت

۵ – مقدار ترافیک

۶ – بودجه

۱-۳ مدل های شبکه:

در یک شبکه، یک کامپیوتر می‌تواند هم سرویس دهنده وهم سرویس گیرنده باشد. یک سرویس دهنده (Server) کامپیوتری است که فایل های اشتراکی وهمچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بعهده دارد، را نگهداری می‌کند. برای آنکه سرویس گیرنده "Client" بتواند به سرویس دهنده دسترسی پیدا کند، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات در خواست شده را به سرویس گیرنده ارسال خواهد کرد.

سه مدل از شبکه‌هایی که مورد استفاده قرار می‌گیرند، عبارتند از :

۱ – شبکه نظیر به نظیر " Peer- to- Peer "

۲ – شبکه مبتنی بر سرویس دهنده " Server- Based "

۳ – شبکه سرویس دهنده / سرویس گیرنده " Client Server"

۱-۴ اجزای شبکه:

اجزا اصلی یک شبکه کامپیوتری عبارتند از:

۱-۴-۱ کارت شبکه **NIC- Network Interface Card**:

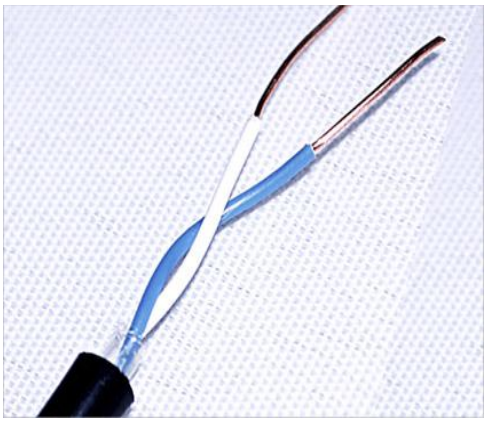
برای استفاده از شبکه وبرقراری ارتباط بین کامپیوترها از کارت شبکه‌ای استفاده می‌شود که در داخل یکی از شیارهای برد اصلی کامپیوترهای شبکه " اعم از سرویس دهنده وگیرنده "

بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می‌گردد.

۱-۴-۲ رسانه انتقال **Transmission Medium** :

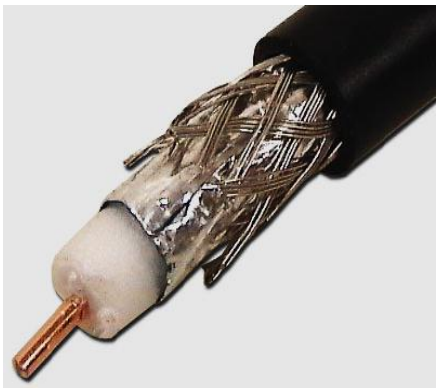
رسانه انتقال کامپیوترها را به یکدیگر متصل کرده وموجب برقراری ارتباط بین کامپیوترهای یک شبکه می‌شود. برخی از متداولترین رسانه‌های انتقال عبارتند از:

کابل زوج سیم بهم تابیده "Twisted- Pair"



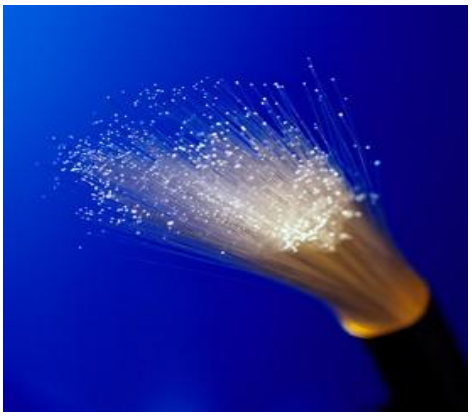
شکل ۲. کابل زوج سیم

کابل کواکسیال " Coaxial"



شکل ۳. کابل کواکس

کابل فیبر نوری "Fiber- Optic"



شکل ۴. کابل فیبر نوری

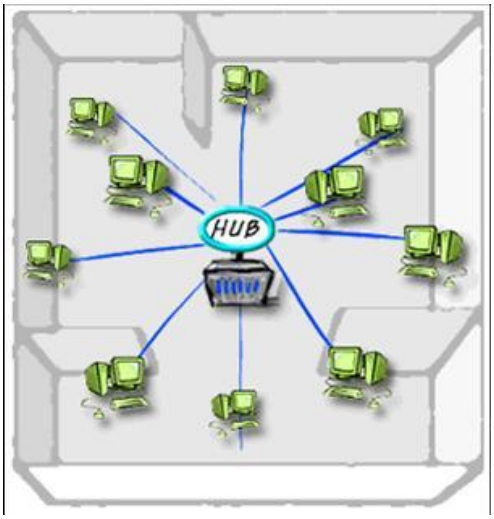
۱-۴-۳ سیستم عامل شبکه **NOS- Network Operating System** :

سیستم عامل شبکه برروی سرویس دهنده اجرا می‌شود و سرویس‌های مختلفی مانند: اجازه ورود به سیستم "Login"، رمز عبور"Password"، چاپ فایل‌ها " Printfiles"، مدیریت شبکه " Net work management " را در اختیار کاربران می‌گذارد.

۱-۵ انواع شبکه‌ها از لحاظ جغرافیائی:

۱. شبکه محلی(LAN (Local Area Network

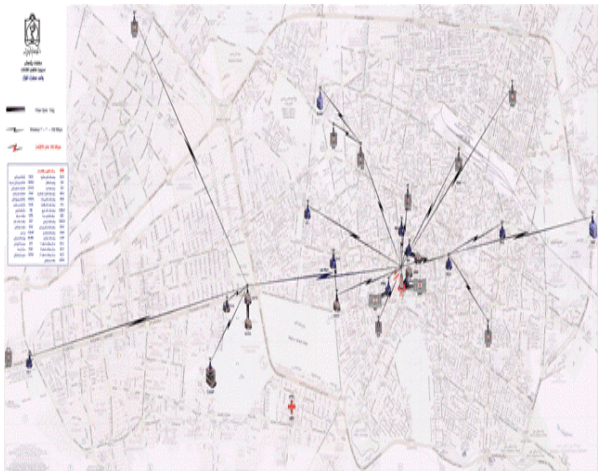
اتصال بیش از دو یا چند کامپیوتر در فضای محدود یک سازمان



شکل ۵. LAN

۲. شبکه شهری MAN (Metro politan Area Network)

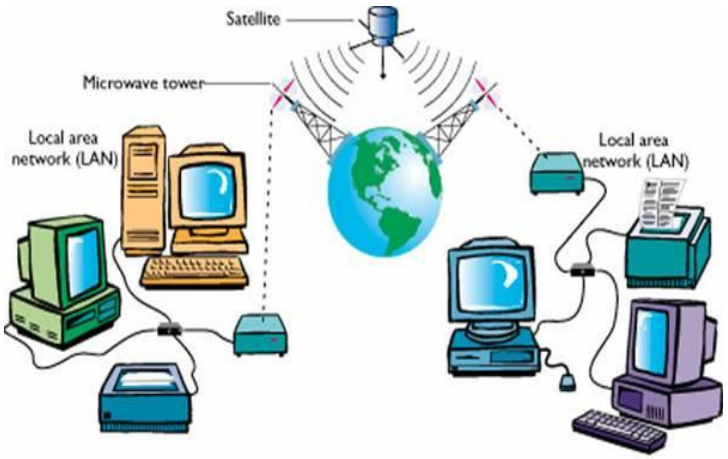
اگر تعدادی شبکه محلی را در محیط‌های بزرگتری در حد یک شهر به هم متصل کنیم



شکل ۶. MAN

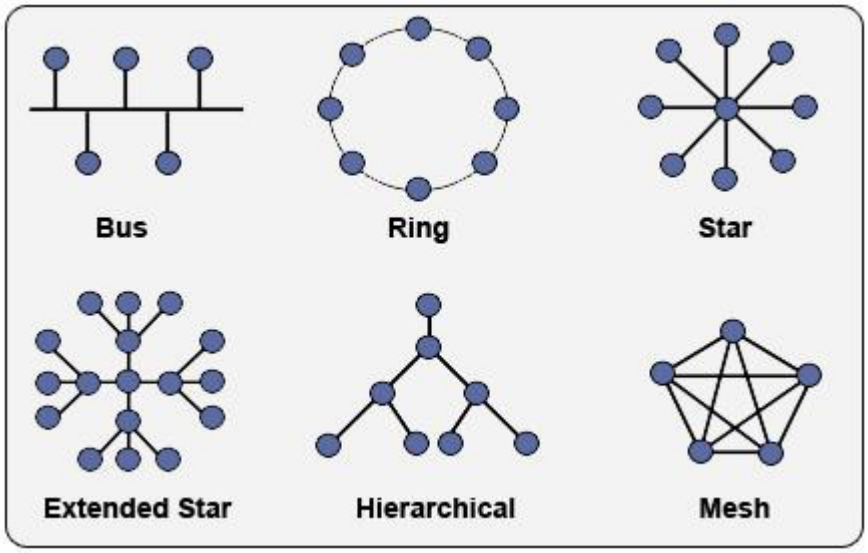
۳. شبکه گسترده WAN (Wide area network)

اتصال شبکه های کوچک از طریق خطوط مخابراتی کابل‌های ارتباطی یا همواره و دیگر سیستم‌های مخابراتی در یک منطقه بزرگتر را شبکه گسترده می گویند.



شکل ۷. WAN

۶- انواع توپولوژی (بهم بندی) شبکه:



شکل ۸ . انواع توپولوژی

شکل فیزیکی اتصال کامپیوترها، کابل ها و سایر اجزا را توپولوژی می‌گویند.

انواع متداول توپولوژی های شبکه:

۱. خطی (Bus)
۲. حلقوی (Ring)
۳. ستاره ای (Star)
۴. توری (Mesh)
۵. درختی (Tree)
۶. ترکیبی (Hybrid)

۱-۶-۱ توپولوژی خطی **Bus**

در این شبکه چندین کامپیوتر به یک کابل به نام گذرگاه متصل می‌شوند اگر کامپیوتری بخواهد اطلاعاتی را به کامپیوتر دیگر بفرستد بسته حاوی اطلاعات را بر روی شبکه ارسال می‌نماید تمامی کامپیوترهای متصل به گذرگاه گوش می‌کنند و بسته هائی را که به آنان مربوط می‌شوند را دریافت می‌نمایند تعداد کامپیوترها در این شبکه ها کم و معمولاً ۱۰عدد است.

۱-۶-۲ توپولوژی حلقوی **Ring**

در این توپولوژی همه کامپیوترها به گونه‌ای به هم متصل می‌شوند که تشکیل یک حلقه را می-دهند همیشه یک بسته به نام ناشنهtorken در این حلقه در حال گردش است این نشانه در حلقه

می‌چرخد هر کامپیوتری که نشانه را در دست داشته باشد می‌تواند اطلاعات را بفرستد در صورتی که کامپیوتر بسته‌ای برای ارسال نداشته باشد نشانه‌ها را به کامپیوتر بعدی می‌دهد بنابراین هر کامپیوتر باید آدرس کامپیوتر بعد از خود را بداند.

۱-۶-۳ توپولوژی ستاره‌ای **Star**

در این توپولوژی تمام کامپیوترها به یک دستگاه کنترل کننده مرکزی به نام هاب یا سوئیچ متصل می‌شوند کامپیوتر مبدا اطلاعات را به هاب یا سوئیچ ارسال می‌نماید هاب آن را بر روی تمام پورت‌ها منتشر می‌کند با توجه به آدرس گیرنده که همراه بسته های ارسالی وجود دارد کامپیوتر مقصد اطلاعات را دریافت می‌نماید.

۱-۶-۴ توپولوژی توری **Mesh**

در این نوع توپولوژی هر کامپیوتر مستقیماً به کلیه کامپیوترهای شبکه متصل می‌باشد به عنوان مثال در یک شبکه با ۱۰ کامپیوتر ایستگاه ۱ نیازمند ۹ کابل برای اتصال به کامپیوترهای ۲تا۱۰می باشد تعداد کل کابل‌های مورد نیاز در این نوع هم بندی زیاد است.

فصل دوم:

نفوذگری در

شبکه

شکل۹. نفوذگری

یکی از مهمترین مشغله های کارشناسان شبکه امنیت شبکه و مقابله با نفوذگران می‌باشد . بنابراین کشف راه‌های نفوذ به شبکه باید همواره مورد توجه مسئولان شبکه‌های کامپیوتری قرار بگیرد. یک مسئول شبکه و حتی یک کاربر ساده باید با راه‌های نفوذ به شبکه آشنا باشد تا با بستن و کنترل این راه‌ها شبکه یا سیستم موردنظر را از حملات هکرها محفوظ بدارد.

در ذهنیت عمومی هکر یک انسان شرور و خرابکار است ولی در واقع اینگونه نیست وهکرها در بسیاری از موارد هدفشان پیدا کردن ضعف های شبکه و برطرف کردن آنهاست.

به همین دلیل در اواخر دهه ۸۰ ، هکرها را بر اساس فعالیت‌هایشان دسته بندی کردند.

۲-۱ انواع نفوذگران:

۱. گروه (White Hacker Group)

نفوذگران کلاه سفید

این گروه در واقع دانشجویان و اساتیدی هستند که هدفشان نشان دادن سیستم های امنیتی شبکه-های کامپیوتری می‌باشد. این گروه به هکرهای خوب معروفند که در تحکیم دیواره حفاظتی شبکه های نقش اساسی دارند. این گروه خلاقیت عجیبی دارند و معمولاً هر بار با روشهای نو و جدیدی از دیواره‌های امنیتی عبور می‌کنند.

۲. گروه (Black Hacker Group)

نفوذگران کلاه سیاه

این گروه خرابکارانه ترین نوع هکرها هستند و به Cracker معروفند. کلاه سیاه ها اغلب ویروس نویسند. و با ارسال ویروس نوشته شده خود بر روی سیستم قربانی به آن نفوذ می کنند. این گروه همیشه سعی در پنهان نمودن هویت خود را دارند.

۳. (Gray Hat Hacker Group)

گروه نفوذگران کلاه خاکستری

نام دیگر این گروه whacker است. هدف اصلی واکرها استفاده از اطلاعات سایر کامپیوترها به مقاصد مختلف می‌باشد. در صورتی که با نفوذ به شبکه صدمه‌ای به کامپیوترها وارد نمی‌کنند. مثلاً در سال ۱۹۹۴ یک هکر "کلاه خاکستری" آمریکا نفوذ پیدا کرد و تمامی اسناد محرمانه متعلق به این Nasa ژاپنی به سایت ناسا سازمان را ربود و به طور رایگان بر روی اینترنت در اختیار عموم قرار داد.

۴. گروه (Pink Hat Hacker Group)

نفوذگران کلاه صورتی

این گروه افراد بی‌سوادی هستند که فقط قادرند به وسیله نرم افزارهای دیگران در سیستمها اختلال به وجود بیاورند و مزاحمت ایجاد کنند. به این افراد booter گفته می‌شود. بوترها خود سواد برنامه نویسی ندارند ولی در بعضی از موارد همین نوع هکرها می‌توانند خطرهای جدی برای شبکه به وجود آورند.

۲-۲ انواع حملات هکرها:

۱. حمله از نوع دستکاری اطلاعات Modification

به این معنی که هکر در حین انتقال اطلاعات به مقصد آنها را مطابق خواسته خود تغییر داده و به کاربر می‌فرستد و کاربر بدون اطلاع از تغییر آنها را مورد استفاده قرار می‌دهد.

۲. حمله از نوع افزودن اطلاعات Farication

در این نوع از حمله هکر به جای تغییر دادن اطلاعات، اطلاعات جدیدی را به آن می‌افزاید مانند یک ویروس جهت اقدامات بعدی.

۳. حمله از نوع استراق سمع Interception

در این نوع حمله هکر فقط به اطلاعات در حین تبادل گوش می‌دهد و در صورت لزوم از آن نسخه برداری می‌کند.

۴. حمله از نوع وقفه Interruption

در این نوع حمله هکر با ایجاد اختلال در شبکه و وقفه در انتقال اطلاعات برای خود فرصت لازم جهت اقدامات بعدی را فراهم می‌آورد.

۲-۳ راه های نفوذ:

- حمله از طریق IP : در این روش ابتدا هکر به روشهای مختلف IP (ایستگاه وب، ISP و ...)را بدست می‌آورد. این کار با پیدا کردن نقشه‌ی شبکه راحت‌تر است. سپس هکر خود را در بین سرویس دهنده و کاربر قرار می‌دهد و با ارسال بسته‌های تقلبی اطلاعات را به سرقت می‌برد. در این روش در واقع هکر خود را برای سرویس دهنده، گیرنده و برای کاربر سرویس دهنده معرفی می‌کند و به عنوان واسط بین کاربر و Server

قادر است بسته‌های خود را با شماره‌های صحیح انتقال دهد.

- حمله به TCP: این حمله از متداولترین نوع حمله به سرویس دهنده‌ها در اینترنت می‌باشد. هکر در این روش ارتباط کاربر را از سرویس دهنده قطع می‌کند و IP خود را به جای کاربر به سرویس دهنده معرفی می‌کند و از این پس هر گونه تبادل اطلاعات بین سرویس دهنده و هکر صورت می‌گیرد. مزیت این روش به روش حمله به IP این است که در این روش هکر تنها یک بار حمله می‌کند و از مقابله با سیستمهای امنیتی رمز عبور در مراحل بعد فرار می‌کند. "برخلاف حمله به IP".
- حملات جاسوسی
- جعل اطلاعات

- جعل IP
- جعل Email
- جعل یک وب

- Applet ها
- Cookie ها
- حمله به کلمات عبور
- حمله به برنامه‌های کاربردی

برای امن کردن یک شبکه نیاز به سه ابزار زیر داریم:

۱. Firewall

۲. IDS (Intrusion Detection System)

۳. Honey Pot

در یک شبکه کامپیوتری برای ایجاد موانع عبور، Firewall نصب می‌کنیم. برای آگاه شدن از وقوع نفوذ، IDS نصب می‌کنیم و برای منحرف کردن و شناسایی رفتار و روش نفوذگر، Honey Pot نصب می‌کنیم.

۲-۴ تعاریفی از Firewall :

یک فایروال شبکه را در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به کامپیوترها حفاظت می‌کند. توابع اولیه یک فایروال به این صورت است که اجازه می دهد ترافیک خوب عبور کند و ترافیک بد را مسدود می‌کند.

دیوار آتش سیستمی سخت افزاری یا نرم افزاری است که بین کامپیوتر شما یا یک شبکه LAN و شبکه بیرونی (مثلا اینترنت) قرار گرفته و ضمن نظارت بر دسترسی به منابع (resource) سیستم، در تمام سطوح ورود و خروج اطلاعات را تحت

نظر دارد. هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات شبکه خود را کنترل کند موظف است تمام ارتباطات مستقیم شبکه خود را با دنیای خارج قطع نموده و هر گونه ارتباط خارجی از طریق یک دروازه که دیوار آتش یا فیلتر نام دارد، انجام شود.

قبل از تحلیل اجزای دیوار آتش عملکرد کلی و مشکلات استفاده از دیوار آتش را بررسی می-کنیم.

بسته های TCP و IP قبل از ورود یا خروج به شبکه ابتدا وارد دیوار آتش می‌شوند و منتظر می-مانند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند. پس از پردازش و تحلیل بسته سه حالت ممکن است اتفاق بیفتد:

۱- اجازه عبور بسته صادر می‌شود (Accept Mode)

۲- بسته حذف می‌شود (Blocking Mode)

۳- بسته حذف شده و پاسخ مناسب به مبدا آن بسته داده شود (Response Mode)

غیر از حذف بسته می‌توان عملیاتی نظیر ثبت، اخطار، ردگیری، جلوگیری از ادامه استفاده از شبکه و توبیخ هم در نظر گرفت.

به مجموعه قواعد دیوار آتش سیاستهای امنیتی نیز گفته می‌شود.

طبق تحقیقات انجام شده تنها یک خطا (error) در مجموعه قواعد کنترل یک دیوار آتش می‌تواند راهی را برای بروز آسیب پذیری بحرانی در سیستم باز کند. چنین مشکل امنیتی‌ای می تواند به مزاحمان اجازه دهد تا به داده ها و برنامه ها دسترسی پیدا کنند که نتیجه آن تجاوز به حریم خصوصی افراد، خرابکاری عمدی صنعتی، کلاهبرداری و دزدی است. حالا این محققان روشی را برای تجزیه و تحلیل فعالیت "فایل‌های لاگ Log" دیوار آتش شخصیت های حقیقی ایجاد کرده‌اند. گزارش‌های مربوط به فعالیت های رایانه نظیر داده‌ها، زمان، بایت های رسیده و ارسال شده و ... در فایلی ذخیره می‌شود که فایل لاگ نامیده می‌شود. تجزیه و تحلیل های این محققان از فایل های لاگ می‌تواند تعیین کند که واقعاً چه قواعدی در دیوار آتش برای ترافیک ورودی و خروجی شبکه اعمال می‌شود. سپس این قواعد را با قواعد اصلی مقایسه کنند تا خطاها و حذفیات را مکان یابی کنند.

از زمان ظهور اینترنت، فناوری دیوار آتش پس از چند نسل ابداع و تحقیق و در یک دوره زمانی کوتاه به سرعت پیشرفت کرده که نتیجه آن ارائه خدماتی است که از نظر هزینه به صرفه و از نظر کیفیت قوی است. اما هیچ دیوار آتشی کامل

نیست و همیشه امکان خطای انسانی یا اشکالات رایانه‌ای وجود دارد که می‌تواند به طور غیرعمدی مسیرهایی را مقابل کاربران بداندیش باز کند و اجازه دسترسی آنها به اجزای شبکه یا سیستم-هایی که لازم است برای دسترسی به آنها محدودیت وجود داشته باشد را بدهد.

۲-۵ امنیت شبکه:

امروزه با بالا رفتن آمار کاربران اینترنت در کشور و آشنایی آنها با نرم‌افزارهای نفوذ به شبکه‌های کامپیوتری و همچنین با رشد میزان اطلاعات موجود بر روی سرورهای سازمانها، نیاز به نظارت بر امنیت شبکه‌های کامپیوتری اهمیت بسزایی پیدا می‌کند. عدم آشنایی بسیاری از کاربران و پرسنل سازمانها، به نفوذگران کمک می‌کند تا به راحتی وارد یک شبکه کامپیوتری شده و از داخل آن به اطلاعات محرمانه دست پیدا کنند یا اینکه به اعمال خرابکارانه بپردازند. هر چه رشد اینترنت و اطلاعات روی آن بیشتر می‌شود نیاز به اهمیت دادن به امنیت شبکه افزایش پیدا می‌کند. از این روست که شرکت داده پردازان دوران با تشکیل یک تیم بسیار قوی در زمینه امنیت شبکه سعی کرده است تا حد زیادی خلا موجود در این زمینه را برای چنین شرکتها و سازمانهایی پر کند.

۲-۶ مدیریت امنیت شبکه

به منظور تعیین اهداف امنیت، ابتدا باید سرمایه‌های مرتبط با اطلاعات و ارتباطات سازمان، شناسایی شده و سپس اهداف تامین امنیت برای هریک از سرمایه‌ها، مشخص شود.سرمایه‌های مرتبط با شبکه سازمان عبارتند از: سخت افزار، نرم‌افزار، اطلاعات، ارتباطات، کاربران.

اهداف امنیتی سازمان‌ها باید به صورت کوتاه‌مدت و میان‌مدت تعیین گردد تا امکان تغییر آن‌ها متناسب با تغییرات تکنولوژی‌ها و استانداردهای امنیتی وجود داشته باشد. عمده اهداف کوتاه مدت در خصوص پیاده‌سازی امنیت در یک سازمان عبارتند از:

- جلوگیری از حملات و دسترسی‌های غیرمجاز علیه سرمایه‌های شبکه
- مهار خسارت‌های ناشی از ناامنی موجود در شبکه
- کاهش رخنه پذیری

اهداف میان‌مدت نیز عمدتاً عبارتند از:

– تامین صحت عملکرد، قابلیت دسترسی برای نرم‌افزارها و سخت‌افزارها و محافظت فیزیکی صرفاً برای

سخت افزارها

– تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات و اطلاعات متناسب با طبقه بندی آن‌ها از

حیث محرمانگی و حساسیت

– تامین قابلیت تشخیص هویت، حدود اختیارات و پاسخگویی، حریم خصوصی و آگاهی‌رسانی امنیتی برای کاربران شبکه، متناسب با طبقه‌بندی اطلاعات قابل دسترس و نوع کاربران

۲-۷ تهدیدهای امنیتی

تهدیدهای بالقوه برای امنیت شبکه‌های کامپیوتری به صورت عمده عبارتند از:

- فاش شدن غیرمجاز اطلاعات در نتیجه استراق‌سمع داده‌ها یا پیام‌های در حال مبادله روی شبکه
- قطع ارتباط و اختلال در شبکه به واسطه یک اقدام خرابکارانه
- تغییر و دستکاری غیر مجاز اطلاعات یا یک پیغام ارسال‌شده. برای جلوگیری از این صدمات باید سرویس‌های امنیتی زیر در شبکه‌های کامپیوتری ارائه شود و زمانی که یکی از سرویس‌های امنیتی نقص شود بایستی تمامی تدابیر امنیتی لازم برای کشف و جلوگیری رخنه در نظر گرفته شود.
- محرمانه ماندن اطلاعات
- احراز هویت فرستنده پیغام
- سلامت داده‌ها در طی انتقال یا نگهداری
- کنترل دسترسی و امکان منع افرادی که برای دسترسی به شبکه قابل اعتماد نمی‌باشد.
- در دسترس بودن تمام امکانات شبکه برای افراد مجاز و عدم امکان اختلال در دسترسی

۲-۸ دلایل توجه به امنیت شبکه

۱. افزایش آگاهی کاربران اینترنت
۲. وجود انگیزه نفوذ با توجه به گسترش اطلاعات مهم روی اینترنت
۳. سهولت نفوذ و خرابکاری با استفاده از ابزارهای رایگان نفوذ روی اینترنت
۴. افزایش روزافزون انواع ویروس‌های کامپیوتری

۵. وجود ضعف‌های امنیتی در سیستم عامل‌ها و برنامه‌های کاربردی
۶. وجود کاربران غیر حرفه‌ای و آموزش ندیده

۲-۹ نتیجه بی‌توجهی به امنیت شبکه

۱. نفوذ به شبکه و دسترسی به اطلاعات محرمانه
۲. سوء استفاده مالی
۳. تخریب اطلاعات موجود و نرم‌افزارها
۴. تخریب سخت افزاری
۵. از کار انداختن سرورها و اشغال پهنای باند

۲-۱۰ نحوه جلوگیری از حملات اینترنتی

سیستم‌های دفاعی در برابر حملات اینترنتی

سرویس‌دهندگان اینترنت و صاحبان سایت‌ها همواره یک نگرانی دائمی در مورد نقاط ضعف و روزنه‌های نفوذ به سیستم‌ها دارند. این نفوذها با استفاده از ضعف سیستم‌ها صورت می‌پذیرد و برای دفاع در برابر آنها لازم است اطلاعات جامعی پیرامون آنها در دسترس باشد. این مقاله نگاهی اجمالی بر انواع مختلف حملات اینترنتی و راهکارهای جلوگیری از آنها دارد.

۲-۱۰-۱ جلوگیری از سرویس‌دهی سرورها

از جمله حملاتی که وب سرورها بسیار زیاد گرفتار آنها می‌شوند، جلوگیری از سرویس‌دهی (Denial of Service) است. این نوع حملات بسیار رایج بوده، زیرا کاربران غیر حرفه‌ای نیز می‌توانند آنها را ایجاد کنند. به عنوان مثال بسیاری از سرورها در بانک‌های الکترونیکی یا سرویس‌دهندگان پست‌الکترونیکی ممکن است به این مشکل گرفتار شوند.

در این نوع از حملات اینترنتی، درخواست‌هایی جعلی از یک یا چند منبع متفاوت به سرور ارسال می‌شود و با حجم زیاد درخواست‌های تقلبی، سرور از پاسخ‌دهی به درخواست‌های واقعی عاجز می‌ماند. این روش اغلب توسط هکرهای غیرحرفه‌ای مورد استفاده قرار می‌گیرد که برنامه‌هایی را به‌صورت ویروس، کرم‌های اینترنتی یا اسب‌های تروا می‌نویسند تا وب سرورها را از حالت سرویس‌دهی خارج کنند.

۲-۱۰-۲ حملات **DOS**

حملات DOS عمدتا زیرساخت پروتکل TCP/IP را هدف قرار می‌دهند و در سه نوع زیر طبقه‌بندی می‌شوند:

۱. حملاتی که از نواقص پیاده سازی پشته TCP/IP استفاده می‌کنند.
۲. حملاتی که از نواقص خود پروتکل TCP/IP استفاده می‌کنند.
۳. حملاتی که از روش سعی و خطا استفاده می‌کنند.

۲-۱۰-۲-۱ حملات نوع اول

از جمله حملات نوع اول می‌توان به Ping of Death و Teardrop اشاره کرد. در روش Ping of Death، شخص مهاجم بسته‌های IP را با حجم‌های غیراستاندارد (خیلی بزرگ) روی شبکه می‌فرستد تا سرور از کار بیفتد و بتواند از پشته آسیب پذیر TCP/IP و یا سیستم عامل استفاده کند.

اما در روش حمله Teardrop، سرور به وسیله بسته‌های IP که فیلدهای offset آنها همپوشانی دارند، بمباران می‌شود. سرور یا روتر نمی‌تواند این بسته‌ها را دور بیندازد و لذا شروع به بازسازی آنها می‌کند که همپوشانی فیلدها باعث بروز مشکل خواهد شد.

راهکار جلوگیری از این نوع حملات، استفاده از دیوار آتش است که جلوی بسته‌های IP غیرمتعارف را می‌گیرد و مانع بروز اشکال در سیستم می‌شود.

۲-۱۰-۲-۲ حملات نوع دوم

رایج‌ترین حملات نوع دوم، تهاجم موسوم به SYN است. وقتی که کامپیوتری قصد برقراری ارتباط با یک کامپیوتر راه‌دور را دارد، این عمل با فرآیندی موسوم به دست‌دهی سه‌مرحله‌ای (Way Hand Shake 3) صورت می‌پذیرد. بدین‌گونه که ابتدا کامپیوتر مبدا یک بسته SYN به کامپیوتر مقصد می‌فرستد و کامپیوتر مقصد با دریافت بسته، یک تائیدیه ACK به مبدا می‌فرستد و بدین ترتیب کامپیوتر مبدا می‌تواند ارتباط مورد نیاز را با کامپیوتر مقصد برقرار سازد. به طور واضح مشخص است که اگر کامپیوتر راه دور گرفتار ازدحام بسته‌های SYN شود، باید برای هر SYN یک بسته تایید بفرستد و بدین ترتیب پهنای باند آن تلف خواهد شد. حال اگر کامپیوتر حقیقی تقاضای ایجاد ارتباط کند، به علت اشغال‌شدن پهنای باند، سرور امکان سرویس‌دهی به سایر کامپیوترها را نخواهد داشت.

اگر چه پهنای باندی که در این روش اشغال می‌شود، اغلب محدود است ولی اگر حملات در حجم بالا صورت پذیرد، مشکلات جدی را برای سرور فراهم می‌کند.

با استفاده از دیوار آتش جلوی این حملات را نیز می‌توان گرفت.

۲-۱۰-۲-۳ حملات نوع سوم

در حملات نوع سوم شخص مهاجم با ارسال تعداد زیادی بسته‌های ICMP (پروتکل کنترل پیام) روتر را مملو از این بسته‌ها می‌کند و از آنجائیکه تقریبا همه وب سرورها به این نوع بسته‌ها پاسخ می‌دهند، پهنای باند به طور کلی از بین می‌رود و کاربران واقعی از ادامه کار عاجز می‌مانند و ترافیک بسیار زیادی برای همه گره‌های شبکه ایجاد می‌شود. امکان این نوع حملات را نیز می‌توان با استفاده از دیوار آتش از بین برد.

۲-۱۱ دیگر حملات

اما حملات اینترنتی برای ممانعت از سرویس دهی سرورها محدود به موارد فوق نیست و تهاجماتی به صورت‌های زیر نیز وجود دارد.

۲-۱۱-۱ ازدحام بسته‌های **UDP**

در این روش شخص مهاجم بسته‌های بلااستفاده‌ای از یک پورت UDP به پورت دیگر UDP روی کامپیوتر مقصد منتقل می‌کند و از آنجائیکه پروتکل UDP وابسته به ارتباط نیست (Connection Less)، ازدحام بسته‌های UDP، مشکل‌ساز می‌شود.

۲-۱۱-۲ بمباران سرور به وسیله نامه‌های الکترونیکی

این روش اغلب به وسیله کاربران غیرحرفه‌ای استفاده می‌شود و در آن شخص مهاجم هزاران نامه الکترونیکی را به یک آدرس خاص می‌فرستد و باعث سرریز نامه‌ها می‌شود. در این روش وقتی تعداد نامه‌های الکترونیکی از حدمجاز سرورهای SMTP تجاوز کند، باعث از کار افتادن سرور شده و سایر کاربران ISP از ادامه کار عاجز می‌شوند. این نوع حملات به آسانی قابل ردیابی هستند و با یافتن IP مبدا نامه‌های الکترونیکی، می‌توان به سایر اطلاعات موردنیاز دست یافت و جلوی حملات را گرفت.

۲-۱۱-۳ باز شدن صفحات اینترنتی بـه صورت پشت سر هم

این نوع از حملات نیز به وسیله کاربران غیرحرفه‌ای صورت می‌پذیرد. در این روش مهاجمان با برنامه‌های کوچک به‌صورت تکراری بعضی از صفحات اینترنتی را مرتبا و پشت سر هم فراخوانی می‌کنند. این عمل نیز باعث اشغال بسیار زیاد پهنای باند سرورها می‌شود و کاربران دیگر را از ادامه کار باز می‌دارد.

جهت رفع این مشکل باید مدیران شبکه به هر کاربر فقط امکان برقراری یک ارتباط را بدهند تا چنین مشکلاتی ایجاد نشود.

۲-۱۱-۴ جلوگیری از سرویس دهی سرورهای غیرمتمرکز

این نوع از حملات از جمله رایج‌ترین حملات اینترنتی است که در آن هزاران یا ده‌ها هزار کامپیوتر آسیب خواهد دید. اغلب این حملات بدین صورت است که فایلی در کامپیوترهای آسیب دیده می‌نشیند و منتظر دستور فرد مهاجم می‌ماند، وقتی که شخص مهاجم دستور ازدحام بسته‌های کنترل پیام‌ها را می‌دهد، به سرعت بسته‌های ICMP روی کامپیوترهای مختلف پخش‌شده و باعث از کارافتادن کامپیوترهای راه دور می‌شوند.

امروزه امکانات و برنامه‌های زیادی برای این نوع حملات وجود دارد؛ به‌گونه‌ای که ارتشی از فایل‌های جست‌وجوگر، سرویس‌ها و پورت‌های سرور را جست‌وجو می‌کنند تا نقاط ضعف آنها را پیدا کنند و به صورت گروهی حملاتی را به سرورهای مختلف انجام دهند. حل این مشکل به وسیله ایمن سازی تک تک کامپیوترها ممکن نیست زیرا فیلترکردن و یا دنبال کردن ترافیک حملات به علت شباهت آنها با ترافیک واقعی شبکه، بسیار دشوار است. از آنجائیکه همواره تعداد بسیار زیادی از کامپیوترهای ناامن روی اینترنت وجود دارد، این کامپیوترها محل بسیار مناسبی برای ایجاد حملات جدید هستند.

۲-۱۲ جلوگیری از حملات:

از آنجائیکه حمله به سیستم‌های غیرمتمرکز منجر به بروز مشکلات بسیار جدی می‌شود، لذا برای جلوگیری

از آنها باید اصول خاصی در نظر گرفته شود:

۱. استفاده از راهکارهای غیرمتمرکز برای سیستم‌های غیرمتمرکز

۲. اجتناب از راهکارهای مضر برای کاربران قانونی
۳. ایمن سازی سیستم در مقابل تهدیدات داخلی و خارجی
۴. طراحی سیستم‌های عملی برای هماهنگی با مشکلات واقعی
۵. ارائه راه‌حل‌های قابل اجرا در محیط‌های کوچک و تعمیم آنها به کل سیستم‌ها.

راه‌حل‌هایی که برای حملات غیرمتمرکز ارائه می‌شود، اغلب به‌صورت محدودکردن سرویس‌ها و یا قطع آنها هستند که مشکلاتی جدی برای فعایت‌های قانونی ایجاد می‌کنند.

اما در اصل باید برای جلوگیری از این حملات، گره‌هایی را که دچار مشکل شده‌اند، شناسایی و آنها را ایزوله کرد و یا از شبکه بیرون انداخت و این عملیات باید به ترتیبی صورت پذیرد که بهترین نتیجه حاصل شود.

DefCOM یکی از سیستم‌های دفاعی در برابر این حملات است که از چندین گره امنیتی غیرمتجانس تشکیل شده است. این گره‌ها ترافیک شبکه را بررسی کرده و سپس نرخ مناسب ترافیک در شبکه را بـرای جلوگیری از ترافیک تقلبی مشخص می‌کنند. درصورت حمله، کامپیوتر قربانی پیام خطر می‌دهد و کامپیوتر امنیتی آن را به همه کامپیوترهای امنیتی دیگر می‌فرستد تا همه در حالت تدافعی قرار گیرند. از این به بعد کامپیوترهای امنیتی پیام‌های بین خود را با برچسب خاصی می‌فرستند تا ارتباطی امن بین خودشان برقرار شود، بدین ترتیب ریشه حمله را پیدا می‌کنند. در این ارتباط، داده‌های شبکه با ۳ نوع برچسب متفاوت ارسال و دریافت می‌شوند:

۱. ترافیک بدون برچسب که ترکیبی از داده‌های خوب و بد است.
۲. ترافیک کنترل شده که با نرخ پایین مبادله می‌شود.
۳. ترافیک قانونی که ترافیک مجاز شبکه است. بررسی روش‌های مختلف حملات اینترنتی و راهکارهای مقابله با آنها نشان می‌دهد که امکان برطرف کردن کامل آنها وجود ندارد و آنچه که مدیران شبکه‌ها قادر به انجام آنها هستند، بررسی چگونگی حملات اینترنتی است تا تدابیری را جهت جلوگیری از تکرار آنها بیندیشند.

نتیجه گیری:

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می‌باشیم. کافی است به اطراف

خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم. همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فن‌آوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه‌های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند . امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری از جمله این مولفه ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد .

منابع:

۱. موسوی.ع. و همکاران- شبکه های کامپیوتری
۲. سایت های آموزش شبکه های کامپیوتری
۳. سایت مهندسان ایران www.iran-eng.com
۴. سایت های نفوذ و هک