دولت جمهوری اسلامی افغانستان
ادارۀ تعلیمات تخنیکی و مسلکی
معاونیت امور اکادمیک
ریاست نصاب و تربیه معلم

امنیت شبکه‌های کمپیوتری

رشته: کمپیوتر ساینس - دیپارتمنت: شبکه

صنف ۱۴ - سمستر دوم

سال: ۱۳۹۹ هجری شمسی

شناسنامه کتاب

نام کتاب: امنیت شبکه های کمپیوتری

رشته: کمپیوتر ساینس

تدوین کننده: پوهنمل محمد حسین سلطانی

همکار تدوین کننده: سید محمد کاظم رجایی

کمیته نظارت:

- ندیمه سحر رئیس ادارۀ تعلیمات تخنیکی و مسلکی
- عبدالحمید اکبر معاون امور اکادمیک ادارۀ تعلیمات تخنیکی و مسلکی
- حبیب الله فلاح رئیس نصاب و تربیه معلم
- عبدالمتین شریفی آمر انکشاف نصاب تعلیمی، ریاست نصاب و تربیه معلم
- روح الله هوتک آمر طبع و نشر کتب درسی، ریاست نصاب و تربیه معلم
- احمد بشیر هیله‌من مسؤل انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- محمد زمان پویا کارشناس انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- علی خیبر یعقوبی سرپرست مدیریت عمومی تألیف کتب درسی، ریاست نصاب و تربیه معلم

کمیته تصحیح:

- مهدی بهار
- محمد باقر موسوی
- محمد امان هوشمند مدیرعمومی بورد تصحیح کتب درسی و آثار علمی

دیزاین: صمد صبا و سیدکاظم کاظمی

سال چاپ: ۱۳۹۹ هجری شمسی

تیراژ: ۱۰۰۰

چاپ: اول

ویب سایت: www.tveta.gov.af

ایمیل: info@tveta.gov.af

سرود ملی

دا وطـــن افغانســـتان دی — دا عـــزت د هـــر افغـــان دی

کـور د سـولې کـور د تـورې — هـر بچـی یـې قهرمـان دی

دا وطـــن د ټولـــو کـــور دی — د بلوڅـــــو، د ازبکـــــو

د پښـــتون او هـــزاره وو — د ترکمنـــــو، د تاجکـــــو

ورسـره عـــرب، ګوجـــر دي — پامیریـــان، نورســـتانیان

براهـــوي دي، قزلبـــاش دي — هـــم ایمـــاق، هـــم پشـــه‌یان

دا هیـــواد بـــه تـــل ځلیـــږي — لکـــه لمـــر پـــر شـــنه آســـمان

پـــه ســـینه کـــې د آســـیا بـــه — لکـــــه زړه وی جاویـــــدان

نـــوم د حـــق مـــو دی رهبـــر — وایـــو الله‌اکبر وایـــو الله‌اکبر

پیام ادارهٔ تعلیمات تخنیکی و مسلکی

استادان نهایت گرامی و محصلان ارجمند!

تربیت نیروی بشری ماهر، متخصص و کارآمد از عوامل کلیدی و انکارناپذیر در توسعهٔ اقتصادی و اجتماعی هر کشور محسوب می‌گردد و هر نوع سرمایه‌گذاری بزرگ در بخش‌های مختلف اقتصادی نیازمند به پلان‌گذاری و سرمایه‌گذاری در بخش نیروی بشری و توسعهٔ منابع این نیرو می‌باشد. بر مبنای این اصل و بر اساس فرمان شماره ۱۱ مقام عالی ریاست جمهوری اسلامی افغانستان به تاریخ ۱۳۹۷/۲/۱ ادارهٔ تعلیمات تخنیکی و مسلکی از بدنهٔ وزارت معارف مجزا و فصل جدیدی در بخش عرضه خدمات آموزشی در کشور گشوده شد.

اداره تعلیمات تخنیکی و مسلکی به‌عنوان متولی و مجری آموزش‌های تخنیکی و مسلکی در کشور محسوب می‌شود که در چارچوب استراتژی ۵ ساله خویش دارای چهار اولویت مهم که عبارت‌اند از افزایش دسترسی عادلانه و مساویانه فراگیران آموزش‌های تخنیکی و مسلکی در سطح کشور، بهبود کیفیت در ارائه خدمات آموزشی، یادگیری مادام‌العمر و پیوسته و ارائه آموزش نظری و عملی مهارت‌ها به‌طور شفاف، کم‌هزینه و مؤثر که بتواند نیاز بازار کار و محصلان را در سطح محلی، ملی و بین‌المللی برآورده کند، می‌باشد.

این اداره که فراگیرترین نظام تعلیمی کشور در بخش تعلیمات تخنیکی و مسلکی است، تلاش می‌کند تا در حیطهٔ وظایف و صلاحیت خود زمینهٔ دستیابی به هدف‌های تعیین‌شده را ممکن سازد و جهت رفع نیاز بازار کار، فعالیت‌های خویش را توسعه دهد.

نظام اجتماعی و طرز زندگی در افغانستان مطابق به احکام دین مقدس اسلام و رعایت تمامی قوانین مشروع و معقول انسانی عیار است. ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان نیز با ایجاد زمینه‌های لازم برای تعلیم و تربیت جوانان و نوجوانان مستعد و علاقه‌مند به حرفه‌آموزی، ارتقای مهارت‌های شغلی در سطوح مختلف مهارتی، تربیت کادرهای مسلکی و حرفوی و ظرفیت‌سازی تخصصی از طریق انکشاف و ایجاد مکاتب و انستیتوت‌های تخنیکی و مسلکی در سطح کشور با رویکرد ارزش‌های اسلامی و اخلاقی فعالیت می‌نماید.

فلهذا جهت نیل به اهداف عالی این اداره که همانا تربیهٔ افراد ماهر و توسعهٔ نیروی بشری در کشور می‌باشد؛ داشتن نصاب تعلیمی بر وفق نیاز بازار کار امر حتمی و ضروری بوده و کتاب درسی یکی از ارکان مهم فرایند آموزش‌های تخنیکی و مسلکی محسوب می‌شود، پس باید همگام با تحولات و پیشرفت‌های علمی نوین و مطابق نیازمندی‌های جامعه و بازار کار تألیف و تدوین گردد و دارای چنان ظرافتی باشد که بتواند آموزه‌های دینی و اخلاقی را توأم با دست‌آوردهای علوم جدید با روش‌های نوین به محصلان انتقال دهد. کتابی را که اکنون در اختیاردارید، بر اساس همین ویژگی‌ها تهیه و تدوین گردیده است.

بدین‌وسیله، صمیمانه آرزومندیم که آموزگاران خوب، متعهد و دلسوز کشور با خلوص نیت، رسالت اسلامی و ملی خویش را ادا نموده و نوجوانان و جوانان کشور را به‌سوی قله‌های رفیع دانش و مهارت‌های مسلکی رهنمایی نمایند و از محصلان گرامی نیز می‌خواهیم که از این کتاب به‌درستی استفاده نموده، در حفظ و نگهداشت آن سعی بلیغ به خرج دهند. همچنان از مؤلفان، استادان، محصلان و اولیای محترم محصلان تقاضا می‌شود نظریات و پیشنهادات خود را در مورد این کتاب از نظر محتوا، ویرایش، چاپ، اشتباهات املایی، انشایی و تایپی عنوانی ادارهٔ تعلیمات تخنیکی و مسلکی کتباً ارسال نموده، امتنان بخشند.

در پایان لازم می‌دانیم در جنب امتنان از مؤلفان، تدوین‌کنندگان، مترجمان، مصححان و تدقیق کنندگان نصاب تعلیمات تخنیکی و مسلکی از تمامی نهادهای ملی و بین‌المللی که در تهیه، تدوین، طبع و توزیع کتب درسی زحمت‌کشیده و همکاری نموده‌اند، قدردانی و تشکر نمایم.

ندیمه سحر

رئیس ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان

فهرست

عنوان صفحه

مقدمه ..... ح

فصل اول: آشنایی با مفاهیم امنیت شبکه‌های کمپیوتری ۱

۱.۱ تمهیدات امنیتی ۲

۱.۲ مفا هیم اولیهٔ امنیت ۵

فصل دوم: انواع حملات در شبکه‌های کمپیوتری ۱۳

۲.۱ حملات شبکه‌های کمپیوتری ۱۴

۲.۲ شناسایی حملات ۱۴

۲.۲.۱ Packet Sniffer ۱۵

۲.۲.۲ Internet information query ۱۶

۲.۲.۳ Ping sweep ۱۷

۲.۲.۴ Port Scan ۱۸

۲.۳ حملهٔ دسترسی ۱۸

۲.۴ حملهٔ DOS ۲۲

۲.۴.۱ Ping of Death ۲۴

۲.۴.۲ Smurt Attack ۲۵

۲.۴.۳ TCP SYN Flood ۲۶

۲.۵ روش‌های کاهش حملات شبکه ۲۸

۲.۵.۱ کا هش حملات شناسایی ۲۸

۲.۵.۲ کاهش حملات دسترسی ۲۹

۲.۵.۳ کاهش حملات DoS ۲۹

۲.۵.۴ ده روش برای کاهش حملات شبکه ۳۰

فصل سوم: مفهوم AAA در امنیت شبکه‌های کمپیوتری ۳۳

۳.۱ AAA چیست؟ ۳۴

۳.۱.۱ مجوز دسترسی (Authorization) ۳۴

۳.۱.۲ احراز هویت (Authentication) ۳۵

۳.۱.۳ حسابداری (Accounting) ۳۵

۳.۲ احراز هویت در AAA ۳۷

۳.۲.۱ احراز هویت محلی AAA ۳۸

۳.۲.۲ احراز هویت مبتنی بر سرور AAA ۳۸

۳.۳ مجوز دسترسی در AAA ۳۸

۳.۴ حسابداری در AAA ۳۹

۳.۵ چگونگی عیارسازی احراز هویت در AAA محلی ۴۰

۳.۶ مشخصات AAA مبتنی بر سرور ۴۴

۳.۷ تنظیم‌کردن پارامترهای پروتوکول‌های RADIUS و TACACS+ ۴۶
۳.۸ تنظیم‌کردن AAA Authentication ۴۶
۳.۹ تنظیم‌کردن AAA Authorization ۴۸
۳.۱۰ تنظیم‌کردن AAA Accounting ۴۹

فصل چهارم: دیوار آتش (Firewall) ۵۳
۴.۱ دیوار آتش یا (Firewall) ۵۴
۴.۲ سؤالات متداول در مورد دیوار آتش (Firewall) ۵۵
۴.۲.۱ چه کسی به دیوار آتش نیاز دارد؟ ۵۵
۴.۲.۲ چرا به دیوار آتش (Firewall) احتیاج داریم؟ ۵۵
۴.۲.۳ آیا چیز ارزشمندی برای محافظت دارم؟ ۵۶
۴.۲.۴ یک دیوار آتش چگونه عمل می‌کند؟ ۵۷
۴.۳ دیوارهای آتش "سیاست‌گذاری امنیت" هستند ۵۸
۴.۴ خلاصهٔ عملکرد دیوار آتش ۶۱
۴.۵ دیوار آتش در عمل ۶۲
۴.۶ نصب یک دیوار آتش ۶۳
۴.۷ تعیین سیاست دسترسی به داخل ۶۴
۴.۸ تعیین سیاست دسترسی به خارج ۶۵
۴.۹ ملزومات اولیهٔ زندگی در DMZ ۶۶

فصل پنجم: شبکه‌های خصوصی مجازی ۷۰
۵.۱ شبکهٔ خصوصی مجازی (Virtual Private Network-VPN) ۷۱
۵.۲ مقایسه: VPNها به شکلی امن با LAN ارتباط برقرار می‌کنند ۷۲
۵.۳ نمای کلی از VPN ۷۴
۵.۴ مزایا و اهداف VPN ها ۷۵
۵.۵ استراتیژی‌های به‌کارگیری VPN ۷۶
۵.۶ تونل‌زنی دوگانه ۷۸
۵.۷ نمای کلی از VPNهای IPSec ۷۸
۵.۸ معتبر سازی و یکپارچگی داده ۸۰
۵.۹ تونل‌زنی دیتا ۸۰
۵.۱۰ حالت‌های رمزنگاری ۸۲
۵.۱۰.۱ حالت تونل ۸۲
۵.۱۰.۲ حالت حمل ۸۲
۵.۱۱ پروتوکول‌های IPSec ۸۳

فصل ششم: سیستم‌های شناسایی نفوذ ۸۶
۶.۱ چرا از (IDS) در شبکه‌های کمپیوتری استفاده می‌کنیم؟ ۸۷
۶.۲ مفهوم IDS ۸۸
۶.۳ آیا IDS همان فایروال است؟ ۸۹
۶.۴ ملزومات اولیهٔ شناسایی حمله ۹۰

۶.۵ نگاهی بر عملکرد IDS ۹۲
۶.۶ روش تشخیص رفتار غیر عادی ۹۴
۶.۷ روش تشخیص سوء استفاده یا تشخیص مبتنی بر امضا ۹۴
۶.۸ معماری سیستم‌های تشخیص نفوذ ۹۵
۶.۸.۱ سیستم شناسایی حملات شبکه‌یی (NIDS) ۹۵
۶.۸.۲ سیستم شناسایی حملهٔ مبتنی بر میزبان (HIDS) ۹۶
۶.۸.۳ سیستم تشخیص نفوذ توزیع‌شده (DIDS) ۹۷
۶.۹ حملات چگونه شناسایی می‌شوند؟ ۹۹
۶.۹.۱ بازسازی مجدد جریان ارتباطی ۹۹
۶.۹.۲ تحلیل پروتوکول ۱۰۰
۶.۹.۳ شناسایی نا محسوس ۱۰۰
۶.۹.۴ همخوانی الگو/امضا ۱۰۰
۶.۹.۵ تحلیل لاگ (LOG) ۱۰۱
۶.۹.۶ ترکیب روشها ۱۰۲
۶.۱۰ جلوگیری از حمله ۱۰۲
۶.۱۱ عملکردها و پاسخ‌های IPS ۱۰۲
۶.۱۲ محصولات IDS ۱۰۵
۶.۱۳ Snort ۱۰۵
۶.۱۴ محدودیت‌های IDS ۱۰۶

فصل هفتم: سیستم‌های جلوگیری از نفوذ ۱۱۰
۷.۱ IPS - یک راهکار امنیتی فعال ۱۱۱
۷.۲ تفاوت میان IPS و IDS چیست؟ ۱۱۱
۷.۳ انواع عملکردهای IPS در زمان یافتن ترافیک مشکوک: ۱۲۲

منابع (References) ۱۴۲

مقدمه

پس از ظهور انترنت و تجارت الکترونیکی، اگر کمپیوترهای شخصی و همچنین شبکه‌های کمپیوتری به‌صورت مناسب محافظت‌نشده و ایمن نباشند، به‌طرز افزایشی در خطر حملات زیانبار قرار خواهند گرفت. Hackerها، ویروس‌ها، کارمندان کینه‌جو و حتا خطاهای انسانی همگی بیانگر خطرات موجود و آشکار بر شبکه‌ها می‌باشند و همه کاربران کمپیوتر، از اکثر کاربران سادهٔ انترنتی گرفته، تا کاربران شرکت‌های بزرگ می‌توانند، بر اثر رخنه‌های موجود در امنیت شبکه، تحت تأثیر قرار گیرند؛ با وجود این، رخنه‌هایی‌که در امنیت شبکه وجود دارند، به سادگی قابل پیش‌گیری می‌باشند. تحقیق زیر یک دید عمومی در رابطه با معمول‌ترین تهدیدهای امنیتی شبکه و گام‌هایی که یک سازمان می‌تواند در جهت محافظت خود از این حملات و اطمینان از این‌که دیتایی که از شبکهٔ شما می‌گذرد، ایمن خواهد بود، داشته باشد، ارائه می‌دهد.

امنیت شبکه شامل مقررات و سیاست‌های گرفته‌شده توسط مدیریت شبکه است که به‌منظور جلوگیری و نظارت بر دسترسی غیرمجاز، سوء استفاده، اصلاح، یا ایجاد محدودیت در شبکه‌های کمپیوتر ی و منابع قابل دسترس در شبکه، تدوین و اعمال می‌شود. عبارت‌های «امنیت شبکه» و «امنیت اطلاعات» غالباً به جای هم، مورد استفاده قرار می‌گیرند. عدم آشنایی بسیاری از کاربران و کارکنان سازمان‌ها، به نفوذگران کمک می‌کند تا به راحتا وارد یک شبکهٔ کمپیوتر ی شده، از داخل آن به اطلاعات محرمانه، دست پیدا کنند یا این‌که به اعمال خراب‌کارانه بپردازند. هرچه رشد انترنت و اطلاعات روی آن بیشتر می‌شود، نیاز به اهمیت امنیت شبکه، افزایش پیدا می‌کند. امنیت شبکه به‌طور کلی برای فراهم‌کردن امکان حفاظت از مرزهای یک سازمان در برابر نفوذگران (مانند هکرها) به‌کار می‌رود. برای تأمین امنیت بر روی یک شبکه، یکی از بحرانی‌ترین و خطیرترین مراحل، تأمین امنیت دسترسی و کنترول تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سویچ یا دیوارهای آتش. بااین‌حال، امنیت اطلاعات به‌صراحت بر روی محافظت از منابع اطلاعاتی در برابر حملهٔ ویروس‌ها یا اشتباهات ساده توسط افراد درون سازمان متمرکز شده‌است و برای این منظور از تکنیک‌های جلوگیری از ازدست‌رفتن داده‌ها (DLP)[1] بهره می‌برد. یکی از این تکنیک‌ها، تقسیم‌بندی شبکه‌های بزرگ توسط مرزهای داخلی است.

[1] Data Loss Protection

هدف کلی کتاب

آشنایی با مفاهیم اساسی امنیت شبکه، نصب و اعیارسازی وسایل چون firewall، IDs، IPs و شبکه های VPN.

فصل اول

آشنایی با مفاهیم امنیت شبکه‌های کمپیوتری

هدف کلی: در این فصل انتظار می‌رود محصلان با مفاهیم اولیهٔ امنیت شبکه‌های کمپیوتری آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. امنیت شبکه را تشریح نمایند.
۲. Confidentiality را شرح دهند.
۳. Availability را توضیح دهند.
۴. مفهوم Integrity بیان کنند.
۵. Vulnerability را بیان نمایند.

امنیت شبکهٔ Network Security عبارت از دیرگاه است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می‌شود. در این فصل معرفی امنیت شبکه‌های کمپیوتری، مفاهیم اولیهٔ امنیت شبکه کمپیوتری مانند طرح امنیتی، خدمات امنیتی، محرمانگی، احراز هویت و انواع حملات فعال و غیر فعال رامورد بحث قرار خواهیم داد. دانشجویان عزیز این فصل را بادقت مطالعه نمایند، زیرا اصطلاحات به‌کار گرفته در این فصل، در یادگیری فصل‌های بعدی این کتاب کمک خواهند کرد.

۱.۱ تمهیدات امنیتی

دنیایی که در آن زیست می‌کنیم سرشار از قطعات ریز و درشت الکترونیکی شده است. مظاهر زیبای طبیعت آرام‌آرام از زندگی انسان عصر جدید رخت بسته و ساختمان‌های سربه‌فلک‌کشیدهٔ فولادی و بتونی بشر شهرنشین را به زندانیان شادمان مدرنیسم تبدیل کرده است. پیرامون زندگی هر انسان امروزی کمپیوترهای شخصی، سیستم‌های متعدد تلفن ثابت و همراه، دستیاران دیجیتالی[1]، کمپیوترهای کیفی، (خودپرداز بانک)، انواع و اقسام کارت‌های اعتباری، کارت‌های هوشمند، دستگاه‌های کنترول از راه دور، دزدگیر بی‌سیم، وسایل آشپزخانه تمام دیجیتال، سیستم‌های ماهواره‌یی، موقعیت‌یاب دیجیتال[2]، ابزارهای لیزری و مایکروویو، سیستم‌های رادیو و تلویزیون و ده‌ها نوع دیگر از این وسایل و ابزارها جمع شده است.

وقتی زندگی سنتی در حال تغییر به سمت الگوهای مدرن باشد، ناهنجاری‌های اجتماعی نیز رنگ و بوی مدرنیته به خود می‌گیرد! در سال ۱۹۸۸ یک دانشجوی کارشناسی دانشگاه کورنل به نام «روبرت موریس» اولین کرم کمپیوتری را به جان کمپیوترها انداخت تا با آلوده‌ساختن کمپیوترها، منجر به خاموشی آنها شود. هرچند نیت واقعی او صرفاً اثبات برتری هوش و خرد انسان در مقابل ماشین و صرفاً یک تفریح علمی بود ولی سرآغاز ایجاد یک جبههٔ جدید علیه اعصاب و روان اجتماع شد که بعداً به دلیل گره‌خوردن کمپیوترها به زندگی مردم امروزی، خسارت‌های مالی و معنوی هنگفتی نیز در پی داشت. تا جایی که در سال ۱۹۹۴ کلاه‌برداری انترنتی یک گروه روس منجر به ۱۰/۴ میلیون دالر خسارت به Citibank شد.

گروه‌های اخلال‌گر برای آنکه قدرت خود را به رخ جهانیان بکشند، در سال ۱۹۹۶ به وب‌سایت‌های CIA و USA DOJ (که خود از امنیتی‌ترین مراکز آمریکا به شمار می‌آیند) تعرض کردند و با نفوذ در آنها، چهرهٔ این وب سایت‌ها را تغییر دادند.

پس از سال ۲۰۰۰ تقریباً هر سال بیش از یک میلیون حمله علیه معلومات مؤسسات و سازمان‌های دولتی، خصوصی، مراکز مالی و اعتباری، شرک‌های خدماتی و تجارت الکترونیکی گزارش شده است. این تعداد از حملات فقط آنهایی بوده که رسماً اعلام و گزارش شده است، درحالی‌که بسیاری از اخلال‌گری‌ها هرگز در جایی ثبت نمی‌شوند.

---

[1] Personal Digital Assistant

[2] Global Positioning System

اگر وقایع ناخوشایند و خطرناک را در یکی از رده‌های دسترسی غیر مجاز به دیتا، نشتر معلومات محرمانه، از دسترس خارج شدن خدمات یک سرویس‌دهنده، تغییر مخفیانه در دیتا، سرقت دیتا، نابودشدن دیتا، جعل دیتا، اختلال در عملکرد صحیح ماشین کاربران و هر نوع تعرض به حریم دیتای یک ماشین تلقی کنیم، امنیت دیتا عبارتست از مجموعهٔ تمهیدات و روش‌هایی که در یکی از بندهای زیر قرار بگیرد:

الف) تمهیداتی که اطمینان می‌دهند وقایع ناخوشایند هرگز حادث نمی‌شوند؛
ب) تدابیری که احتمال وقوع وقایع خطرناک را کاهش می‌دهند؛
ج) تدابیری که نقاط حساس به خرابی و استراتژیک را در سطح شبکه توزیع کند؛
د) تدابیری که اجازه می‌دهند به محض وقوع وقایع خطرناک، شرایط در اسرع وقت و با کمترین هزینه به شکل عادی برگردد و کمترین خسارت را بر جا بگذارد.

به‌عنوان یک مثال خارج از دنیای کمپیوتر، فرض کنید، بخواهیم مجموعهٔ تمهیدات لازم برای حفظ امنیت منزل شخصی از تعرض سارقان را در چهار ردهٔ بالا دسته‌بندی کنیم، در اینجا رخداد ناخوشایند سرقت مایملک افراد و آسیب به صیانت زندگی و حریم خصوصی عموم مردم است:

الف) تعبیهٔ قفل‌های مستحکم، درب‌های غیر قابل نفوذ، دیوارهای بلند و دارای حصار، نصب سیستم‌های حفاظتی و به کار گماشتن نگهبان، از تمهیدات ردهٔ اول محسوب می‌شود.
ب) هماهنگی با همسایه‌ها، اعتمادنکردن به افراد بیگانه، تکثیرنکردن کلیدها، تغییر متناوب قفل‌ها، مراقبت از کلید، پنهان‌نگه‌داشتن، عدم حضور در منزل، از تمهیداتی است که در ردهٔ دوم از احتمال وقوع وقایع ناخوشایند خواهد کاست.
ج) عدم نگهداری پول و اشیای قیمتی در یک نقطهٔ متمرکز، تقسیم آنها به چند مجموعه و مخفی‌کردن آن‌ها در نقاط مختلف و مطمئن منزل، از تمهیدات ردهٔ سوم به‌شمار می‌آید.
د) با تمام تمهیدات فوق باید وضعیت را به‌گونه‌یی تنظیم کنید که در صورت وقوع یک سرقت چیزی باقی بماند تا بتوان روال زندگی را در اسرع وقت به‌شکل عادی از سر گرفت.

متأسفانه تمهیدات امنیتی یک شمشیر دو لب هستند که هر چه دقیق‌تر و مفصل‌تر به اجرا گذاشته شوند؛ نخست، دسترسی افراد مجاز و خودی را به منابع شبکه، دشوارتر و دست‌وپاگیرتر می‌کنند. دوم هزینهٔ پیاده‌سازی و نگهداری سیستم را به‌شدت بالا می‌برند؛ مثلاً: برای تضمین امنیت منازل شخصی بدیهی است که شما می‌توانید از درب‌های فولادی چندتُنی استفاده کنید. سیم‌های خاردار اطراف منزلتان را به برق فشار قوی متصل کنید و پشت دیوارا را ماین‌گذاری کنید و بجای سگ نگهبان، یک پلنگ گرسنهٔ وحشی در منزل

خود رها کنید. چنین تمهیداتی امنیت منزل شما را به حد متعالی می‌رساند ولی هیچکس حاضر نیست در چنین جهنمی زندگی کند. در چنین وضعیتی اصطلاحاً قابلیت دسترسی[1] به مخاطره افتاده است.

بزرگ‌ترین چالش‌هایی که پیش روی طراحان میکانیزم‌های امنیتی قرار دارد عبارتند از:

- حفظ امنیت سیستم‌هایی که ذاتاً متفاوت و عموماً ناسازگارند، چندان ساده نیست.
- ایجاد اتصال امن بین دو سیستم ناهمگون، نیاز به تمهیدات و مراقبت‌های ویژه دارد.
- نیازها و اهداف امنیتی سیستم‌ها کاملاً متفاوتند.
- بخشی از امنیت یک سیستم به هوش فردی و رعایت یک مجموعه از اصول و ضوابط توسط تک تک کاربران وابسته است.
- تمام راه‌های ورودی و خروجی یک سیستم باید به‌دقت تحت نظارت و مراقبت باشند.
- هزینهٔ پیاده‌سازی، تمهیدات امنیتی باید در سطح معقولی پایین باشد.
- تمهیدات امنیتی نباید دست‌وپاگیر بوده، سیستم را از بهره‌وری ساقط کند.

آرمانی‌ترین حالت وقتی حاصل می‌شود که تمهیدات امنیتی برای کاربران مجاز و افراد خودی، اصلاً به چشم نیاید و به اصطلاح شفاف[2] باشد درحالی‌که برای کاربران غیر مجاز یک حصار تاریک و غیر قابل نفوذ ایجاد کند.

سنگ‌بنای تمام تمهیدات و میکانیزم‌های امنیتی بر بدبینی مفرط و و سواس بی‌حد گذاشته می‌شود. همیشه فرض بر آن خواهد بود که دشمن در کمین و منتظر فرصت است و هیچگاه از حالاتی‌که ممکن است، به ندرت اتفاق بیفتند، چشم‌پوشی نخواهد شد. به‌حیث مثال همیشه می‌توان فرض کرد، دشمن در کمین دیتا، دارای یک ابررایانه با صد هزار پردازنده و قدرت پردازشی هزار میلیارد دستورالعمل در ثانیه است! هر چند چنین احتمالی در عمل صفر است ولی وقتی میکانیزمی با این فرض طراحی شود جای اما و اگر باقی نخواهد ماند و امید دشمن، بدل به یاس خواهد شد.

شاید بزرگترین چالش در دنیای امنیت معلومات آنست که نبرد واقعی بین الگوریتم‌های امنیتی و هوش و خرد انسان اتفاق می‌افتد. وقتی یک طراح، میکانیزم یا تمهیدی را طراحی و آن را در قالب سخت‌افزار یا نرم‌افزار پیاده می‌کند و پی کار خود می‌رود؛ از آن پس در یک طرف جبههٔ الگوریتمی اجراشده بر روی ماشینی بدون شعور قرار دارد و در طرف دیگر دشمنی مجهز به هوش و ذکاوت در تلاش برای شکست‌دادن حریف است.

[1] - Availability

[2] Transparent

۱.۲ مفا هیم اولیهٔ امنیت

در بخش قبل تعریفی ساده از وقایع ناخوشایند و خطرناک ارائه دادیم و دانستیم که در تعریفی عام امنیت عبارت است از میکانیزم‌های پیش‌گیری یا کاهش احتمال وقوع وقایع خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین وقوع وقایع ناخوشایند (وقتی‌که وقایع خطرناک حادث می‌شوند). هر عاملی که به‌طور بالقوه بتواند منجر به وقوع اتفاقی خطرناک بشود، یک تهدید امنیتی[1] به‌شمار می‌آید. تهدیدهای امنیتی می‌توانند، از عوامل ذیل ناشی شوند:

الف) تهدیدهای طبیعی: این تهدیدها از عواملی مثل زلزله، سیل، گردباد، رعدوبرق، آتش‌سوزی، آتشفشان و نظایر آن از قوه به فعل می‌رسند و نسل بشر چنین تهدیدهایی را به‌حیث حقایق زندگی پذیرفته است. این تهدیدها همانگونه که زندگی را هدف گرفته‌اند، می‌توانند در درجات خفیف‌تر منجر به نابودشدن یا افشای معلومات محرمانه و اختلال در سرویس‌دهی مولفه‌های اساسی شبکه شوند. از آنجا که خدمات یا افشای معلومات محرمانه و اختلال در سرویس‌دهی مولفه‌های اساسی شبکه شوند. از آنجا که خدمات شبکه‌های کمپیوتر ی مرزهای جغرافیایی را در نوردیده است، لذا تهدیدهای طبیعی می‌توانند، در خارج از محدودهٔ دید نیز منجر به اختلال در عملیات روزمرهٔ افراد و انتشار بحران در سطح وسیع شوند؛ لذا اگرچه تهدیدهای طبیعی خارج از قدرت بشرند ولی برای بازگرداندن خدمات شبکه از وضعیت بحران به وضعیت عادی از همان ابتدای طراحی شبکه، تمهیداتی برای جلوگیری از گسترش دامنهٔ بحران به مناطق دیگر پیش‌بینی و اجرا می‌شود. به‌حیث مثال ایجاد مراکز پشتیبان در دیگر مناطق جغرافیایی و بهره‌گیری از خطوط ماهواره‌یی در کنار خطوط فایبر نوری در این رده از تمهیدات قرار می‌گیرد.

ب) تهدیدات غیر عمد: تهدیدات غیر عمد از اشتباهات سهوی و ناخودآگاه عوامل انسانی (همانند مدیران شبکه، کارکنان و کاربران) ناشی می‌شود و می‌تواند، منجر به افشا یا نابودی معلومات یا اختلال در خدمات معمول شبکه و گاه تحمیل زیان‌های کلان به جمیع کاربران شود. از این تهدیدات غیرعمد، می‌توان به موارد زیر اشاره کرد:

۱. طراحی نادرست زیرساخت شبکهٔا عدم وجود افزونگی[2] در تجهیزات شبکه؛
۲. عدم تهیل نسخه‌های پشتیبان از دیتای حیاتی؛
۳. سهل‌انگاری در وظایف روزمره (مثل بررسی مستمر سیستم‌ها از لحاظ آلودگی به ویروس)؛
۴. بروز اشکالات پیش‌بینی‌نشده[3] در سطح سخت‌افزار، نرم‌افزار، یا سیستم‌عامل؛
۵. عدم اعمال درست سیاست‌های انتخاب و تعویض مداوم کلمات عبور توسط عوامل درگیر در شبکه.

---

[1] Security Threat

[2] - Redundancy

[3] - Bug

ج) تهدیدات عمدی: تهدیدات عمدی (که بیشترین خسارت و دشوارترین راه مقابله را دارند) عبارتست از هرگونه اقدام برنامه‌ریزی‌شده جهت افشا، نابودی یا تغییر در دیتای حیاتی شبکهٔا ایجاد اختلال در خدمات معمول سرویس‌دهنده‌ها. به‌طور عام هرگونه اقدام برنامه‌ریزی‌شده برای تحقق یک رخداد خطرناک یک تهدید امنیتی عمدی تلقی می‌شود.

واژه‌های زیر در دنیای امنیت معلومات کاربرد بسیار فراوانی دارند:

حمله: هرگاه تهدیدی از قوه به فعل در آید اصطلاحاً یک حمله رخ داده است؛ خواه آن حمله موجب خسارت به منابع شود؛ خواه یک تلاش نافرجام باشد.

آسیب یا خسارت: حمله‌یی‌که در اثر آن منابع شبکه از بین برود یا دستکاری شود، یا معلومات و دیتای محرمانه افشا ویا حریم خصوصی افراد مورد تعرض قرار بگیرد، یا با توسل به جعل هویت و فریب‌کاری، از خدمات معمول شبکه سوءِ استفاده شود اصطلاحاً حمله به مرحلهٔ آسیب رسیده است.

حاشیهٔ امنیت: میزان تخمین قبلی از تهدیدهایی‌که متوجه یک موجودیت در شبکه است و تعیین تمهیدات لازم برای پیش‌گیری از این تهدیدات به حاشیهٔ امنیت موسوم است. قبل از ارائهٔ هرگونه سرویس ابتدا بایستی حاشیهٔ امنیت تمام مولفه‌های شبکه را تعیین کرد.

نقطهٔ آسیب‌پذیر[1]: هرگونه ضعف یا اشکال یک مؤلفه از شبکه در مقابل تهدیدات احتمالی (شامل اشکالات نرم‌افزاری یا سخت‌افزاری، سیستم‌های عامل یا اشتباهات انسانی) که بتواند منجر به حمله شود، اصطلاحاً نقطهٔ آسیب‌پذیر گفته می‌شود. در تعیین حاشیهٔ امنیت بایستی نقاط آسیب‌پذیر شبکه به درستی تعیین و مراقبت‌های لازم به عمل آید. گاه وجود اشکالات بالقوه در یک مؤلفه از قبل قابل پیش‌بینی نیست و ناگهانی بروز می‌کند. لذا همیشه برای تعیین حاشیهٔ امنیت باید با فرض آن‌که نقاط آسیب‌پذیر، نابهنگام آشکار و موجب خسارت می‌شوند، پیش‌بینی‌های لازم را انجام داد.

میزان خطر[2]: تخمینی از احتمال وقوع یک حمله و همچنین پیش‌بینی خساراتی که متعاقب آن حمله به بار می‌آید، به میزان خطر شهرت یافته است. یک مهندس امنیت باید بتواند میزان خطری را که هر یک از مولفه‌های شبکه را تهدید می‌کند، تحلیل کرده و پیامدهای امن را به دقت برآورده کند؛ به‌حیث مثال: باید برآورد شود که به ازای هر یک ساعت که خدمات شبکه از دسترس خارج شود، چه میزان خسارت مالی وارد خواهد آمد.

---

[1] - Vulnerability

[2] - Risk

استراتیژی امنیتی/استراتیژی خطر[1]: تبیین دقیق راهکارهای مقابله با تهدیدات احتمالی شامل تعیین حد اقل حاشیهٔ امنیت و ارائهٔ استدلال هر راهکار (به‌گونه‌یی‌که موفقیت خود را در تیوری و عمل به اثبات رسانده باشد)، استراتیژی امنیتی خوانده می‌شود.

طرح امنیتی[2]: نقشه‌یی دقیق برای نظارت و کنترول تهدیدها، پیاده‌سازی عملی استراتیژی امنیتی و تحت کنترول در آوردن نقاط آسیب‌پذیر (که ناآگاهانه خود را نشان می‌دهند) و به حداقل‌رساندن آسیب‌های احتمالی درصورت بروز حمله‌یی موفق، به طرح امنیتی شهرت دارد.

میکانیزم امنیتی: هر روش یا الگوریتمی‌که برای تشخیص یا پیش‌گیری از وقوع حمله یا برگشت به وضعیت معمولی (پس از وقوع حمله) طراحی می‌شود، میکانیزم امنیتی نامیده می‌شود. هیچ میکانیزم واحدی که بتواند، امنیت دیتا را تضمین کند، وجود ندارد.

خدمات امنیتی[3]: پیاده‌سازی هر نوع میکانیزم امنیتی و ارائهٔ آن‌ها به کاربران به نحوی که میزان خطر را به حد اقل برساند، خدمات امنیتی نام دارد. عمده‌ترین خدمات امنیتی مورد نیاز در شبکه‌های کمپیوتری عبارتند از:

۱. محرمانه ماندن معلومات[4]: به مجموعه مکانیزم‌هایی که تضمین می‌کند دیتا و معلومات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگه‌داشته شود، سرویس محرمانگی اطلاق می‌شود. این سرویس‌ها که عموماً با روش‌های رمزنگاری تحقق می‌یابند، موضوع فصل‌های بعدی خواهد بود.
۲. روش‌های مختلف رمزنگاری معلومات، زیربنای مابقی سرویس‌های امنیتی است.
۳. احراز هویت[5]: مجموعه مکانیزم‌هایی که این امکان را فراهم می‌کنند که بتوان مبدأ (صاحب) واقعی ک پیام، سند یا ترانسکشن[6] را بدون ذره‌یی تردید یا ابهام مشخص کرد، سرویس احزار هویت نامیده می‌شود.
۴. تضمین صحت معلومات[7]: مجموعه مکانیزم‌هایی که از هر گونه تحریف، دستکاری، تکرار[8]، حذف یا آلوده‌سازی دیتا پیشگیری می‌کنند یا حد اقل باعث کشف چنین اقداماتی می‌شوند، سرویس تضمین صحت معلومات نامیده می‌شود.

---

[1] - Security Strategy / Risk Strategy

[2] - Security Plan

[3] - Security Service

[4] - Confidentiality

[5] Authentication

[6] Transaction

[7] Integrity

[8] Replay

۵. انکارناپذیر ساختن پیام‌ها[1]: مجموعه مکانیزم‌هایی که به پیام‌ها و ترانسکشن‌ها، پشتوانهٔ حقوقی می‌بخشد و اجازه نمی‌دهد که فرستنده به هر طریق ارسال پیام خود را انکار کند و یا گیرنده منکر دریافت آن شود، به سرویس انکار ناپذیر ساختن، پیام‌ها شهرت دارد.
۶. کنترول دسترسی[2]: مکانیزم‌هایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترول در آورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آنها قرار می‌دهد، کنترول دسترسی خوانده می‌شود.

منابع اشتراکی بسیار متنوعند: فراخوانی یک تابع کتابخانه‌ای کوچک بر روی ماشین راه دور، میزان پهنای باند مصرفی هر پروسه یا کاربر، کل سیستم فایل، میزان حافظهٔ مصرفی، رکوردهای بانک معلوماتی و حتی فیلدهای یک رکورد در مقولهٔ منابع اشتراکی می‌گنجند. مکانیزم‌های کنترول دسترسی، تمام منابع ریز و درشت شبکه را تحت تسلط در آورده و براساس مجوزهای تعیین‌شده آنها را در اختیار متقاضیان قرار می‌دهند.

حملات مختلف علیه منابع یک شبکهٔا ماشین بسیار متنوع و از شمار خارج‌اند. تمام خدمات امنیتی (شامل محرمانگی، احراز هویت، انکار ناپذیر بودن و صحت پیام‌ها) با این فرض طراحی و پیاده‌سازی می‌شوند که تهدیدهای چهارگانهٔ زیر همیشه علیه آنها وجود دارند و هر لحظه ممکن است اتفاق بیفتند:

الف) استراق سمع[3]: هرگاه یک شخص غیر مجاز به هر نحو بتواند نسخه‌یی از دیتای در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند، حملهٔ استراق سمع به وقوع پیوسته است.
ب) دستکاری[4]: هرگاه دیتای در حال جریان بین مبدأ و مقصد توسط شخص غیر مجاز به هر نحو دستکاری یا تحریف شود، حملهٔ دستکاری دیتا رخ داده است.
ج) جعل[5]: هرگاه یک شخص غیر مجاز اقدام به تولید پیام‌های ساختگی کرده، ارسال آنها را به شخص مجاز دیگری نسبت بدهد، حملهٔ جعل و ارسال دیتای ساختگی به وقوع پیوسته است.
د) وقفه[6]: هرگاه کسی بتواند، سیستم یا سرویسی را در شبکه از کار بیندازد، حملهٔ وقفه رخ داده است.

استراق سمع تهدیدی علیه سرویس محرمانگی دیتا، دستکاری تهدیدی علیه سرویس صحت معلومات، جعل تهدیدی علیه سرویس احراز هویت و وقفه تهدیدی علیه قابلیت دسترسی دائم[7]، به حساب می‌آید. هرگاه

[1] Non-Repudiation
[2] Access control
[3] Interception
[4] Modification
[5] Fabrication
[6] Interruption
[7] Availability

سرویس‌های امنیتی به هر نحو تضمین کنند که هر تهدیدی در تبادل پیام‌های بین طرفین مجاز یک ارتباط، ناکام خواهد ماند، کانالی امن پدیده آمده است.

حملات چهارگانهٔ ذکرشده، احتمال وقوع بالایی دارند و به‌سادگی اتفاق می‌افتند؛ به‌حیث مثال: استراق سمع داده، در محیط شبکه‌های محلی، اغلب به‌سادگی نصب یک برنامهٔ کوچک به نام Sniffer است، همچنین عناصر میانی شبکه مثل روترها می‌توانند، دیتای عبوری را به هر دلیل در اختیار یک شخص ثالث قرار بدهند. برای تهدایداتی مثل دستکاری یا جعل دیتا، انواع و اقسام نرم‌افزار تهیه شده و به وفور در اختیار همگان قرار دارد؛ لذا برای تبدیل‌شدن تهدید به حمله، کافی است یک اخلال‌گر فقط اراده کند. سهل‌ترین شرایط برای اخلال‌گر زمانی است که او به هر طریق به عناصر میانی مثل سویچ‌ها یا روترها دسترسی داشته باشد.

حملاتی که علیه منابع و موجودیت‌های یک شبکه شکل می‌گیرند، به دو ردهٔ کلی‌تر (حملات فعال[1] و حملات غیر فعال[2]) تقسیم‌بندی می‌شوند. حملات فعال، آن‌هایی هستند که به محض شروع، علایم آشکاری از خود بروز می‌دهند و کشف آنها امکان‌پذیر است؛ به‌حیث مثال: حملهٔ نوع وقفه با ازکارافتادن یک سرویس در شبکه خود را نشان خواهد داد. حملهٔ نوع دستکاری پیام یا حملهٔ جعل پیام با توسل به میکانیزم‌های خاص قابل کشف است و در ردهٔ حملات فعال دسته‌بندی می‌شوند. میزان آسیب به منابع و موجودیت‌های شبکه در حملهٔ فعال به قدرت سیستم‌های آشکارسازی حمله و و اکنش سریع آنها بستگی دارد.

حملات غیر فعال هیچ علامت آشکاری در شبکه از خود نشان نمی‌دهند و ممکن است برای ساعت‌ها و هفته‌ها مخفی بمانند. حملهٔ نوع استراق سمع از این دسته حملات محسوب می‌شود و یک اخلاگر می‌تواند، مدت‌های طولانی، به شنود دیتا مشغول بوده، از آنها به نفع خود بهره‌برداری کند، درحالی‌که هیچ ابزار تشخیصی، قادر به کشف چنین حملهٔ خاموشی نباشد. حملات غیر فعال بسیار خطرناک و موجب آسیب بسیار زیاد به موجودیت‌های شبکه هستند. برای پیش‌گیری از چنین حملاتی باید بین طرفین یک ارتباط کانالی امن ایجاد کرد. حملات غیر فعال را می‌توانید، به تومورهای پنهان تشبیه کنید که هیچ علایمی از خود نشان نمی‌دهند و عموماً زمانی خود را نشان می‌دهند که کار از کار گذشته است.

فرض کنید که بین هر دو موجودیت در شبکهٔک کانال امن ایجاد و دیتا به نحوی رمزنگاری شوند که استراق سمع آنها هیچ ارزشی برای افراد غیر مجاز نداشته باشد و هیچ حمله‌یی طرفین ارتباط را تهدید نکند. آیا شنود دیتایی که از لحاظ محتوایی هیچ ارزشی ندارند، برای یک بیگانه، آشکارکنندهٔ هیچ معلوماتی نیست؟ فرض کنید یک اخلال‌گر به‌صورت خاموش و مستمر جریان تبادل معلومات بین دو نقطهٔ A و B در شبکه را استراق سمع کرده و متوجه می‌شود حجم تبادل پیام در ساعات ۱۰ تا ۱۲ اولین شنبه هر ماه به ناگاه افزایش می‌یابد. آیا همین مشاهده نمی‌تواند، بیانگر یک واقعیت و نمادی از یک رخداد جدید باشد؟ قطعاً همین‌طور

[1] Active attack

[2] Passive Attack

است و در اینجا حملهٔ غیر فعال دیگری به‌نام حملهٔ تحلیل‌ترافیک مطرح می‌شود: حملهٔ تحلیل‌ترافیک[1] عبارتست از استراق سمع دنبالهٔ پیام‌های جاری بین دو نقطه از شبکه و استخراج شاخص‌های آماری این جریان به‌منظور آگاهی از نحوهٔ تعامل طرفین ارتباط و تحرکات احتمالی آنها، بدون آن‌که محتوای پیام‌ها آشکار باشد. به‌حیث مثال وقتی تعداد پیام‌های جاری بین دو نقطهٔ A که فرضاً محل تجمع تروریست‌هاست و نقطهٔ B در پایتخت کشوری مفروض، مبادله می‌شوند، در یک مقطع زمان، ناگهانی افزایش پیدا کند، می‌توان نگران یک تحرک‌تروریستی بود. برخی از اخلالگران از این شاخص‌های آماری سوءِاستفاده می‌کنند؛ لذا برای جلوگیری از تحلیل ترافیک، ضمن مراقبت‌های فزیکی از کانال‌های انتقال، باید توزیع‌ترافیک در طول زمان، به‌گونه‌یی تنظیم شود که هیچ شاخص آماری مهمی از آن، قابل استخراج نباشد.

[1] Traffic Analysis Attack

خلاصهٔ فصل اول

در این فصل مفاهیم اولیهٔ امنیت به معرفی گرفته شد. به‌طور کلی مفاهیم امنیت را به سه بخش تقسیم می‌کنند: محرمانگی، صحت و قابل‌دسترس‌بودن. در کنار تعریف این مفاهیم، با مفاهیم دیگری نیز از قبیل انکارناپذیری و تازگی اطلاعات آشنا شدیم. افزون بر مفاهیم فوق، با مفهوم حمله، تهدید، انواع حملات فعال و غیر فعال، کنترول دسترسی، جعل یا دستکاری پیام‌ها، وقفه، استراق سمع و مفاهیم دیگری نیز آشنا شدیم.

سوالات و فعالیت های فصل اول

۱. مفاهیم امنیتی زیر را تعریف کنید:

- طرح امنیتی
- خدمات امنیتی
- محرمانگی
- احراز هویت
- صحت معلومات
- انکارناپذیری معلومات
- استراق سمع
- وقفه

۲. حملات فعال و غیر فعال را تعریف کنید.

فعالیت ها

۱. چند نمونه از حملات فعال را پیدا کنید.

۲. چند نمونه از حملات غیر فعال را پیدا کنید.

فصل دوم

انواع حملات در شبکه‌های کمپیوتری

هدف کلی: محصلان با انواع حملات در شبکه‌های کمپیوتری آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. حملات شبکه‌یی را تعریف نمایند.
۲. انواع حملات شبکه‌یی را تحلیل نمایند.
۳. مشهورترین انواع حملات در شبکه‌های کمپیوتری را تشریح کنند.

امنیت شبکه در طول ۴۰ سال اخیر از اقدامات ابتدایی که در ARPAnet اجرا شد، تکامل یافته است. کار مخرب هکرها و نیاز به حفظ عملیات تجاری موجب می‌شود که امنیت شبکه بیش از پیش مورد اهمیت قرار گیرد. در این فصل انواع حملات شبکه‌های کمپیوتری مورد بحث قرارخواهند گرفت؛ مانند: حملات شناسای، حملات دسترسی و حملات Dos. همچنان با روش‌های کاهش حملات کمپیوتری؛ مانند: کاهش حملات شناسای، کاهش حملات دسترسی و کاهش حملات Dos نیز آشنا خواهیم شد.

۲.۱ حملات شبکه‌های کمپیوتری

حملات شبکه‌های کمپیوتری عبارت از شناسای، دسترسی، و قطع سرویس‌ها به واسطهٔ اشخاص غیر مجاز به شبکه‌های کمپیوتری می‌باشد.

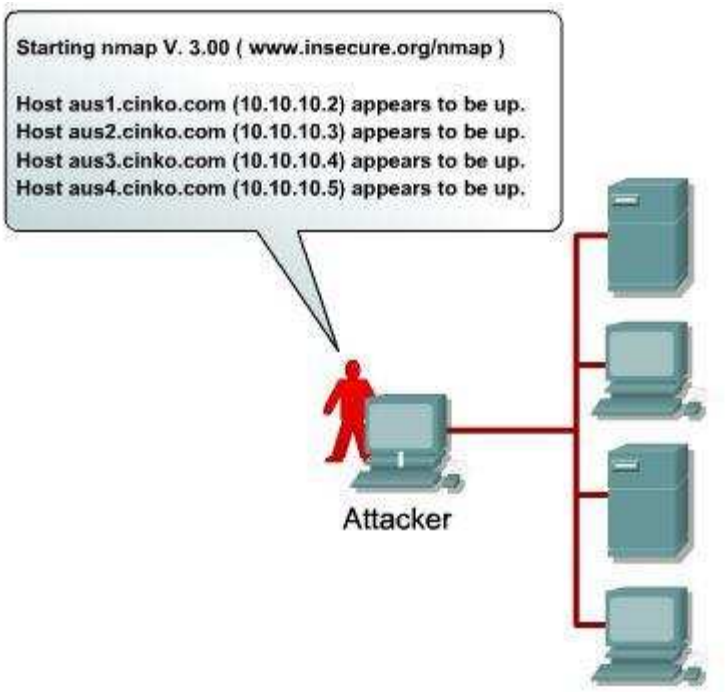
در شبکه‌های کمپیوتری انواع مختلفی از حملات شبکه وجود دارد. برای مقابله با حملات، ابتدا دسته‌بندی انواع مختلف حملات مفید است. با طبقه‌بندی حملات شبکه، می‌توان نوع حملات را به جای حملات فردی مورد توجه قرار داد. هیچ روش استندرد برای طبقه‌بندی حملات شبکه وجود ندارد. روش مورد استفاده در این کتاب، حملات را در سه دستهٔ اصلی طبقه‌بندی می‌کند.

- حملات شناسایی؛
- حملهٔ دسترسی؛
- حملات انکار سرویس.[1]

۲.۲ شناسایی حملات

حملات شناسایی شامل کشف غیر مجاز و نقشه‌برداری از سیستم‌ها، سرویس‌ها یا آسیب‌پذیری‌ها می‌شود. حملات شناسایی غالباً از packet sniffers و port scanner ها استفاده می‌کنند که به‌صورت رایگان در انترنت قابل دسترسی است. شناسایی مشابه با دزدانی است که در محلهٔ خانه‌های آسیب‌پذیر قرار می‌گیرند؛ مانند: یک محل اقامت غیر قانونی یا یک خانه با یک درب یا پنجرهٔ آسان برای بازکردن.

[1] Denial of Service



شکل ۲-۱حملهٔ شناسایی

حملات شناسایی همچنین به‌عنوان جمع‌آوری معلومات شناخته می‌شود و در بیشتر موارد پیش از حملهٔ دسترسی یا حملهٔ DoS انجام می‌شود. یک حملهٔ شناسایی، اخلالگر مخرب، معمولاً با انجام ping sweep از شبکهٔ هدف، به‌منظور تعیین این که کدام آدرس‌های IP فعال هستند، آغاز می‌شود؛ پس از آن اخلالگر تعیین می‌کند که چه سرویس‌ها یا پورت‌ها در آدرس‌های IP فعال در دسترس هستند. Nmap محبوب‌ترین نرم‌افزار برای انجام اسکن پورت است. با استفاده از معلومات مربوط به پورت به‌دست آمده، نفوذگر روی پورت‌ها query می‌گیرد تا نوع و نسخهٔ برنامه و سیستم‌عامل را که در میزبان مقصد اجرا می‌شود، تعیین کند. در بسیاری موارد، مهاجمان به دنبال خدمات آسیب‌پذیر هستند که می‌توانند، بعداً زمانی‌که احتمال کشف حمله کمتر است، مورد سوءِاستفاده قرار گیرند.

حملات شناسایی برای دسترسی به شبکه از ابزارهای مختلف استفاده می‌کند:

- Packet sniffer
- Pring sweep
- Port scan
- Internet information query

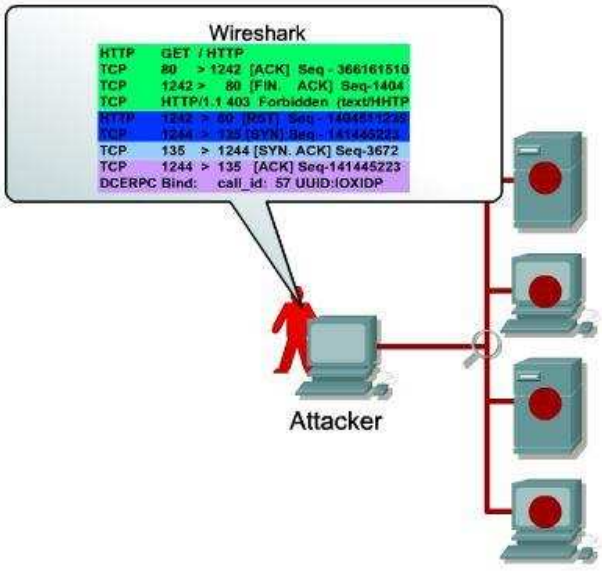
۲.۲.۱ Packet Sniffer

Packet Sniffer یک برنامهٔ نرم‌افزاری است که از کارت شبکه استفاده می‌کند تا تمام پاکِت‌ها در سراسر شبکه را ضبط کند. برخی از برنامه‌های تحت شبکه، پاکِت‌ها را به‌صورت متن سادهٔ رمزگذاری‌نشده ارسال

می‌کنند. از آنجا که پاکِت‌های شبکه رمزگذاری نمی‌شوند، می‌توان آنها را با هر برنامه‌یی که بتواند پاکِت‌ها را از شبکه بخواند، پردازش کند.

Packet Sniffer فقط می‌تواند در همان شبکه که کار می‌کند، حمله کند، مگر این‌که مهاجم به سویچ‌های میانی در شبکه نیز دسترسی داشته باشد.

تعداد زیادی از packet sniffer های رایگان، مانند Wireshark، در دسترس هستند و کاربر نیازی به تمامی‌پروتوکول‌های اساسی شبکه ندارد.

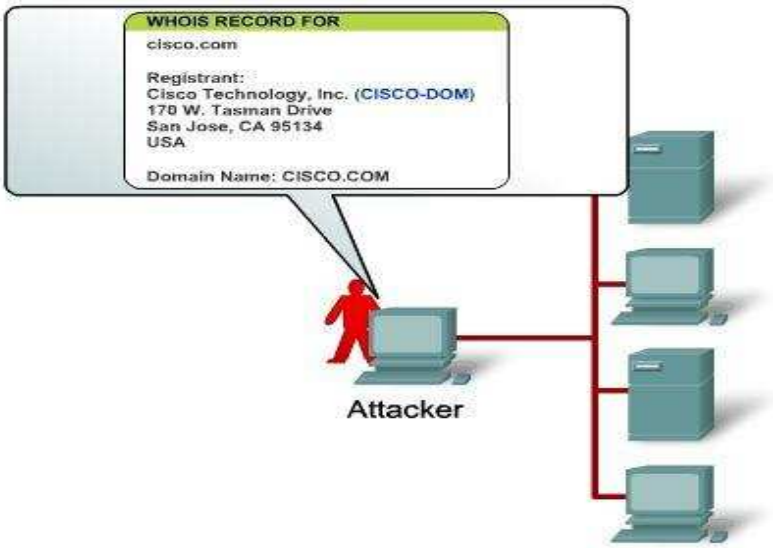


شکل ۲-۲ حملهٔ packet sniffer

برنامه‌های Ping sweep و port scan هنگامی‌که به‌حیث ابزار، مورد استفاده قرار می‌گیرند، یک سری از تست‌ها را علیه میزبان و دستگاه برای شناسایی سرویس‌های آسیب‌پذیر انجام می‌دهند. این معلومات توسط بررسی آدرس IP، پورت، بنر، دیتای هر دو پورت TCP و UDP جمع‌آوری می‌شود. مهاجم از این معلومات برای تهدید سیستم استفاده می‌کند.

۲.۲.۲ Internet information query

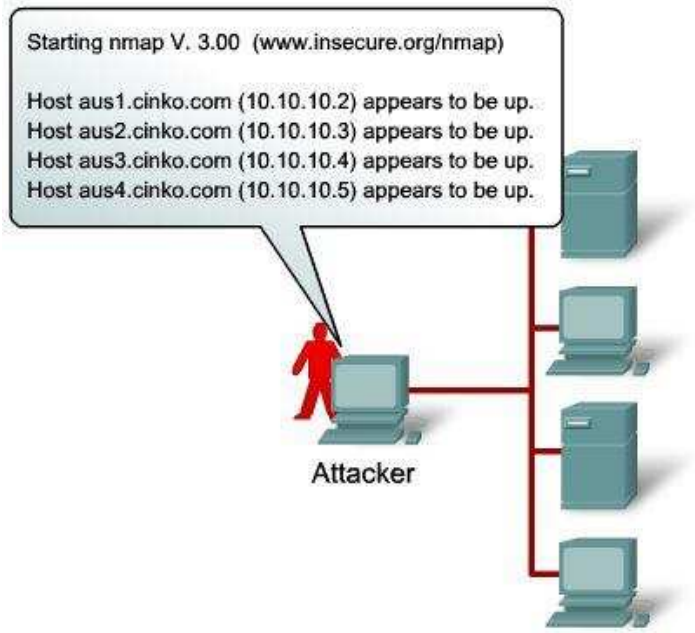
Internet information query می‌تواند معلوماتی نظیر این‌که چه کسی مالک یک دامنهٔ خاص است و چه آدرس‌هایی به آن دامنه اختصاص داده شده است، را نشان می‌دهد. آن‌ها همچنین می‌توانند، نشان دهند که چه کسی دارای یک آدرس IP خاص است و کدام دامنه با کدام آدرس مرتبط است.



شکل ۲-۳حملهٔ internet information query

۲.۲.۳ Ping sweep

Ping sweep یک تکنیک سادهٔ اسکن شبکه است که تعیین می‌کند، کدام محدودهٔ آدرس‌های IP به کمپیوترها یا دستگاه‌ها فعال هستند. یک ping به تنهایی نشان می‌دهد که آیا یک کمپیوتر مشخص در شبکه وجود دارد یا نه. Ping sweep شامل درخواست‌های echo ICMP است که به دستگاه‌های متعدد ارسال می‌شود. اگر یک آدرس داده‌شده فعال باشد، آدرس یک پاسخ echo ICMP را می‌دهد. Ping sweep یکی از روش‌های قدیمی و کند برای اسکن یک شبکه می‌باشد.

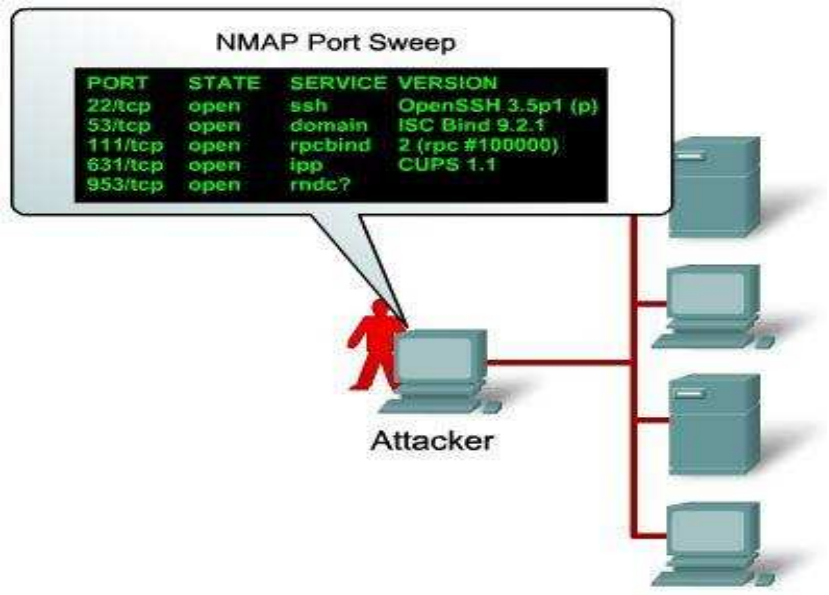


شکل ۲-۴ حملهٔ ping sweep

۲.۲.۴ Port Scan

هر سرویس یک دستگاه با یک شمارهٔ پورت مشخص، مرتبط است. Port scan اسکن محدوده‌یی از پورت‌های TCP یا UDP در یک دستگاه برای شناسایی سرویس‌های فعال است. این کار شامل ارسال پیام به هر پورت دستگاه است. پاسخی که فرستنده دریافت می‌کند، نشان می‌دهد که آیا این پورت استفاده می‌شود یا نه.

Ping sweep آدرس‌ها، در کنار internet information query می‌تواند لستی از دستگاه‌های فعال در یک محیط خاص را پیدا کند. پس از ایجاد این لست، ابزار port scan می‌تواند، از طریق اسکن تمام پورت‌های شناخته‌شده، لست کاملی از تمام سرویس‌هایی را که در دستگاه‌ها اجرا می‌شود، شناسایی کند. سپس هکرها می‌توانند ویژگی‌های برنامه‌های فعال را بررسی کنند، که می‌تواند، به معلومات خاصی دست یابد که برای یک هکر مفید است.



شکل ۲-۵ حملهٔ port scan

به یاد داشته باشید که حملات شناسایی معمولاً پیش از حملات دیگر با هدف دسترسی غیر مجاز به شبکهٔا اختلال در عملکرد شبکه انجام می‌شوند. افراد حرفه‌یی امنیت شبکه، می‌توانند، هنگامی‌که یک حملهٔ شناسایی در حال انجام است، با هشدار (alarm) تنظیم‌شده، زمانی‌که پارامترهای خاص از جمله تعداد درخواست‌های بیش از حد ICMP در هر ثانیه انجام می‌شود، حملات را شناسایی کند. انواع مختلف تکنالوژی‌ها و دستگاه‌ها می‌توانند برای نظارت بر این نوع فعالیت و ایجاد زنگ هشدار استفاده شوند.

۲.۳ حملهٔ دسترسی

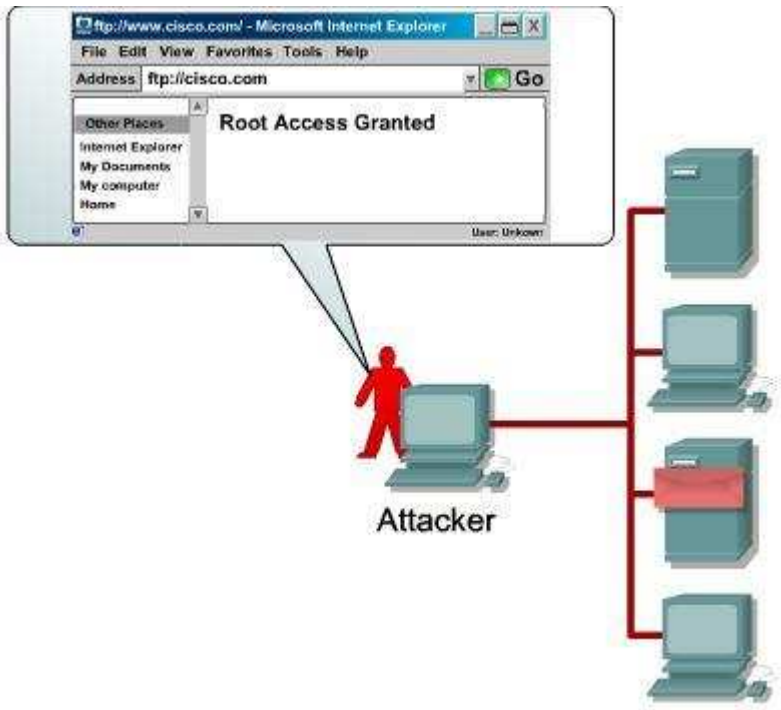
حملات دسترسی از آسیب‌پذیری شناخته‌شده در سرویس‌های احراز هویت، سرویس‌های FTP و سرویس‌های وب برای دسترسی به حساب‌های وب، از دیتابیس‌های محرمانه و دیگر معلومات حساس استفاده

می‌کند. حملهٔ دسترسی می‌تواند به روش‌های مختلف انجام شود. یک حملهٔ دسترسی اغلب یک حملهٔ دیکشنری را برای حدس‌زدن کلمهٔ عبور سیستم استفاده می‌کند. همچنین دیکشنری‌های مخصوصی برای زبان‌های مختلف وجود دارد که می‌تواند مورد استفاده قرار گیرند.

هکرها به سه دلیل از حملات دسترسی در شبکه‌ها یا سیستم‌ها استفاده می‌کنند: استخراج دیتا، دسترسی به آنها و افزایش سطح دسترسی.

حملات دسترسی غالباً حملات رمز عبور را برای حدس‌زدن کلمهٔ عبور سیستم انجام می‌دهند. حملات رمز عبور را می‌توان با استفاده از چندین روش، از جمله حملات brute-force، برنامه‌های تروجان، جعل IP و packet sniffer اجرا کرد. با این حال، بیشتر حملات رمز عبور به حملات brute-force اشاره دارند که شامل تلاش‌های مکرر بر اساس یک دیکشنری برای شناسایی یک حساب کاربری یا رمز عبور است.

حملهٔ brute-force غالباً با استفاده از یک برنامه در سراسر شبکه اجرا می‌شود و تلاش می‌کند تا به یک منبع مشترک مانند سرور دسترسی پیدا کند. پس از این‌که مهاجم دسترسی به یک منبع را به دست آورد، مهاجم دارای حقوق دسترسی مشابه به‌عنوان کاربری است که حساب آن به خطر افتاده است. اگر این حساب دارای امتیازات کافی باشد، مهاجم می‌تواند، یک درب پشتی (back door) برای دسترسی در آینده را بدون هیچ مشکلی برای تغییر وضعیت و رمز عبور حساب کاربری ایجاد کند.



شکل ۲-۶ حملهٔ access attack

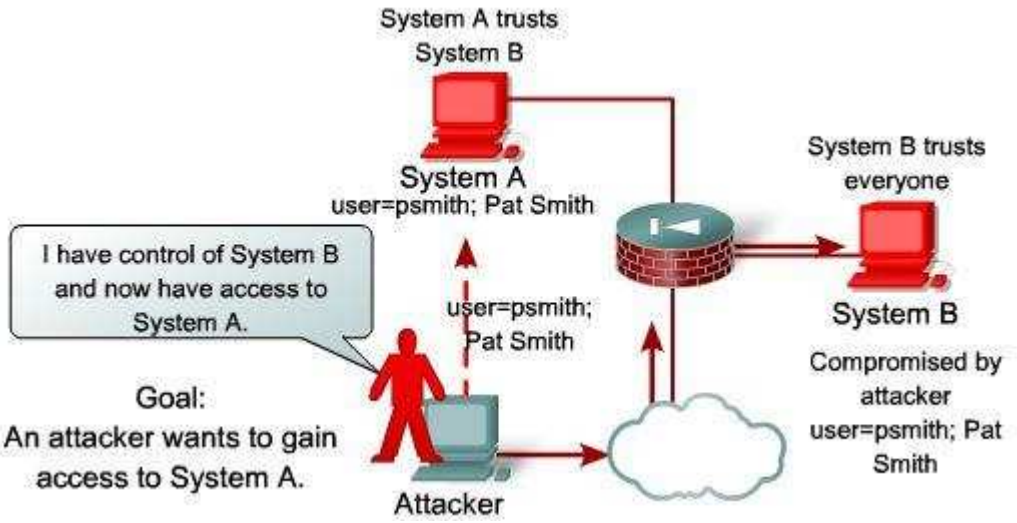
به‌حیث مثال، یک کاربر می‌تواند، برنامهٔ phtCrack۰L یا ۵LC را اجرا کند تا حملهٔ brute-force را برای به‌دست‌آوردن رمز عبور ویندوز سرور انجام دهد. هنگامی‌که رمز عبور به‌دست می‌آید، مهاجم می‌تواند،

یک keylogger را نصب کند که یک کپی از تمام اعمال کلید به یک مقصد دلخواه ارسال می‌کند. یا یک اسب‌تروجان را می‌توان نصب کرد تا یک کپی از تمام پاکِت‌های فرستاده‌شده و دریافت‌شده توسط هدف را به یک مقصد خاص ارسال کند؛ بنابراین امکان نظارت بر تمام‌ترافیک را از آن سرور فراهم می‌کند.

پنج نوع حملهٔ دسترسی وجود دارد:

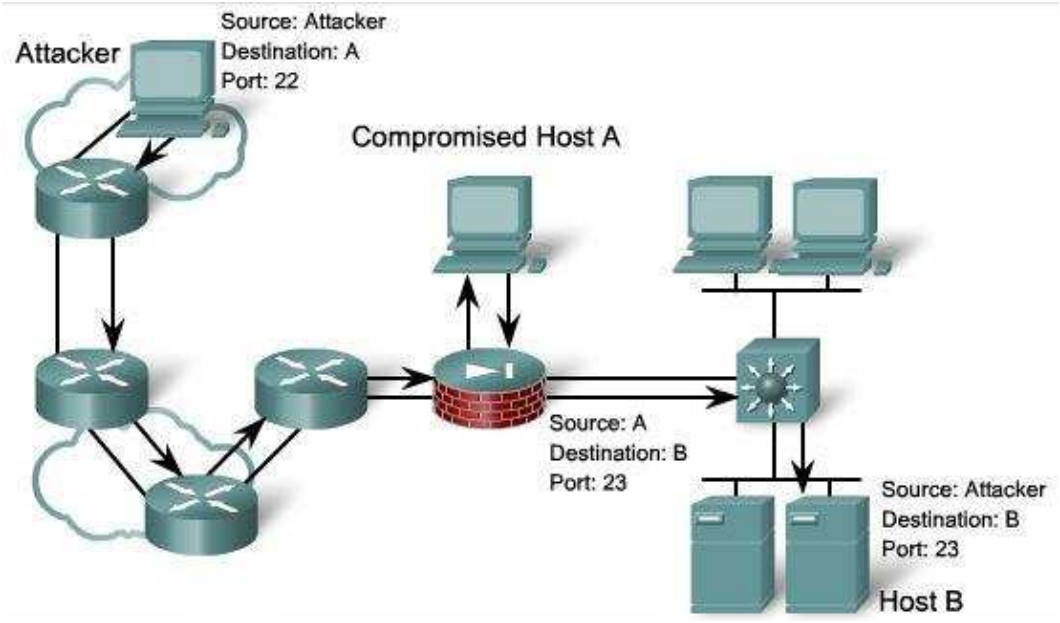
Password attack - مهاجم تلاش می‌کند تا کلمه عبور سیستم را حدس بزند. یک مثال معمول یک حملهٔ دیکشنری است.

Trust exploitation- مهاجم از امتیازات اعطاشده به یک سیستم توسط یک روش غیر مجاز استفاده می‌کند.



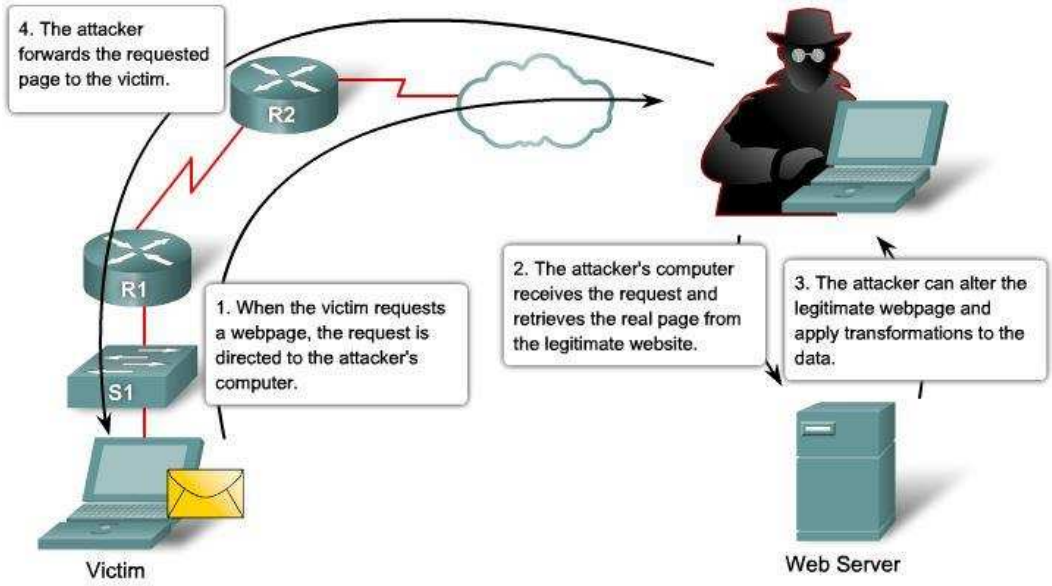
شکل ۲-۷ حملهٔ trust exploitaion

Port Redirection- یک سیستم که قبلاً نفوذ شده به‌عنوان نقطهٔ شروع، برای حملات علیه اهداف دیگر مورد استفاده قرار می‌گیرد.



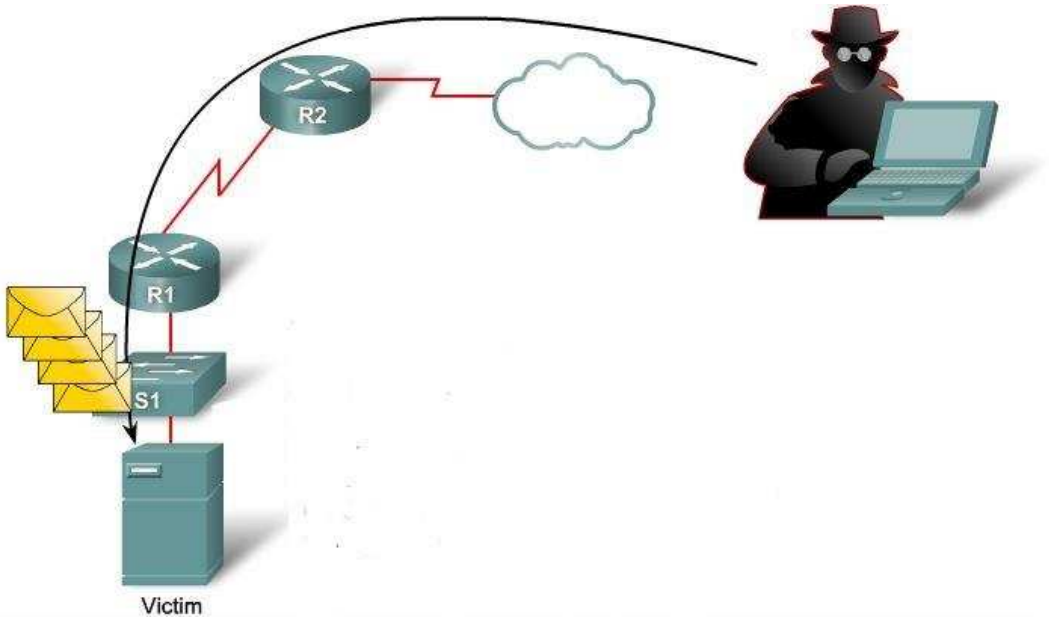
شکل ۲-۸ حملهٔ Port Redirection

Man in the middle: مهاجم در وسط ارتباطات بین دو موجودیت مجاز قرار گرفته است تا معلوماتی را که بین دو طرف در حال مبادله است، بخواند یا اصلاح کند. یک حملهٔ معمول MIM یک لب‌تاپ است که به‌عنوان یک نقطهٔ دسترسی (access point) کار می‌کند و تمام ترافیک شبکه از یک کاربر را ضبط و کاپی می‌کند.



شکل ۲-۹ حملهٔ Man-In-The-Middle

Buffer overflow: یک برنامه، دیتایی را بیشتر از حافظهٔ اختصاص‌یافته بافر می‌نویسد. سرریز بافر معمولاً در نتیجه از یک اشکال نرم‌افزاری در برنامهٔ C یا C++ به‌وجود می‌آید. نتیجهٔ سرریز این است که دیتای معتبر برای اجرای کُدهای مخرب مجدداً مورد استفاده یا سوءِاستفاده قرار می‌گیرند.



شکل ۲-۱۰ حمله buffer overflow

حملات دسترسی به‌طور کلی می‌تواند با بررسی لاگ، میزان استفاده از پهنای باند و process load، شناسایی شود.

سیاست امنیتی شبکه باید مشخص کند که لاگ برای تمام دستگاه‌های شبکه و سرورها نگهداری می‌شود. با بررسی لاگ، پرسونل امنیتی شبکه می‌توانند، تعیین کنند که چه تعداد لاگین ناموفق رخ داده است. سرورهای یونیکس و ویندوز نیز یک لاگ از لاگین‌های ناموفق را ذخیره می‌کند. روترهای سیسکو و دستگاه‌های فایروال می‌توانند برای جلوگیری از لاگین‌های ناموفق پیهم برای یک زمان معین از یک منبع خاص کانفیگ شوند.

حملات MITM اغلب شامل کاپی و تکرار دیتا می‌شود. نشانه‌های این حمله مقدار غیر معمول از فعالیت شبکه و استفاده از پهنای باند است، همان‌طور که توسط نرم‌افزار مانیتورینگ شبکه، نشان داده شده است.

۲.۴ حملهٔ DOS

حملات انکار سرویس تعداد زیادی درخواست (request) را از طریق یک شبکهٔا انترنت ارسال می‌کند. این درخواست‌های بیش از حد، باعث می‌شود که دستگاه هدف به‌طور مطلوب کار نکند. در نتیجه، دستگاه مورد حمله، برای دسترسی و استفادهٔ مجاز از دسترس خارج می‌شود. با استفاده از exploit یا ترکیبی از exploit ها، حملات DoS برنامه‌ها و پروسس‌ها را آهسته یا متوقف می‌کند.

حملهٔ DoS یک حملهٔ شبکه است که منجر به نوعی وقفهٔ سرویس به کاربران، دستگاه‌ها ویا برنامه‌های کاربردی می‌شود. چندین میکانیزم می‌تواند یک حملهٔ DoS ایجاد کند. ساده‌ترین روش این است که مقدار زیادی‌ترافیک شبکه که ظاهراً معتبر است، ایجاد کنیم.

یک حملهٔ DoS از این واقعیت استفاده می‌کند که سیستم‌های هدف مانند سرورها باید معلومات مهم را حفظ کنند. برنامه‌ها ممکن است بر اساس اندازهٔ بافر و محتوای خاص پاکِت‌های شبکه کار می‌کنند. حملهٔ DoS می‌تواند، با ارسال اندازه پاکِت بیش از اندازه سرویس‌ها را از کار بیندازد.

دو دلیل اصلی برای حملهٔ DOS وجود دارد:

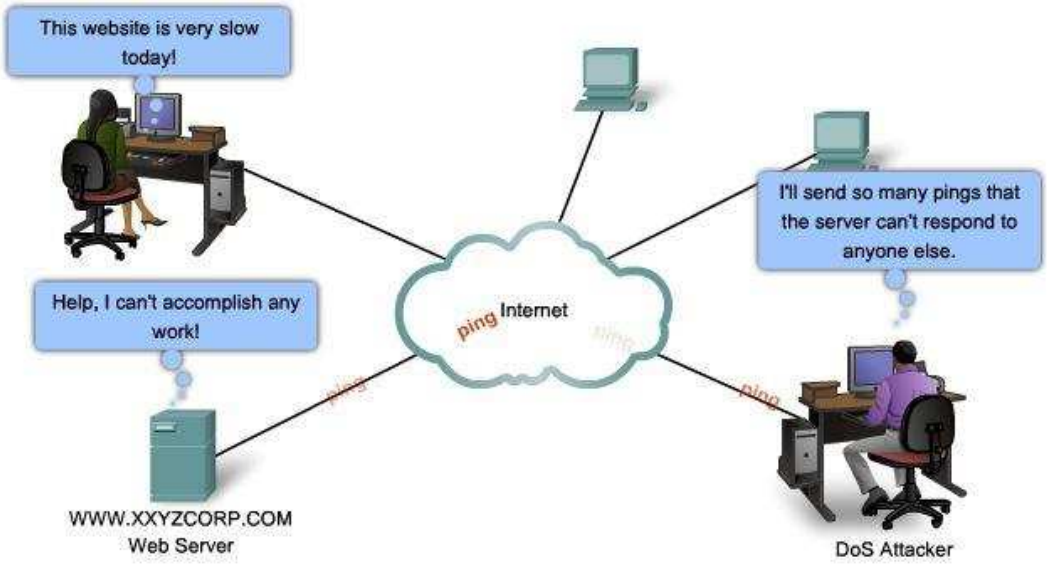
یک دستگاه یا برنامه نتواند به شرایط غیر منتظره مانند دیتای ورودی مخرب رسیدگی کند.

یک شبکه، دستگاه یا برنامه قادر به ادارهٔ مقدار زیادی دیتا نیست و باعث می‌شود سیستم متوقف شده یا بسیار کند شود.

حملات DoS تلاش می‌کنند تا دسترسی به یک شبکه، دستگاه یا برنامه را به خطر بیندازند. این حملات خطر عمده‌یی برای سیستم‌ها حساب می‌شوند زیرا می‌توانند، به‌راحتی یک فرآیند کاری را متوقف کنند و باعث ضرر قابل توجهی شوند. انجام این حملات حتا برای یک مهاجم غیر متخصص نسبتاً ساده است.

یک مثال از حملهٔ DoS یک پاکِت سمی است. یک پاکِت سمی یک پاکِت فارمت‌بندی‌شدهٔ نادرست است که باعث می‌شود، دستگاه دریافت‌کننده، پاکِت را به‌صورت نامناسب پردازش کند. پاکِت‌های سمی باعث می‌شود دستگاه دریافت‌کننده متوقف شود ویا به کندی اجرا شود. این حمله می‌تواند، تمام ارتباطات دستگاه را مختل کند.

در مثال دیگری، مهاجم تعداد زیادی از پاکِت‌ها را ارسال می‌کند که پهنای باند موجود شبکه را از بین ببرد. در اغلب موارد، غیر ممکن است، بین ترافیک مهاجم و ترافیک معتبر شبکه تفکیک شود و منبع حمله به سرعت ردیابی شود. اگر بسیاری از سیستم‌های هستهٔ انترنت به خطر افتاده باشند، ممکن است، مهاجم بتواند از پهنای باند فضای نامحدود استفاده کند تا توفان‌های بسته را به سمت اهداف مورد نظر رها کند.



شکل ۲-۱۱ حملهٔ DOS

DDoS مشابه حملهٔ DoS است، با این تفاوت که یک حملهٔ DDoS از منابع مختلف به‌صورت هماهنگ‌شده انجام می‌شود. حملهٔ DDoS نیاز به متخصص امنیت شبکه برای شناسایی و جلوگیری از حملات توزیع‌شده از منابع مختلف دارد.

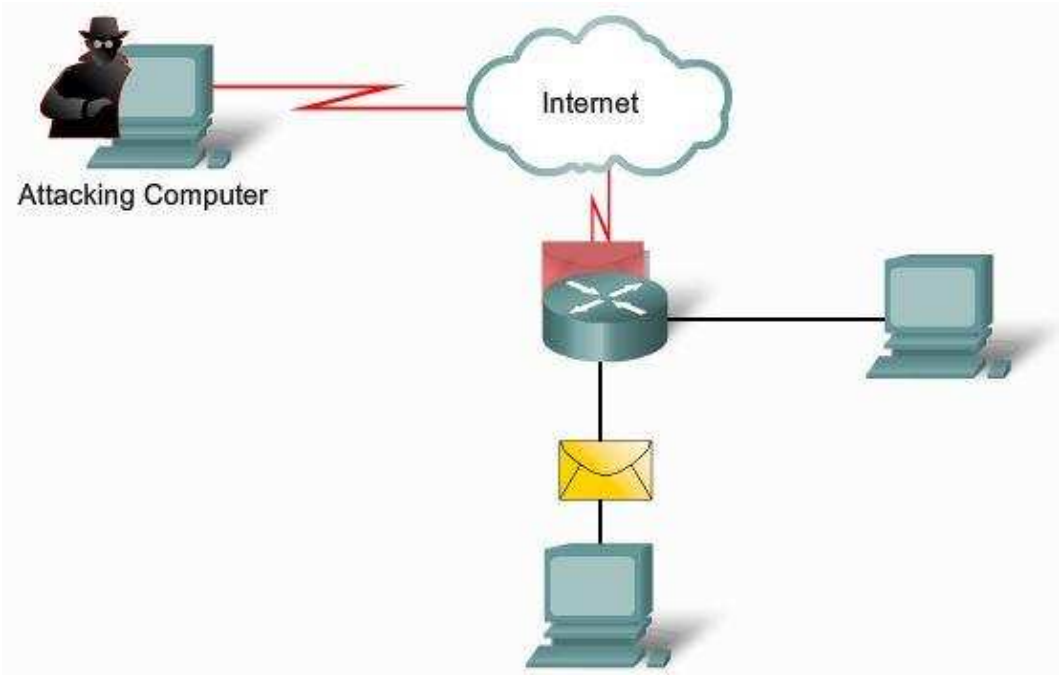
به‌حیث مثال، یک حملهٔ DDoS می‌تواند، به‌صورت زیر عمل کند:

- یک هکر سیستم‌هایی را که در دسترس هستند، اسکن می‌کند.
- پس از این‌که هکرها به چندین سیستم "دستگیره" دسترسی داشته باشند، هکر نرم‌افزار «زامبی» را بر روی آنها نصب می‌کند.
- زامبی‌ها سپس سیستم‌عامل را اسکن و آلوده می‌کنند.
- هنگامی که هکر دسترسی به سیستم عامل پیدا کند، کُد نرم‌افزاری مخرب برای حمله و کنترول از راه دور جهت حملهٔ DDoS آپلود می‌شود.

بهتر است که سه حملهٔ معمولی DoS را برای درک بهتر این که چگونه حملهٔ DOS انجام می‌شود، توضیح دهیم.

۲.۴.۱ Ping of Death

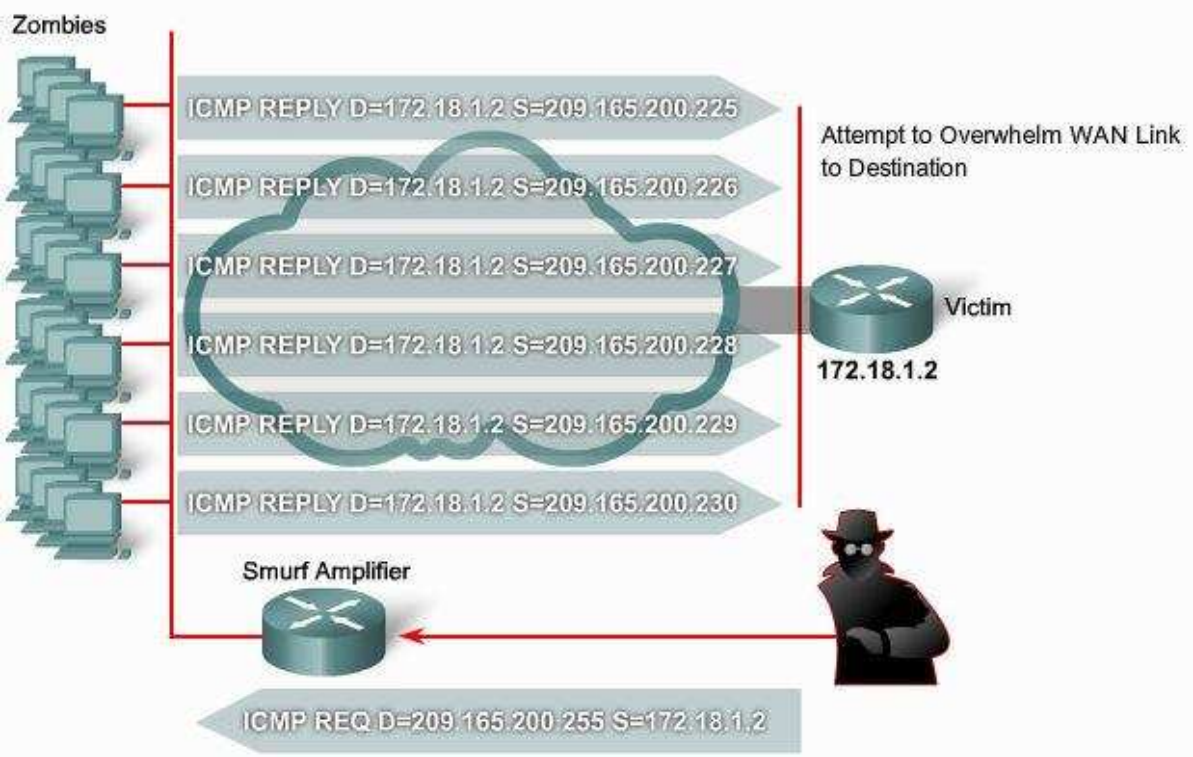
در حملهٔ پینگ مرگ، هکر یک درخواست اکو را در یک پاکِت IP که بزرگتر از حد اکثر اندازهٔ پاکِت یعنی ۶۵،۵۳۵ بایت است، ارسال می‌کند. ارسال یک پینگ با این اندازه می‌تواند، کمپیوتر هدف را خراب کند. یک نوع از این حمله این است که سیستم را با ارسال درخواست‌های ICMP، که بافرهای کمپیوتر هدف را پر می‌کنند، از کار بیندازند.



شکل ۲-۱۲ حملهٔ Ping of Death

۲.۴.۲ Smurt Attack

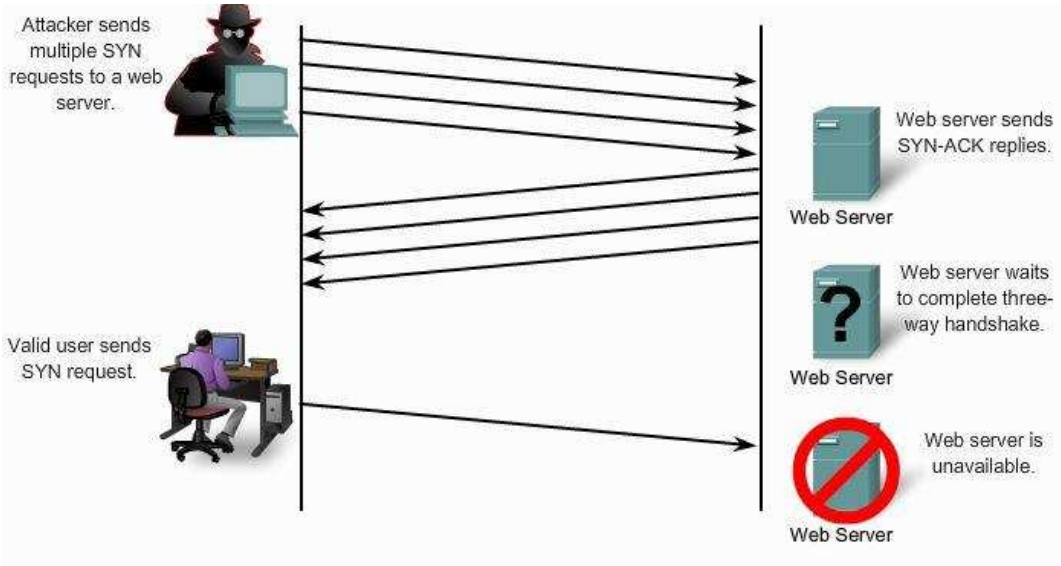
در smurf attack، مهاجم تعداد زیادی از درخواست‌های ICMP را به آدرس‌های شبکه broadcast می‌کند. همهٔ این درخواست‌ها با آدرس‌های جعلی فرستاده می‌شود؛ طوری‌که آدرس منبع را آدرس دستگاه مورد هدف در شبکه قرار می‌دهند. اگر روتر که ترافیک را به آن آدرس‌ها ارسال کند، کمپیوترهای شبکه، پاسخ‌های ICMP را ارسال می‌کنند و میزان ترافیک بسیار بالایی به‌طرف هدف ارسال می‌شود و این ترافیک باعث کندشدن یا متوقف‌شدن سرویس‌های دستگاه خواهد شد.



شکل ۲-۱۳ حملهٔ smurf attack

۲.۴.۳ TCP SYN Flood

در حملهٔ TCP SYN Flood، یک سیل پاکِت‌های TCP SYN اغلب با یک آدرس فرستندهٔ جعلی ارسال می‌شود. هر پاکِت مانند درخواست اتصال پردازش می‌شود و باعث می‌شود، سرور با اتصال یک پاکِت TCP SYN-ACK و در انتظار پاسخ پاکِتی از آدرس فرستنده، یک اتصال نیمه‌باز برقرار کند. با این حال، چون آدرس فرستنده جعل شده است، پاسخ هرگز نمی‌رسد. این اتصالات نیمه‌باز، تعداد اتصالات موجود را که سرور قادر به انجام آن است، اشغال می‌کند، و سرور را از پاسخ به درخواست‌های قانونی تا زمانی‌که حمله به پایان می‌رسد، منع می‌کند.



شکل ۲-۱۴ حملهٔ Syn Flood

حملات TCP SYN Flood، Ping of Death و حملات smurf نشان می‌دهد که یک حملهٔ DOS چقدر می‌تواند مخرب باشد. پنج روش اساسی وجود دارد که از طریق حملات DoS می‌تواند به سیستم‌ها آسیب برساند:

۱. مصرف منابع مانند پهنای باند، فضای دسک یا زمان پردازشگر (cpu)؛
۲. اختلال در معلومات عیارسازی، مانند معلومات روتری؛
۳. اختلال در معلومات حالت، مانند ریست‌شدن ناخواسته TCP Session؛
۴. اختلال در اجزای فزیکی شبکه؛
۵. تضعیف ارتباط بین سیستم قربانی و دیگران.

معمولاً تشخیص این‌که آیا حملهٔ DoS اتفاق افتاده، دشوار نیست. تعداد زیاد شکایات در مورد عدم دسترسی به منابع، اولین نشانه از حملهٔ DoS می‌باشد. برای کاهش چشمگیر تعداد حملات، نرم‌افزاری برای نظارت از میزان استفاده و ترافیک شبکه باید همیشه در حال اجرا باشد. یک گراف میزان استفاده از شبکه می‌تواند، فعالیت غیر عادی یک حملهٔ DoS را نشان دهد.

به یاد داشته باشید که حملات DoS می‌تواند، جزء یک حملهٔ بزرگ‌تر باشد. حملات DoS می‌تواند، منجر به مشکلات در بخش‌های داخلی کمپیوترهای شبکه شود؛ به‌حیث مثال: ظرفیت packet-per-second روتر بین انترنت و شبکه ممکن است از یک حدی تجاوز کند و نه‌تنها سیستم هدف، بلکه کل شبکه را نیز به خطر بیندازد. اگر حمله در مقیاس کافی وسیع باشد، کل مناطق جغرافیایی اتصال به انترنت می‌تواند، به خطر بیفتد.

در هر صورت، حملات DoS یکی از خطرناک‌ترین نوع حملات است و بسیار مهم است که یک متخصص امنیتی شبکه بتواند، به‌سرعت تأثیرات چنین حملات را کاهش دهد.

۲.۵ روش‌های کاهش حملات شبکه

انواع حملات شبکه، روش‌های حملهٔ شبکه و طبقه‌بندی حملات شبکه وجود دارد. سؤال مهم این است، «چگونه می‌توانم این حملات شبکه را کاهش دهم؟»

نوع حمله، همانگونه که توسط طبقه‌بندی شناسایی، دسترسی یا حملهٔ DoS مشخص شده است، ابزارهایی را برای کاهش تهدید شبکه تعیین می‌کند.

۲.۵.۱ کا هش حملات شناسایی

حملات شناسایی را می‌توان از راه‌های مختلفی کاهش داد.

استفاده از احراز هویت قوی، اولین گزینه برای دفاع در برابر packet sniffer ها است. احراز هویت قوی روش احراز هویت برای کاربرانی است که به آسانی قابل دورزدن نباشد. رمز عبور یکبارمصرف (OTP) یک روش احراز هویت قوی است. OTP از احراز هویت دومرحله‌یی استفاده می‌کند. احراز هویت مرحله‌یی‌ترکیبی از چیزی است که یک فرد در اختیار دارد، مانند یک کارت شناسایی، با چیزی که می‌داند، مانند یک رمز عبور. دستگاه‌های خودپرداز (ATM) از احراز هویت دو مرحله‌یی استفاده می‌کنند.

رمزگذاری نیز برای کاهش حملات packet sniffer مؤثر است. اگر ترافیک رمزگذاری شده باشد، استفاده از یک packet sniffer استفادهٔ زیادی نخواهد داشت، زیرا اطلاعات گرفته‌شده قابل خواندن نیست.

ابزارهای نرم‌افزاری و سخت‌افزاری ضد شنود (anti-sniffer)، تغییرات زمان پاسخ (response time) دستگاه را تشخیص می‌دهند تا تعیین کنند آیا دستگاه ترافیک بیشتری را نسبت به ترافیک حالت عادی خود استفاده می‌کند یا نه. بااین‌که این کار تهدید را به‌طور کامل حذف نمی‌کند، اما می‌تواند تعداد موارد تهدید را کاهش دهد.

امروزه استفاده از شبکه با زیرساخت سویچ، امری معمول است که باعث می‌شود هر کس به جز دیتایی‌که در دامنهٔ برخورد (collision domain) خودش قرار دارد، به دیتای دیگری دسترسی نداشته باشد. شبکه با زیرساخت سویچ تهدید packet sniffer را کاملاً برطرف نمی‌کند، اما می‌تواند تا حد زیادی اثر Sniffer ها را کاهش دهد.

جلوگیری کامل از حملهٔ اسکن پورت ناممکن است. اما استفاده از IPS و فایروال می‌تواند اطلاعاتی را که می‌توان با port scanner کشف کرد، محدود کند. اگر ICMP echo و echo-reply روی روترهای مرزی غیر فعال شود، می‌تواند جلو ping sweep و port scan را بگیرد. بااین‌حال، هنگامی‌که این سرویس‌ها خاموش می‌شوند، اطلاعات تشخیص شبکه از بین می‌رود. افزون‌براین، اسکن‌های پورت را می‌توان بدون ping sweep کامل اجرا کرد. اسکن‌ها کمی بیشتر طول می‌کشد زیرا آدرس‌های غیر فعال نیز باید اسکن شوند.

IPS مبتنی بر شبکه و IPS مبتنی بر میزبان معمولاً هنگامی‌که یک حملهٔ شناسایی در حال انجام است، می‌تواند، به مدیر شبکه اطلاع دهد. این هشدار، مدیر را قادر می‌سازد تا برای حملهٔ بعدی بهتر آماده شود یا به ISP اطلاع دهد که کجا حملهٔ شناسایی در حال انجام است.

۲.۵.۲ کاهش حملات دسترسی

تکنیک‌های متعددی برای کاهش حملات دسترسی نیز وجود دارد.

تعداد زیادی از حملات دسترسی با استفاده از حدس‌زدن رمز عبور ویا حملهٔ دیکشنری brute-force روی رمز عبور انجام می‌شود. استفاده از پروتوکول‌های رمزنگاری احراز هویت یا روش‌های هشینگ (hashing)، همراه با یک رمز عبور قوی، احتمال موفقیت این حملات را بسیار کاهش می‌دهد. شیوه‌های خاصی وجود دارد که به‌منظور اطمینان از یک سیاست رمز عبور قوی کمک می‌کند:

بعد از تعداد مشخصی از لاگین‌های ناموفق، حساب کاربر را غیر فعال کنید. این شیوه برای جلوگیری از تلاش‌های مداوم برای پیدا کردن رمز عبور کمک می‌کند.

از رمز عبور ساده استفاده نکنید. از رمز عبور یکبارمصرف (OTP) یا رمز عبور hash شده استفاده کنید.

از رمز عبور قوی استفاده کنید. رمزهای عبور قوی حد اقل هشت کاراکتر دارند و حاوی حروف بزرگ، حروف کوچک، اعداد و کاراکترهای خاص هستند.

شبکه باید با استفاده از اصل حد اقل اعتماد طراحی شود. این بدان معنا است که اگر سیستمی به سیستم دیگر نیاز ندارد، نباید بتواند، از آن استفاده کند. به‌حیث مثال، اگر یک سازمان دارای یک سرور است که توسط دستگاه‌های غیر قابل اعتماد مورد استفاده قرار می‌گیرد، مانند سرورهای وب، دستگاه مورد اعتماد (سرور) نباید به دستگاه‌های غیر قابل اعتماد (سرورهای وب) بدون قید و شرط اعتماد کند.

رمزنگاری یک جزء حیاتی از هر شبکهٔ امن مدرن است. توصیه می‌شود برای دسترسی از راه دور به یک شبکه، از رمزگذاری استفاده شود. ترافیک پروتوکول روتری نیز باید رمزگذاری شود. هر چه بیشتر ترافیک رمزگذاری شده باشد، هکرها فرصت کمتری برای متوقف‌کردن دیتا با حملات MITM دارند.

۲.۵.۳ کاهش حملات DoS

شرکت‌هایی که حضور گسترده‌یی در انترنت دارند، باید پیشاپیش چگونگی پاسخ به حملات احتمالی DoS را پیش‌بینی کنند. از لحاظ تاریخی، بسیاری از حملات DoS از آدرس‌های منبع جعلی گرفته شده‌اند. این نوع حملات را می‌توان با استفاده از تکنالوژی‌های anit-apoofing در روترها و فایروال‌ها کاهش داد. امروزه بسیاری از حملات DoS، حملات DDoS هستند که توسط کمپیوترهای آلوده در شبکه‌های مختلف انجام می‌شوند. مقابله با حملات DDoS نیاز به تشخیص دقیق، برنامه‌ریزی و همکاری از ISP ها دارد.

مهم‌ترین عناصر برای مقابله با حملات DoS عبارتند از فایروال‌ها و IPSها. هم IPS مبتنی بر میزبان و هم IPS مبتنی بر شبکه برای شبکه‌های کمپیوتری شدیداً توصیه می‌شود.

روترها و سویچ‌های سیسکو از تعدادی از تکنولوژی‌های anti-spoofing، مانند port security، DHCP snooping، IP Source Guard، Dynamic ARP Inspection و ACL ها را پشتیبانی می‌کنند.

درنهایت، هرچند کیفیت سرویس (QoS) به‌حیث یک تکنالوژی امنیتی طراحی نشده است، یکی از برنامه‌های کاربردی آن، نظارت بر ترافیک (traffic policing)، می‌تواند برای محدودکردن ترافیک ورودی از هر مشتری به یک روتر مرزی استفاده شود. این کار تأثیر استفاده از پهنای باند توسط یک منبع را می‌تواند محدود کند.

۲.۵.۴ ده روش برای کاهش حملات شبکه

دفاع از شبکه در برابر حمله مستلزم مراقبت و آموزش مداوم است. ده روش بهتری که تا حدودی امنیت شبکهٔ شما را تأمین می‌کنند، به‌صورت زیر است:

۱. پَچ‌ها (patch) را همیشه آپدیت نگهدارید و آنها را در صورت امکان هر هفته یا هر روز نصب کنید تا از سرریز بافر (buffer overflow) و حملات مشابه جلوگیری شود.

۲. سرویس‌ها و پورت‌های غیر ضروری را غیر فعال کنید.

۳. از رمز عبور قوی استفاده کنید و هر چند وقت یکبار آن‌ها را تغییر دهید.

۴. دسترسی فزیکی به سیستم‌ها را کنترول کنید.

۵. از ورودی غیر ضروری در صفحات وب اجتناب کنید. برخی از وب‌سایت‌ها به کاربران امکان می‌دهند، نام کاربری و کلمهٔ عبور خود را وارد کنید. هکر می‌تواند بیش از یک نام کاربری را وارد کند. برای مثال، ورود "jdoe; rm –rf /" ممکن است به مهاجم اجازه دهد سیستم فایل root را از یک سرور یونیکس حذف کند. برنامه نویسان باید کاراکترهای ورودی را محدود کنند و کاراکترهای نامعتبر مانند |؛ <> به‌حیث ورودی قبول نکنند.

۶. بک‌اپ‌گیری و تست‌کردن فایل بک‌اپ را به‌صورت منظم انجام دهید.

۷. کارکنان را در مورد خطرات مهندسی اجتماعی آموزش دهید و استراتژی‌هایی برای احراز هویت تلفونی، از طریق ایمیل ویا به‌صورت شخصی ایجاد کنید.

۸. اطلاعات حساس را رمزگذاری و با رمز عبور قوی از آن محافظت کنید.

۹. امنیت را با پیاده‌سازی سخت‌افزار و نرم‌افزار امنیتی انجام دهید، مانند فایروال‌ها، IPSها، VPN، نرم‌افزار آنتی ویروس و فیلترکردن محتوا.

۱۰. یک سیاست امنیتی به‌صورت کتبی برای شرکت ایجاد کنید.

این روش‌ها فقط یک نقطهٔ شروع برای مدیریت امنیت هستند. سازمان‌ها باید همیشه در برابر تهدیدات مستمر آمادگی داشته باشند. با استفاده از این روش‌های اثبات‌شده برای تأمین شبکه و استفاده از دانش در این فصل، شما اکنون آماده هستید تا راه‌حل‌های امنیتی شبکه را آغاز کنید. یکی از اولین ملاحظات اولیه، امنیت دسترسی به دستگاه‌های شبکه است.

خلاصهٔ فصل دوم

امنیت شبکه در طول ۴۰ سال اخیر از اقدامات ابتدایی که در ARPAnet اجرا شد، تکامل یافته است. کار مخرب هکرها و نیاز به حفظ عملیات تجاری موجب می‌شود که امنیت شبکه بیش از پیش مورد اهمیت قرار گیرد. سازمان‌های امنیتی شبکهٔک انجمن برای متخصصان جهت همکاری و بهبود مهارت‌های خود فراهم می‌کنند. امنیت شبکه شامل دامنه‌های مختلفی است که به متخصصان اجازه می‌دهد که در زمینهٔ امنیت شبکه تخصص و ساختار خود را ارائه دهند. سیاست‌های امنیتی شبکهٔک چارچوب عملی را برای ارتباط همه اقدامات امنیتی شبکه در یک سازمان فراهم می‌کند.

در این فصل سه نوع کلی حملات مورد بررسی قرار گرفت: حملات شناسایی، حملات دسترسی و حملات DoS. حملات شناسایی شامل کشف غیر مجاز و نقشه‌برداری از سیستم‌ها، خدمات و آسیب‌پذیری‌ها می‌شود. دسترسی به حملات از آسیب‌پذیری شناخته‌شده در سرویس‌های احراز هویت، سرویس‌های FTP و خدمات وب برای دسترسی به حساب‌های وب، دیتابیس‌های محرمانه و دیگر اطلاعات حساس استفاده می‌کند. حملات DoS تعداد بسیار زیادی از درخواست‌ها را در یک شبکهٔا انترنت ارسال می‌کند. این درخواست‌های بیش‌ازحد، دستگاه هدف را بیش‌ازحد تحریک می‌کند که عملکرد را کاهش می‌دهد. شناسایی، دسترسی و حملات DoS با تکنیک‌ها، دستگاه‌ها و تکنیک‌های خاص حل‌وفصل می‌شود.

سوالات و فعالیت فصل دوم

۱. در حالت کلی حملات به چند دسته تقسیم می‌شوند؟

۲. انواع حملات شناسایی را نام ببرید

۳. انواع حملات دسترسی را نام ببرید.

۴. انواع حملات DoS را نام ببرید.

۵. روش‌های کاهش حملات شناسایی را بیان کنید.

۶. روش‌های کاهش حملات دسترسی را بیان کنید.

۷. روش‌های کا هش حملات DoS را بیان کنید.

فعالیت

۱. غیر از حملاتی که در این فصل معرفی شد، حد اقل دو حملهٔ دیگر برای حملات شناسایی، دسترسی و DoS بیان کنید.

فصل سوم

مفهوم AAA در امنیت شبکه‌های کمپیوتری

هدف کلی: محصلان با مفاهیم AAA آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. AAA را شرح دهند
۲. AAA Authentication را توضیح دهند.
۳. AAA Authorization را بیان نمایند.
۴. AAA Accounting را تشریح نمایند.

در این فصل در مورد مفهوم AAA در امنیت شبکه‌های کمپیوتری بحث می‌شود. هر یک از این حروف A مفهوم یا نقش خاصی را شامل می‌شود که وقتی طراحی و پیاده‌سازی شد، امنیت شبکهٔ شما را افزایش می‌دهد. لهذا در جریان فصل با موضوعاتی چون نحوهٔ کار و عملکرد پروتوکول احراز هویت، مجوز و حسابداری (AAA)، عیارسازی یک روتر سیسکو برای انجام احراز هویت AAA با یک دیتابیس محلی و تنظیمات AAA مبتنی بر سرور آشنا خوا هیم شد.

۳.۱ AAA چیست؟

AAA مجموعه‌یی از مفاهیم پایه‌یی است که در فهم امنیت کمپیوتر و شبکه به کمک ما می‌آیند. ما بدون آن‌که متوجه شویم، روزانه بارها و بارها در مواردی مانند محافظت از معلومات و سیستم‌ها در برابر تهدیدات عمدی و غیر عمدی از اصول AAA استفاده می‌کنیم. اما واقعاً AAA چیست؟

در واقع AAA از کنار هم قرارگرفتن حروف اول Authorization، Authentication و Accounting تشکیل شده است. اما این سه مفهوم چه کاری را انجام می‌دهند؟ علاوه بر در دسترس قراردادن پلت‌فرم در شبکه، مهم‌ترین هدف هر سه اصل بالا، پشتیبانی و محافظت از محرمانگی، صحت و قابل‌دسترس‌بودن و در یک کلام CIA است.

به‌طور خلاصه می‌توان CIA را به این‌صورت تعریف کرد:

- محرمانگی (Confidentiality): معلومات و محتوای موجود مورد سرقت قرار نگیرد.
- صحت (Integrity): معلومات و محتوای موجود دست‌نخورده باقی بماند و ویرایش نشود.
- قابلیت دسترسی (Availability): در صورت مجازبودن، معلومات و محتوای موجود در دسترس باشد.

این سه مفهوم اگرچه ظاهراً سه بخش مختلف را تشکیل می‌دهند، اما درواقع در کنار هم ارتباط تنگاتنگی دارند و با یکدیگر کار می‌کنند. سطح استفاده از هر کدام از سه مفهوم بالا، به‌طور مستقیم سطح کنترول دسترسی به منابع و تجهیزات شبکه را مشخص می‌کند. در ادامه به بررسی جزئی‌تر هر یک از سه مفهوم تشکیل‌دهندهٔ AAA خواهیم پرداخت.

۳.۱.۱ مجوز دسترسی (Authorization)

مجوز دسترسی را می‌توان یک پالیسی، مولفهٔ نرم‌افزاری ویا عنصر سخت‌افزاری در نظر گرفت که در دسترس قراردادن ویا جلوگیری از دسترسی به یک سورس در شبکه استفاده می‌شود. برای این کار می‌توان از کامپوننت‌های پیشرفته‌یی مثل Smart Card، دیوایس‌های Biometric ویا سخت‌افزارهای دسترسی به شبکه مثل روترها، ریموت‌اکسس‌پاینت‌ها (RAS و VPN ها) ویا اکسس‌پاینت‌های وایرلس (WAP) استفاده کرد. فارغ از بُعد سخت‌افزاری، مجوز دسترسی می‌تواند به‌صورت تعیین حق دسترسی (permission) بر روی یک فایل ویا سورس به اشترک‌گذاشته‌شده در شبکه باشد. برای نمونه می‌توان به

خصوصیت نرم‌افزار NTFS در ویندوز مایکروسافت اشاره کرد. درنهایت با کنارگذاشتن دو بُعد سخت‌افزاری و نرم‌افزاری که در بالا به آن اشاره شد، کنترول دسترسی می‌تواند به‌صورت قانونی (rule) باشد که محدودیت‌های یک نرم‌افزار را در محیط سیستم ویا شبکه تعیین می‌کند.

۳.۱.۲ احراز هویت (Authentication)

احراز هویت را می‌توان فرآیندی تعریف کرد که در طی آن هویت ماشین ویا کاربری که قصد دسترسی به شبکه و یا منابع شبکه را دارد، تشخیص و مورد بررسی قرار می‌گیرد.

۳.۱.۳ حسابداری (Accounting)

Accounting را می‌توان فرآیند پیگیری و مرور رخدادها، خطاها، دسترسی‌ها و تلاش‌های دسترسی در یک سیستم تعریف کرد. مشابه روش‌های مرسوم حساب‌رسی برای پیگیری جریان مالی یک سازمان، در زمینهٔ امنیت هم شما نیاز دارید تا بتوانید، سابقه و جریان تلاش‌های دسترسی، دسترسی‌های موفق ویا ناموفق، مشکلات رخداده در سیستم یا خطاها و رخدادهای دیگر را که در بحث مانیتورینگ و کنترول یک سیستم حائز اهمیت هستند، پیگیری کنید.

قابلیت Accounting به‌طور پیش‌فرض بر روی بسیاری از سیستم‌های عامل فعال نیست و مدیر سیستم یا مدیر شبکه باید بر حسب نیاز خود آن را فعال بسازد.

AAA مزایای زیر را برای ما فراهم می‌کند:

۱. افزایش امنیت برای تنظیمات دستگاه‌ها با اجازه‌دادن به تعداد محدودی از کاربران؛
۲. امکان داشتن چندین بک‌اپ از دسترسی‌های انجام‌شده در شبکه؛
۳. استفاده از پروتوکول‌های استندرد مانند TACACS+ و RADIUS و Kerberos.

یک شبکه باید طوری طراحی شود که افرادی که مجاز به اتصال به آن هستند و آنچه که آنها مجاز به انجام آن هستند و زمانی که آنها متصل هستند، را کنترول کند. این مشخصات طراحی در سیاست امنیتی شبکه مشخص شده است. این سیاست مشخص می‌کند که چگونه مدیران شبکه، کاربران شرکت‌های بزرگ، کاربران از راه دور، شرکای تجاری و مشتریان به منابع شبکه دسترسی پیدا کنند. سیاست امنیتی شبکه همچنین می‌تواند اجرای یک سیستم حسابداری (accounting) را تعیین کند که چه کسی، در چه زمانی وارد سیستم شده و چه کاری انجام داده است.

مدیریت دسترسی شبکه در حالت کاربر (user mode) یا حالت privilege محدود است و برای تمام مقیاس‌های شبکه‌های کوچک و بزرگ مناسب نیست. در عوض، استفاده از پروتوکول احراز هویت، مجوز و حسابداری (AAA)، چارچوب لازم را برای دستیابی به امنیت دسترسی در مقیاس شبکه‌های بزرگ و کوچک فراهم می‌کند.

روترهای سیسکو IOS را می‌توان برای استفاده از AAA برای دسترسی به‌نام کاربری و رمز عبور در یک دیتابیس محلی عیارسازی کرد. استفاده از یک نام کاربری و رمز عبور در دیتابیس محلی، امنیت بیشتری نسبت به یک رمز ساده ایجاد می‌کند و یک راه‌حل امنیتی مؤثر است که به‌راحتی اجرا می‌شود.

مزاحمان شبکه به‌طور بالقوه می‌توانند، به تجهیزات و سرویس‌های حساس شبکه دست پیدا کنند. کنترول دسترسی این را که چه کسی به چه چیزی از منابع و سرویس‌های خاص می‌تواند، استفاده کند، محدود می‌کند. بسیاری از انواع روش‌های احراز هویت بر روی یک دستگاه سیسکو می‌توانند، انجام شوند و هر یک از روش‌ها، سطوح مختلف امنیتی را ارائه می‌دهد.

ساده‌ترین نوع احراز هویت کلمهٔ عبور است. این روش با استفاده از یک‌ترکیب login و password بر روی پورت کنسول، پورت vty و پورت‌های aux عیارسازی می‌شود. این روش ساده‌ترین روش از نظر پیاده‌سازی و همچنین ضعیف‌ترین و با کمترین امنیت است. لاگین‌هایی که فقط با پس‌ورد کار می‌کنند، در مقابل حملهٔ brute-force بسیار آسیب‌پذیر هستند. افزون‌براین، این روش هیچگونه حساب‌رسی (accounting) را فراهم نمی‌کند. هر کسی با رمز عبور می‌تواند وارد دستگاه شود و تنظیمات را تغییر دهد.

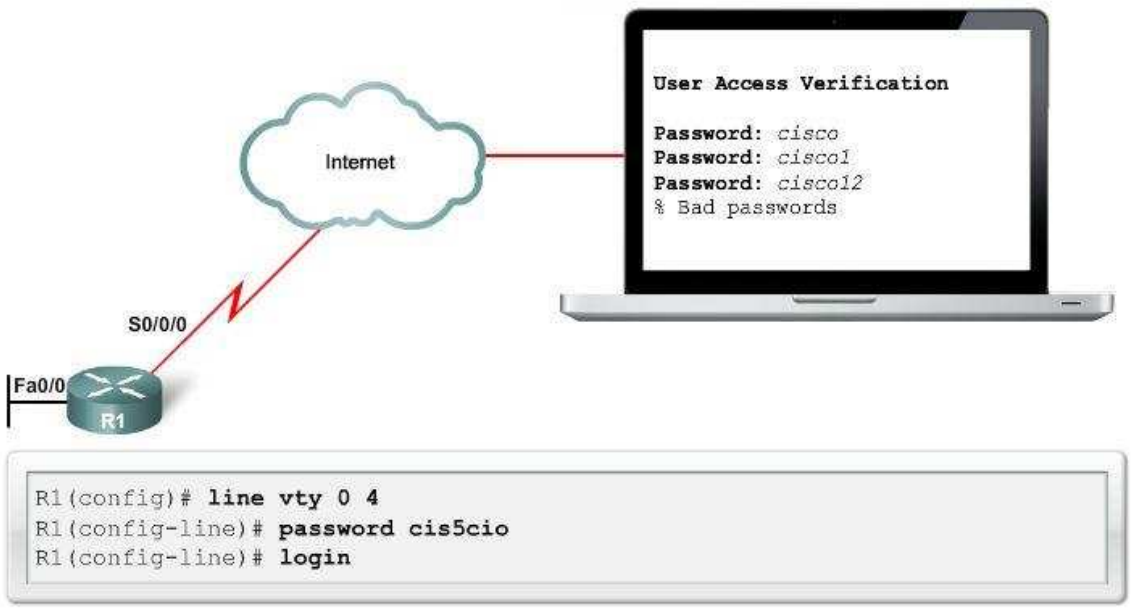
برای accountability بهتر، احراز هویت با استفاده از دیتابیس محلی با یکی از دستورات زیر اجرا می‌شود:

username username **password** password

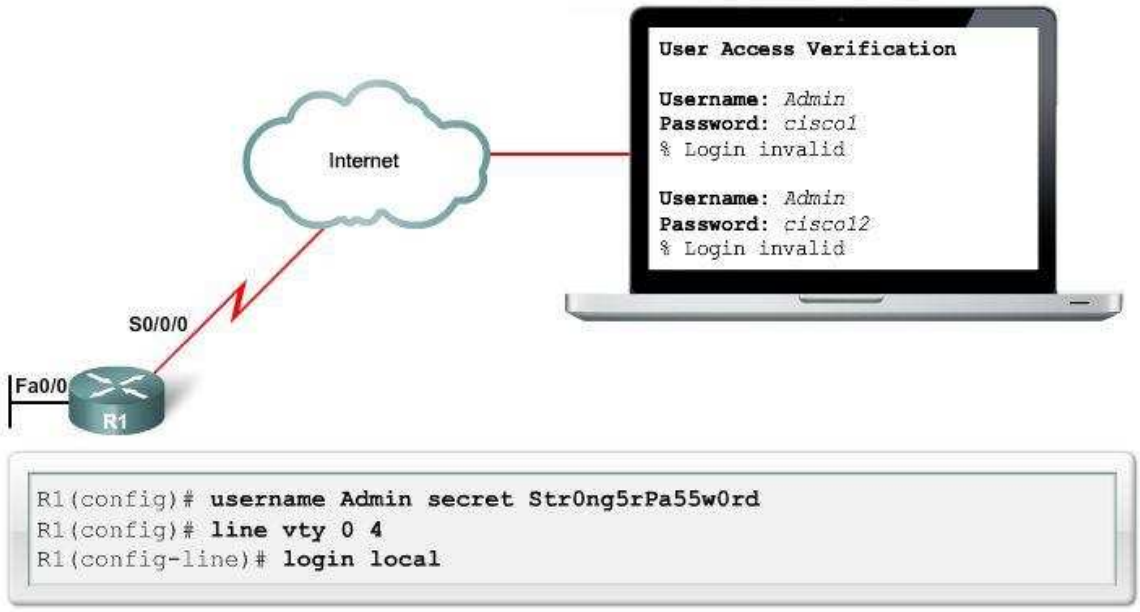
username username **secret** password

این دستور حساب کاربری را در دستگاه ایجاد می‌کند و یک رمز عبور مشخص برای هر کاربر ایجاد می‌کند. استفاده از دیتابیس محلی، امنیت بیشتری را فراهم می‌کند، زیرا مهاجم باید هم نام کاربری و هم رمز عبور را بداند. همچنین حسابداری بیشتری را در اختیار شما قرار می‌دهد زیرا نام کاربری در زمان ورود به سیستم ثبت می‌شود. در نظر داشته باشید که اگر دستور service password-encryption غیر فعال باشد، دستور password رمز عبور را به‌صورت متن ساده در فایل کانفیگ ذخیره می‌کند. استفاده از دستور secret به همراه نام کاربری روش بسیار بهتری است، زیرا از روش MD۵ برای ذخیرهٔ رمز عبور استفاده می‌کند.

روش دیتابیس محلی محدودیت‌هایی دارد. حساب‌های کاربری باید روی هر دستگاه تنظیم شوند. در محیط سازمانی بزرگ که دارای روترهای متعدد و سویچ‌ها برای مدیریت است، پیاده‌سازی و تغییر دیتابیس‌های محلی در هر دستگاه ممکن است، زمان‌گیر باشد. افزون‌براین، عیارسازی دیتابیس محلی هیچ روشی احراز هویت مجدد را فراهم نمی‌کند؛ به‌حیث مثال: اگر مدیر سیستم نام کاربری و رمز عبور آن دستگاه را فراموش کرد، هیچ راهی برای بازیابی نام کاربری و رمز عبور وجود ندارد. در این حالت بازیابی رمز عبور (password recovery) تنها گزینه است. راه‌حل بهتر این است که تمام دستگاه‌ها به یک دیتابیس از نام‌های کاربری و کلمهٔ عبور از یک سرور مرکزی مراجعه کنند.



شکل ۳-۱ ورود با فقط رمز عبور



شکل ۳-۲ استفاده از دیتابیس لوکل برای لاگین

۳.۲ احراز هویت در AAA

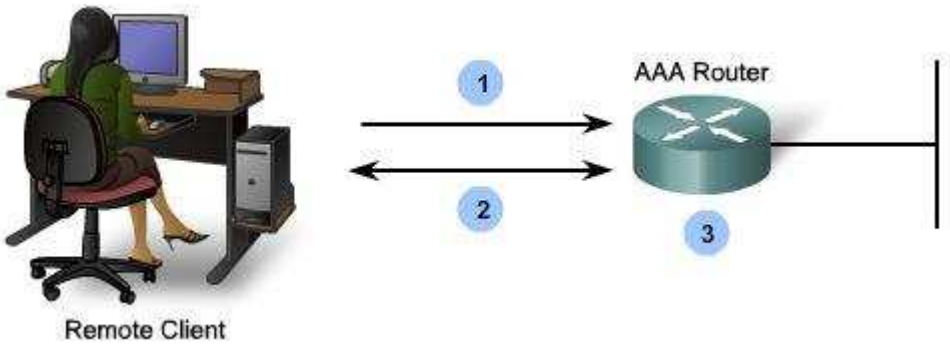
AAA می‌تواند برای تأیید هویت کاربران برای دسترسی مدیریتی یا برای احراز هویت کاربران برای دسترسی به شبکه از راه دور استفاده شود. این دو روش دسترسی برای درخواست خدمات AAA از حالت‌های مختلف استفاده می‌کنند:

۱. حالت کاراکتر: یک کاربر یک درخواست برای ایجاد یک پروسهٔ EXEC با روتر برای اهداف مدیریتی می‌فرستد.
۲. حالت پاکِت: کاربر یک درخواست برای ایجاد یک ارتباط از طریق روتر با یک دستگاه در شبکه ارسال می‌کند.

به جز دستورالعمل‌های حسابداری، تمام دستورات AAA به هر حالت کاراکتر و حالت پاکِت اعمال می‌شود. این موضوع روی امنیت دسترسی در حالت کاراکتر تمرکز دارد. برای یک شبکهٔ واقعاً امن، مهم است که روتر را برای دسترسی مدیریتی امن و دسترسی به شبکه از راه دور با استفاده از خدمات AAA نیز عیارسازی کنید. سیسکو دو روش معمول برای اجرای خدمات AAA را فراهم می‌کند.

۳.۲.۱ احراز هویت محلی AAA

AAA محلی از یک دیتابیس محلی برای احراز هویت استفاده می‌کند. این روش نام کاربری و کلمهٔ عبور را در روتر سیسکوی محلی ذخیره می‌کند و کاربران بر اساس دیتابیس محلی احراز هویت می‌شوند. این دیتابیس همان است که برای ایجاد CLI مبتنی بر نقش مورد نیاز است. AAA محلی برای شبکه‌های کوچک مناسب است.



شکل ۳-۳ استفاده از AAA لوکال

۳.۲.۲ احراز هویت مبتنی بر سرور AAA

روش مبتنی بر سرور از یک سرور دیتابیس خارجی استفاده می‌کند که پروتوکول RADIUS یا TACACS را پشتیبانی می‌کند؛ برای مثال: می‌توان از CISCO Secure ACS برای ویندوز سرور استفاده کرد. اگر روترهای متعدد وجود داشته باشند، AAA مبتنی بر سرور مناسب‌تر است.

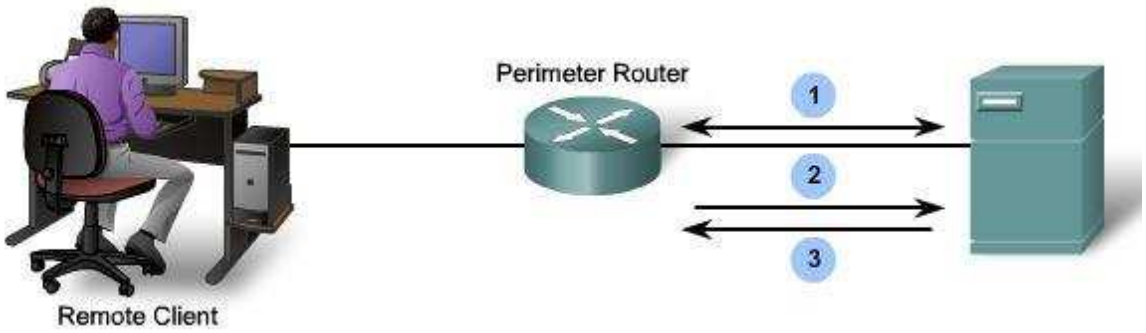
۳.۳ مجوز دسترسی در AAA

پس از آن‌که کاربران با موفقیت بر اساس AAA محلی یا مبتنی بر سرور احراز هویت می‌شوند، برای منابع شبکهٔ خاص مجاز می‌شوند. مجوز اساساً چیزی است که یک کاربر می‌تواند و نمی‌تواند در شبکه انجام دهد،

پس از آن کاربر تأیید هویت شده است، شبیه به این‌که چگونه سطح دسترسی و CLI مبتنی بر نقش به کاربران خاص حقوق و امتیازات خاصی را برای برخی از دستورات در روتر انجام می‌شود.

مجوز معمولاً با استفاده از یک راه‌حل مبتنی بر سرور AAA اجرا می‌شود. مجوز از مجموعه‌یی از ویژگی‌های ایجادشده استفاده می‌کند که کاربر دسترسی به شبکه را توصیف می‌کند. این صفات با معلومات موجود در دیتابیس AAA مقایسه می‌شوند و تعیین محدودیت‌هایی برای آن کاربر ساخته شده و به روتر محلی که کاربر متصل است، تحویل داده می‌شود.

مجوز به‌صورت خودکار است و نیازی به انجام مراحل اضافی بعد از احراز هویت نیست. مجوز بلافاصله بعد از تأیید هویت کاربر اجرا می‌شود.



شکل ۳-۴ مراحل مجوز دسترسی در AAA مبتنی بر سرور

۱. هنگامی که یک کاربر احراز هویت شد، یک session با سرور AAA برقرار می‌شود.
۲. روتر درخواست مجوز سرویس را از سرور AAA درخواست می‌کند.
۳. سرور AAA یک پاسخ PASS / FAIL برای مجوز دسترسی ارسال می‌کند.

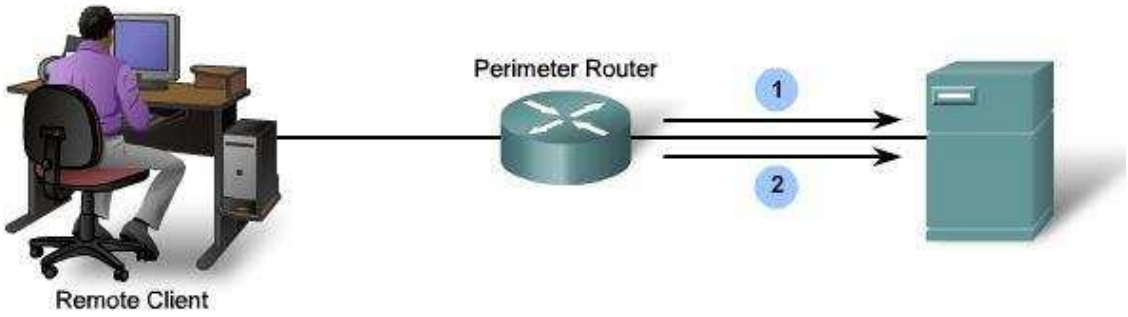
۳.۴ حسابداری در AAA

حسابداری جمع‌آوری و گزارش دیتای استفاده‌شده را جمع‌آوری و گزارش می‌کند؛ طوری‌که بتوان آن را برای اهدافی مانند تفتیش و صورت‌حساب مالی استفاده کرد. دیتای جمع‌آوری‌شده ممکن است، شامل زمان شروع و توقف اتصال، دستورات اجراشده، تعداد پاکِت‌ها و تعداد بایت‌ها باشد.

حسابداری با استفاده از یک راه‌حل مبتنی بر سرور AAA اجرا می‌شود. این سرویس گزارش آمار استفاده را به سرور ACS گزارش می‌دهد. این آمار را می‌توان برای ایجاد گزارش‌های دقیق دربارهٔ عیارسازی شبکه استفاده کرد.

یک استفادهٔ گسترده از حسابداری، ترکیب آن با احراز هویت AAA برای مدیریت دسترسی به ابزارهای شبکهٔ داخلی توسط کارکنان مدیریتی شبکه است. حسابداری امنیت بیشتری را نسبت به احراز هویت فراهم می‌کند. سرورهای AAA دقیقاً همان چیزی را که کاربر لاگین‌شده در دستگاه انجام می‌دهد، به‌صورت فایل

لاگ (Log File) ثبت می‌کند. این شامل تمام دستورات EXEC و عیارسازی توسط کاربر می‌شود. این لاگ حاوی فیلدهای دیتای متعدد، از جمله نام کاربری، تاریخ و زمان و دستور واقعی که توسط کاربر وارد شده است. این معلومات در هنگام عیب‌یابی دستگاه مفید است. این لاگ همچنین اهرم فشاری است در برابر افرادی که قصد اقدامات مخرب را دارند.



شکل ۳-۵ مراحل حسابداری در AAA مبتنی بر سرور

1. هنگامی‌که یک کاربر تأیید شده است، فرآیند حسابداری AAA یک پیام شروع برای شروع فرایند حسابداری تولید می‌کند.
2. وقتی کاربر خاتمه می‌یابد، پیام متوقف می‌شود و فرایند حسابداری به پایان می‌رسد.

۳.۵ چگونگی عیارسازی احراز هویت در AAA محلی

احراز هویت محلی AAA، که به‌حیث احراز هویت مستقل نیز یاد می‌شود، باید برای شبکه‌های کوچک عیارسازی شود. شبکه‌های کوچک شبکه‌هایی هستند که دارای یک یا دو روتر هستند که دسترسی به تعداد محدودی از کاربران را فراهم می‌کنند. این روش از نام کاربری و رمزهای ذخیره‌شده در روتر استفاده می‌کند. مدیر سیستم باید با مشخص‌کردن نام کاربری و پروفایل‌های رمز عبور برای هر کاربری که ممکن است، وارد سیستم شود، دیتابیس امنیتی محلی را ایجاد کند.

روش احراز هویت محلی AAA مشابه استفاده از دستور login local است ولی تنها یک فرق دارد. AAA یک راه برای عیارسازی روش پشتیبان احراز هویت استفاده می‌شود.

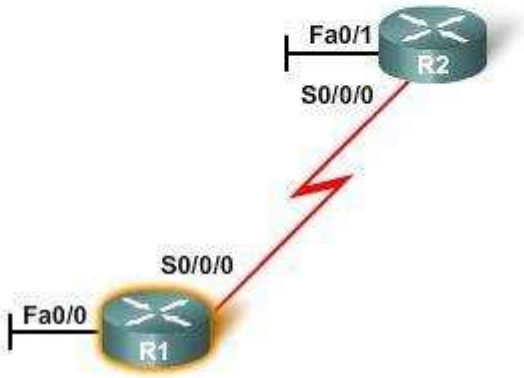
عیارسازی سرویس‌های محلی AAA برای احراز هویت سطح دسترسی مدیر (دسترسی به حالت کاراکتر) نیاز به چند مرحلهٔ اولیه دارد:

مرحلهٔ اول: اضافه‌کردن نام کاربری و رمز عبور به دیتابیس محلی روتر برای کاربرانی که نیاز به دسترسی مدیریتی به روتر دارند.

مرحلهٔ دوم: فعال‌کردن AAA بر روی روتر؛
مرحلهٔ سوم: تنظیم پارامترهای AAA در روتر؛

مرحلهٔ چهارم: تأیید و عیب‌یابی تنظیمات AAA.

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```



شکل ۳-۶ ایجاد احراز هویت با استفاده از AAA

برای فعال‌کردن AAA، از دستور aaa new-model استفاده کنید. برای غیر فعال‌کردن AAA، از دستور no قبل از دستور استفاده کنید.

پس از فعال‌شدن AAA، برای عیارسازی احراز هویت در پورت‌های vty، tty، پورت Aux یا پورت Console، یک لست از روش‌های احراز هویت تعریف کنید و سپس این لست را به انترفیس‌های مختلف اعمال کنید.

برای تعریف یک لست از روش‌های احراز هویت، از دستور aaa authentication login استفاده کنید. این دستور نیاز به نام لست و روش‌های احراز هویت دارد. نام لست، لست روش‌های احراز هویت فعال را زمانی‌که یک کاربر وارد سیستم می‌شود، مشخص می‌کند. لست روش، یک لست پیوندی است که روش‌های احراز هویت یک کاربر را مشخص می‌کند. لست روش‌ها، مدیر را قادر می‌سازد تا برای احراز هویت یک یا چند پروتوکول امنیتی را تعیین کند. استفاده از بیش از یک پروتوکول، یک سیستم پشتیبان برای احراز هویت در صورت عدم موفقیت روش اولیه در اختیار ما قرار می‌دهد.

برای نشان‌دادن روش می‌توان از چند کلمهٔ کلیدی استفاده کرد. برای فعال‌کردن احراز هویت محلی با استفاده از یک دیتابیس محلی ازپیش‌تعیین‌شده، از کلمهٔ کلیدی local یا local-case استفاده کنید. تفاوت بین این دو گزینه این است که local نام کاربری را صرف‌نظر از نوع حروف قبول می‌کند و local-case به حروف کوچک و بزرگ حساس است. برای مشخص‌کردن این‌که یک کاربر می‌تواند با استفاده از

enable password احراز هویت شود، از کلمهٔ کلیدی enable استفاده کنید. برای اطمینان از این‌که احراز هویت حتا اگر همه روش‌ها یک خطا را بر می‌گرداند، موفق شوند، کلمهٔ none را به‌حیث روش نهایی انتخاب کنید. برای اهداف امنیتی، تنها در هنگام آزمایش عیارسازی AAA از کلمهٔ کلیدی none استفاده کنید. از این کلمه هرگز نباید در یک شبکهٔ زنده استفاده کرد. به‌حیث مثال، درصورتی‌که نام کاربری و رمز عبور فراموش شود، روش enable می‌تواند به‌حیث یک میکانیزم احراز هویت مجدد استفاده شود.

aaa authentication login TELNET-ACCESS local enable

در این مثال، یک لست احراز هویت AAA به نام TELNET-ACCESS ایجاد شده است که در آن کاربران، ابتدا باید به دیتابیس محلی روتر لاگین کنند. اگر این تلاش یک خطا را بر می‌گرداند، مانند یک دیتابیس کاربر محلی عیارسازی نشده است، کاربر می‌تواند با دانستن رمز عبور enable، لاگین کند.

حد اقل یک روش و حد اکثر چهار روش را می‌توان برای یک لست روش‌های احراز هویت مشخص کرد. هنگامی‌که کاربر برای ورود به سیستم تلاش می‌کند، اولین روش ذکرشده، استفاده می‌شود. نرم‌افزار IOS سیسکو تنها زمانی از روش احراز هویت‌های بعدی استفاده می‌کند که هیچ پاسخی نیاید یا خطایی از روش قبلی رخ دهد. اگر روش احراز هویت اول سطح دسترسی کاربر را انکار کند، روند احراز هویت متوقف می‌شود و هیچ روش احراز هویت دیگر اجرا نخواهد شد.

لست تعریف شده از روش‌های احراز هویت باید روی انترفیس‌ها یا پورت‌های مشخص اعمال شود. برای انعطاف‌پذیری بیشتر، لست روش‌های مختلف می‌تواند به انترفیس‌ها و پورت‌های مختلف اعمال شود Y به‌حیث مثال: یک مدیر می‌تواند، یک لاگین خاص برای سرویس Telnet اعمال کند و سپس یک روش لاگین متفاوت برای پورت کنسول داشته باشد. برای فعال‌کردن یک نام لست خاص، از دستور aaa login authentication list-name در حالت عیارسازی انترفیس استفاده کنید.

این گزینه برای کانفیگ‌کردن یک نام لست پیش‌فرض نیز وجود دارد. هنگامی‌که AAA برای اولین بار فعال می‌شود، لست میتود پیش‌فرض به نام "default" به‌طور پیش‌فرض برای تمام انترفیس‌ها اعمال می‌شود، اما هیچ روشی برای احراز هویت ندارد. برای اختصاص چندین روش احراز هویت به لست پیش‌فرض، از دستور aaa authentication login default method1…[method2] استفاده می‌شود.

روش‌های احراز هویت در لست روش پیش‌فرض در تمام پورت‌ها استفاده می‌شود، مگر این‌که یک لست روش احراز هویت جداگانه برای آن ایجاد شده باشد. اگر یک انترفیس یا پورت، لستی از روش احراز هویت داشته باشد، این لست، لست پیش‌فرض برای این انترفیس را لغو می‌کند. اگر لست پیش‌فرض تنظیم نشده و لست دیگری نیز وجود نداشته باشد، تنها دیتابیس محلی بررسی می‌شود. این همان کاری است که دستور aaa authentication login default local انجام می‌دهد. در پورت کنسول، اگر لست پیش‌فرض تنظیم نشده باشد، کاربر بدون احراز هویت، موفق به لاگین می‌شود.

هنگامی‌که یک لست احراز هویت سفارشی برای یک انترفیس ایجاد می‌شود، می‌توان با استفاده از دستور no aaa authentication login *list-name* به لست پیش‌فرض بازگشت. اگر لست پیش‌فرض تعریف نشده باشد، احراز هویت AAA انجام نمی‌دهد.

با استفاده از دستور aaa local authentication attempts max-fail *number-of-unsuccessful-attempts* می‌توان امنیت بیشتری را روی پورت‌ها فراهم کرد. این فرمان، با قفل‌کردن حساب‌هایی که لاگین‌های ناموفق زیادی دارند، از حساب‌های کاربری AAA محافظت می‌کند. برای حذف دستور تعداد لاگین ناموفق، از دستور no در ابتدای دستور بالا استفاده کنید.

برای نمایش یک لست از تمام کاربران قفل‌شده، از دستور show aaa local user lockout در حالت privileged EXEC استفاده کنید. از دستور clear aaa local user lockout {username username | all} نیز برای قفل‌کردن حساب کاربر خاص یا تمام حساب‌های کاربری می‌توانید استفاده کنید.

دستور aaa local authentication attempts max-fail متفاوت از دستور login delay در نحوهٔ مدیریت‌کردن لاگین‌های ناموفق است. دستور aaa local authentication attempts max-fail درصورتی‌که احراز هویت ناموفق باشد، حساب کاربر را قفل می‌کند. این حساب تا زمانی‌که توسط یک مدیر آزاد نشود، قفل‌شده باقی می‌ماند. دستور login delay بین لاگین‌های ناموفق بدون قفل‌کردن حساب تأخیر ایجاد می‌کند.

هنگامی‌که یک کاربر وارد یک روتر سیسکو می‌شود و از AAA استفاده می‌کند، یک شناسهٔ منحصربه‌فرد برای session اختصاص داده می‌شود. در طول عمر جلسه، مشخصات مختلف مربوط به session در داخل دیتابیس AAA جمع‌آوری و ذخیره می‌شوند. این مشخصات می‌توانند شامل آدرس IP کاربر، پروتوکول استفاده‌شده برای دسترسی به روتر، مانند پروتوکول PPP یا Serial Line Internet Protocol (SLIP)، سرعت اتصال و تعداد پاکِت یا بایت‌های دریافت‌شده یا منتقل‌شده باشد.

برای نمایش مشخصاتی‌که برای یک AAA session جمع‌آوری شده، از دستور show aaa user *{all | unique id}* در حالت privileged EXEC استفاده کنید. دستور ID منحصربه‌فرد در حالت EXEC منحصربه‌فرد است. این دستور معلومات تمام کاربران لاگین‌شده را نشان نمی‌دهد، بلکه فقط کاربرانی را که با استفاده از AAA احراز هویت شده یا مجوز دسترسی گرفته‌اند یا session آن‌ها توسط ماژول AAA ذخیره شده است، نشان می‌دهد

دستور show aaa sessions می‌تواند برای نمایش شناسه منحصر به فرد یک session استفاده شود.

۳.۶ مشخصات AAA مبتنی بر سرور

پیاده‌سازی محلی AAA به‌خوبی مقیاس‌پذیر نیست. اکثر شرکت‌های بزرگ دارای تعداد زیاد روتر و تعداد زیادی مدیران روتر و صدها یا هزاران کاربر هستند که نیاز به دسترسی به شبکهٔ شرکت دارند. نگهداری یک دیتابیس محلی برای هر روتر سیسکو برای شبکه‌یی با این اندازه امکان‌پذیر نیست.

برای حل این چالش، یک یا چند سرور AAA مانند Cisco Secure ACS می‌تواند برای مدیریت نیازهای کاربر و دسترسی مدیریتی برای تمام شبکهٔ شرکت استفاده شود. Cisco Secure ACS می‌تواند یک دیتابیس مرکزی ایجاد کند که تمام دستگاه‌های موجود در شبکه بتوانند، به آن دسترسی پیدا کنند. همچنین می‌تواند با بسیاری از دیتابیس‌های خارجی، از جمله Active Directory و Lightweight Directory Access Protocol (LDAP) کار کند. این دیتابیس‌ها معلومات حساب کاربری و رمزهای عبور را ذخیره می‌کنند و اجازه می‌دهند تا حساب‌های کاربری توسط یک مدیریت مرکزی اداره شود.

خانوادهٔ محصولات CISCO Secure ACS از هر دو پروتوکول Terminal Access Control Access Control Server Plus (TACACS+) and Remote Authentication Dial-In User Services (RADIUS) پشتیبانی می‌کند که دو پروتوکولی هستند که غالباً توسط لوازم امنیتی سیسکو، روترها و سویچ‌ها برای اجرای AAA استفاده می‌شود.

درحالی‌که هر دو پروتوکول می‌تواند، برای برقراری ارتباط بین سرورهای AAA و مشتری مورد استفاده قرار گیرد، TACACS+ پروتوکول امن‌تری به نظر می‌رسد. به این دلیل که همه مبادلات پروتوکول TACACS+ رمزگذاری می‌شوند؛ RADIUS فقط رمز عبور کاربر را رمزگذاری می‌کند و نام‌های کاربری، معلومات حسابداری یا هرگونه معلومات دیگر که در پیام RADIUS حمل می‌شود، رمزگذاری نمی‌کند.

TACACS+ و RADIUS هر دو پروتوکول‌های احراز هویت هستند. هر یک از قابلیت‌ها و کارهای مختلف پشتیبانی می‌کند. این که آیا TACACS+ یا RADIUS انتخاب شود، بستگی به نیازهای سازمان دارد؛ به‌حیث مثال: یک ISP بزرگ ممکن است RADIUS را انتخاب کند، زیرا از حسابداری دقیق مورد نیاز برای صورت‌حساب‌دادن کاربران پشتیبانی می‌کند. یک سازمان با گروه‌های کاربری مختلف ممکن است TACACS+ را انتخاب کند، زیرا نیاز دارد تا پالیسی‌های مجوز را بر اساس یک کاربر یا بر اساس هر گروه ایجاد کند.

این نکته مهم است که تفاوت بین پروتوکول‌های TACACS+ و RADIUS را درک کنیم. نکات مهم در مورد TACACS+ عبارتند از:

- با نسخه‌های قبلی TACACS و XTACACS ناسازگار است.
- احراز هویت و مجوز دسترسی را از هم جدا می‌کند.
- همه ارتباطات را رمزگذاری می‌کند.
- از پورت TCP 49 استفاده می‌کند.

نکات مهم در مورد RADIUS عبارتند از:

۱. از سرورهای پروکسی RADIUS برای مقیاس‌پذیری استفاده می‌کند.
۲. احراز هویت و مجوز دسترسی را با هم‌ترکیب می‌کند و به‌حیث یک فرآیند استفاده می‌کند.
۳. فقط رمز عبور را رمزگذاری می‌کند.
۴. از UDP استفاده می‌کند.

از تکنالوژی‌های دسترسی از راه دور، 802.1X و SIP پشتیبانی می‌کند TACACS+یک نسخهٔ پیشرفتهٔ سیسکو برای پروتوکول TACACS اصلی است. با وجود نام آن، TACACS+یک پروتوکول کاملاً جدید است که با هیچ نسخهٔ قبلی TACACS سازگار نیست. TACACS+توسط خانوادهٔ سیسکو روترها و سرورهای دسترسی پشتیبانی می‌شود.

TACACS+سرویس‌های AAA به‌صورت جداگانه انجام می‌دهد. جداکردن سرویس‌های AAA، پیاده‌سازی را انعطاف‌پذیرمی سازد، زیرا امکان استفاده از TACACS+برای مجوز دسترسی و حسابداری و روش دیگری برای احراز هویت وجود دارد.

امکانات جدید پروتوکول TACACS+بیشتر از TACACS اصلی، درخواست‌های احراز هویت و کدهای پاسخ فراهم می‌کند. TACACS+ از پروتوکول‌های مختلف مانند IP و AppleTalk پشتیبانی می‌کند. عملیات TACACS+در حالت عادی، تمام پاکِت‌ها را برای ارتباطات امن‌تر رمزگذاری می‌کند و از پورت ۴۹ TCP استفاده می‌کند.

RADIUS، که توسط شرکت Livingston Enterprises توسعه یافته است، یک پروتوکول باز استندرد IETF برای AAA برای کاربردهایی مانند دسترسی به شبکه است. RADIUS در شرایط محلی و رومینگ کار می‌کند و معمولاً برای اهداف حسابداری مورد استفاده قرار می‌گیرد.

پروتوکول RADIUS در حین انتقال رمز های عبور را حتا با Password Authentication Protocol(PAP)، با استفاده از یک عملیات نسبتاً پیچیده که شامل Message Digest5 (MD5) و یک کلید مشترک مخفی دیگر است، مخفی می‌کند. با این حال، بقیه پاکِت‌ها به‌صورت متن ساده ارسال می‌شود.

RADIUS احراز هویت و مجوز دسترسی را به‌حیث یک فرآیند ترکیب می‌کند. هنگامی‌که یک کاربر احراز هویت می‌شود، آن کاربر مجاز نیز است. رادیوس با استفاده از پورت ۱۶۴۵ UDP یا ۱۸۱۲ برای احراز هویت و پورت ۱۶۴۶ UDP یا ۱۸۱۳ برای حسابداری استفاده می‌کند.

RADIUS به‌طور گسترده توسط ارائه‌دهندگان خدمات VoIP استفاده می‌شود. پروتوکول Diameter قرار است جایگزین RADIUS شود. Diameter با استفاده از یک پروتوکول انتقال حمل‌ونقل به نام Stream Control Transmission Protocol (SCTP) و TCP به جای UDP استفاده می‌کند.

۳.۷ تنظیم‌کردن پارامترهای پروتوکول‌های RADIUS و TACACS+

برای این‌که بتوانیم، از این پروتوکول‌ها برای AAA استفاده کنیم؛ نیاز است، ابتدا پارامترهای آنها در Cisco IOS Device تنظیم شود. برای این کار باید سرورهای مربوط به آنها را تعریف کنیم که از دستور زیر استفاده می‌کنیم.

```
Switch(config)# radius-server host 172.16.0.1 auth-port 1812 acct-port 1813 key Cisco
Switch(config)# tacacs-server host 172.16.0.2 port 49 key Cisco
```

در دستور اول ۱۸۱۲ پورت پیش‌فرض برای Authentication, Authorization و ۱۸۱۳ پورت پیش‌فرض برای Accounting در Server RADIUS می‌باشد.

در دستور دوم ۴۹ پورت پیش‌فرض برای هر سه نوع AAA در TACACS+ Server می‌باشد.

در هر دو دستور Cisco برای رمزنگاری بین سرورها و دستگاهی‌که AAA روی آن تنظیم می‌شود، به‌کار می‌رود.

۳.۸ تنظیم‌کردن AAA Authentication

Authentication AAA روشی است که امکان شناسایی هر کاربر را با استفاده از نام کاربری و پس‌ورد آن و پروتوکول امنیتی که برای آن تعریف‌شده است، برای دسترسی به شبکه فراهم می‌کند. فارمت کلی دستور AAA Authentication به‌صورت زیر می‌باشد:

```
aaa authentication {method-type} {default | list-name} method1 [method2…]
```

می‌توانیم برای AAA Authentication از نام برای لست روش آن استفاده کنیم و در انتهای آن لست روش را با آن نام بر روی انترفیس ویا لاین‌های مورد نظر اعمال کنیم درصورتی‌که برای تعریف لست روش از نام "Default" استفاده کنیم، این لست روش به‌صورت اتوماتیک بر روی تمام انترفیس‌هایی‌که لست روش برای آنها تعریف نشده است، اعمال می‌شود.

برای لست روش در AAA Authentication می‌توان از حالت‌های زیر استفاده کرد:

۱. Group: در این روش از سرورهای TACACS+ و RADIUS برای AAA استفاده می‌شود و نام کاربر و پس‌ورد آن کاربر در این سرورها تعریف می‌شوند. از این روش در AAA Authorization برای تعریف دسترسی‌های هر کاربر در سرورهای نام‌برده‌شده نیز استفاده می‌شود.
۲. Local: در این روش از دیتابیسی‌که در خود دستگاه تعریف‌شده است، استفاده می‌شود.
۳. Line: در این روش از پس‌وردی که برای لاین تعریف‌شده است، استفاده می‌شود.
۴. Enable: در این روش از پس‌وردی که برای Password Enable تعریف‌شده است، استفاده می‌شود.
۵. None: این روش AAA Authentication را غیر فعال می‌کند.

AAA Authentication Authentication انواع مختلفی دارد که در زیر به حالت‌هایی از آن اشاره می‌شود:

Enable: این حالت لست روش را برای Enable Password با استفاده از روش‌های تعریف‌شده برای آن تنظیم می‌کند. مثال:

```
Switch(config)# aaa authentication enable default group radius group TACACS+
enable
```

در این حالت ابتدا Enable Password وارد شده را در سرورهای RADIUS که اولین روش است جستجو می‌کند (در سرورهای RADIUS باید نام کابری "$enable15$"با پس‌ورد مورد نظر ما و در سرورهای TACACS+باید نام کابری، نامی‌باشد که کاربر با آن به دستگاه وارد شده، با پس‌ورد موردنظر ما تعریف شوند) درصورتی‌که پس‌ورد واردشده درست بود، اجازهٔ ورود به Global Configuration را به کاربر می‌دهد و درصورتی‌که اشتباه بود، این دسترسی از کاربر گرفته می‌شود. فقط درصورتی AAA Authentication از روش دوم که سرورهای TACACS+است، استفاده می‌کند که از طرف سرورهای RADIUS پاسخی دریافت نکند و همچنان اگر روش دوم بی‌پاسخ ماند، به سراغ روش‌های بعدی تعریف‌شده برای آن می‌رود.

Dot.۱x: این حالت لست روش را برای IEEE 802.1X با استفاده از روش‌های تعریف‌شده برای آن تنظیم می‌کند. مثال:

```
Switch(config)# aaa authentication login METHOD-LOGINgroup TACACS+ local
```

در این حالت برای لیست روش از نامی به غیر از Default استفاده شده است که در این صورت باید این لیست روش را بر روی انترفیس ویا لاین مورد نظر را با نام انتخاب‌شده فعال کنیم.

```
Switch(config)#interface line vty 0 15
Switch(config-line)#login authentication METHOD-LOGIN
```

حال AAA Authentication بر روی Vty Line فعال شده است و نام کاربری و پس‌ورد کاربر قبل از ورود به دستگاه توسط اولین روش که سرورهای TACACS+می‌باشند بررسی می‌شوند.

PPP: این حالت لست روش را برای سریال انترفیسی که از پروتوکول PPP استفاده می‌کند، تنظیم می‌کند. مثال:

```
Switch(config)#aaa authentication ppp radius-ppp if-needed group radius
Switch(config)#interface serial 0
Switch(config-serial)# encapsulation ppp
Switch(config-serial)#ppp authentication radius-ppp
```

۳.۹ تنظیم‌کردن AAA Authorization

AAA Authorization به ما اجازه می‌دهد که سرویس‌هایی را که هر کاربر امکان استفاده از آنها را دارد، محدود کنیم. برای این کار دستگاهی که AAA روی آن تنظیم می‌شود، معلومات هر کاربر را از پروفایل کاربر که در روی خود دستگاه ویا سرور AAA تعریف شده است دریافت می‌کند و سرویس‌هایی را که کاربر اجازهٔ دسترسی به آنها را دارد، به آن اختصاص می‌دهد.

فارمت کلی دستور AAA Authorization به‌صورت زیر می‌باشد:

```
aaa authorization {method-type} {default | list-name} method1 [method2...]
```

مانند AAA Authentication می‌توانیم، از نام برای لست روش آن استفاده کنیم و در انتهای آن لست روش را با آن نام بر روی انترفیس ویا لاین‌های موردنظر اعمال کنیم. درصورتی‌که برای تعریف لست روش از نام "Default" استفاده کنیم، این لست روش به‌صورت اتوماتیک بر روی تمام انترفیس‌هایی‌که لست روش برای آنها تعریف نشده است، اعمال می‌شود.

AAA Authorization Authorization انواع مختلفی دارد که در زیر به حالت‌هایی از آن اشاره می‌شود:

Auth-Proxy: این حالت لست روش را برای اختصاص‌دادن سیاست‌های امنیتی به کاربر تنظیم می‌کند.

Exec: این حالت لست روش را برای اختصاص‌دادن پارامترهای مربوط به Shell مانند سطح دسترسی (از ۱ تا ۱۵) که کاربر برای کار با دستگاه، به آن نیاز دارد، تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa authorization exec default group TACACS+ if-authenticated
```

در روش دوم که if-authenticated می‌باشد. درصورتی‌که کاربر فقط بتواند، با روش‌های AAA Authentication وارد دستگاه شود، تمام مجوزهای مربوط به Shell آن صادر می‌شود.

Config-Command: این حالت اجازهٔ دسترسی یا عدم دسترسی به دستورات مربوط به تنظیم‌کردن دستگاه‌ها با استفاده از حالتی‌که به دستورات مربوط به هر کاربر مجوز می‌دهد، را فعال می‌کند و با دستور زیر تنظیم می‌شود.

```
Switch(config)#aaa authorization config-commands
```

Configuration: این حالت امکان دانلودشدن دستورات هر دستگاه از سرور AAA را فراهم می‌کند؛ مثال:

```
Switch(config)#aaa authorization configuration default group TACACS+
```

Commands: این حالت لست روش را برای مجموعه دستوراتی که هر کاربر اجازهٔ استفاده از آن را در دستگاه دارد تنظیم می‌کند. این دستورات می‌توانند از سطح ۰ تا ۱۵ را شامل شوند؛ مثال:

```
Switch(config)#aaa authorization commands 1 COMMAND-LEVEL1 group TACACS+ none
Switch(config)#aaa authorization commands 15 COMMAND-LEVEL15 group TACACS+
Switch(config)#interface line vty 0 15
Switch(config-line)#authorization commands 1 COMMAND-LEVEL1
Switch(config-line)#authorization commands 15 COMMAND-LEVEL15
```

در این حالت AAA Authorization برای دستورات سطح ۱ و ۱۵ در دستگاه فعال شده است و حالا می‌توانیم، برای کاربران در سرورهای TACACS+ و برای این سطح دستورات مجوزهایی را که باید داشته باشند، تعریف کنیم (این حالت فقط برای سرورهای TACACS+ تنظیم می‌شود).

Network: این حالت لست روش را برای سرویس‌های ارتباطی شبکه مانند PPP و ARAP و SLIP تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa authorization network default group radius none
```

Console: این حالت AAA Authorization را برای لاین کنسول فعال می‌کند و با دستور زیر تنظیم می‌شود:

```
Switch(config)#aaa authorization console
```

۳.۱۰ تنظیم‌کردن AAA Accounting

AAA Accounting Accounting به ما امکان مشاهدهٔ سرویس‌هایی را که کاربران به آنها دسترسی پیدا کرده‌اند و مقدار منابعی از شبکه که مصرف کرده‌اند و همچنین دستوراتی که کاربر برای تنظیم‌کردن دستگاه‌های شبکه استفاده کرده است، می‌دهد.

فارمت کلی دستور AAA Accounting به‌صورت زیر می‌باشد:

```
aaa accounting {method-type} {default | list-name} method1 [method2...]
```

مانند AAA Authentication می‌توانیم، از نام برای لست روش آن استفاده کنیم و در انتهای آن لست روش را با آن نام بر روی انترفیس ویا لاین‌های مورد نظر اعمال کنیم. درصورتی‌که برای تعریف لست روش از نام "Default" استفاده کنیم، این لست روش به صورت اتوماتیک برای روی تمام انترفیس‌هایی‌که لست روش برای آنها تعریف نشده است، اعمال می‌شود.

AAA Accounting انواع مختلفی دارد که در زیر به حالت‌هایی از آن اشاره می‌شود:

Network: این حالت لست روش را برای گرفتن معلومات سرویس‌های ارتباطی شبکه مانند PPP و ARAP و SLIP و فرستادن آنها به سرور AAA تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa accounting network default start-stop group radius
```

برای دیدن زمان شروع و پایان استفاده از این سرویس‌ها از Start-stop استفاده می‌کنیم.

Exec: این حالت لست روش را برای گرفتن معلومات کاربرانی که به Shell دستگاه دسترسی پیدا کرده‌اند، مانند نام کاربری و مدت زمان اتصال و ... تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa accounting exec default start-stop group tacacs...
```

Commands: این حالت لست روش را برای فرستادن دستوراتی که کاربران در دستگاه‌ها استفاده می‌کنند، به سرور AAA تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa accounting commands 15 default start-stop group tacacs...
```

Connection: این حالت لست روش را برای گرفتن معلومات مربوط به تمام ارتباطات خروجی که از روی دستگاه ساخته می‌شود، مانند Telnet و rLogin تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa accounting connection default start-stop group radius
```

Dot.۱x: این حالت لست روش را برای گرفتن معلومات مربوط به Dot.۱x که کاربران با استفاده از آن به شبکه دسترسی پیدا می‌کنند، تنظیم می‌کند؛ مثال:

```
Switch(config)#aaa accounting dot1x default start-stop group tacacs...
```

AAA Session MIB

این ویژگی در AAA به ما اجازه می‌دهد که با استفاده از دستگاه‌های مانیتورینگ و SNMP کاربرهایی را که توانسته‌اند، به دستگاه‌ها دسترسی پیدا کنند، مانیتور کنیم. معلوماتی که با استفاده از این ویژگی به دستگاه مانیتورکننده فرستاده می‌شود، شامل نام کاربری و IP Address و مدت استفادهٔ کاربر از دستگاه و ... می‌باشد و با دستور زیر تنظیم می‌شود:

```
Switch(config)#aaa session-mib disconnect
```

خلاصهٔ فصل سوم

این فصل را با بحث در مورد مفهوم AAA و اهمیت آن در امنیت شبکه شروع کردیم. این مفاهیم که شامل Authentication، Authorization و Accounting است، به‌صورت مفصل در این فصل توضیح داده شد و انواع آن برای پیاده‌سازی در روترها معرفی شدند. Authentication یا احراز هویت به این معنا است که کسی که هویتی را ادعا می‌کند، آیا واقعاً خود همان شخص هست یا خیر. Authorization یا مجوز دسترسی به این معنا است که کسی که احراز هویت شده، آیا مجوز دسترسی به منبع خاصی را دارد یا خیر. Accounting به این معنا است که تمام کارهایی که توسط کاربر احراز هویت‌شده که مجوز دسترسی نیز دارد، باید ثبت شود. AAA معمولاً به دو صورت قابل استفاده است، یکی مبتنی به شبکه محلی و دیگری استفاده از یک دیتابیس خارجی. در مورد همه روش‌ها بحث شد و مورد بررسی قرار گرفتند.

سوالات و فعالیت های فصل سوم

۱. AAA چیست؟

۲. منظور از Authentication چیست؟

۳. منظور از Authorization چیست؟

۴. منظور از Accounting چیست؟

۵. AAA امنیت را برای کدام وجه یک شبکه تأمین می‌کند؟

۶. چه راهکارهای امنیتی دیگری غیر از AAA برای امن سازی شبکه وجود دارد؟

۷. تفاوت‌های RADIUS و TACACS در چیست؟

فعالیت ها

۱. با جستجو در انترنت سه فروشنده که یک RADIUS خوب را ارائه می‌کنند، پیدا کنید. مزایا و خصوصیات هر یک را بیان کنید.

۲. خلاصهٔ فصل را در دو تا سه پاراگراف بنویسید.

فصل چهارم

دیوار آتش (Firewall)

هدف کلی: محصلان با فایروال‌ها آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. فایروال‌ها (Firewalls) را تعریف کنند.
۲. نحوهٔ عملکرد فایروال‌ها (Firewalls) توضیح دهند.
۳. انواع فایروال‌ها (Firewalls) تشریح کنند.
۴. سیاست‌گذاری‌های فایروال‌ها (Firewalls) را بیان کنند.
۵. مفهوم و کاربرد DMZ را تشریح کنند.

دیوار آتش (Firewall) یک ابزار امنیتی است که در محل اتصال شما به انترنت قرار می‌گیرد و به‌عنوان یک عسکر وفادار متمرکز بر انترنت عمل می‌کند. دیوار آتش همه ترافیک ورودی و خروجی از اتصال شما را زیر نظر می‌گیرد، و طبق قوانین تنظیم‌شده می‌تواند ترافیک را قبول یا رد کند. در این فصل در مورد دیوار آتش (FireWall) و نقش آن در امنیت شبکه بحث خواهیم نمود. که دربرگیرنده موضوعات چون: چرا به دیوار آتش یا (Firewall) احتیاج داریم، دیوار آتش یا فایروال چطور باعث توسعهٔ یک سیاست امنیت می‌شود و درنهایت با نصب دیوار آتش یا Cisco Firwall آشنا می‌شویم.

۴.۱ دیوار آتش یا (Firewall)

انترنت برای سیاحت و گشت‌وگذار مکانی جالب و هیجان‌انگیز است. در عالم واقعی، شبکهٔ جهانی وب (World Wide Web) صرفاً مجموعه‌یی از روترها و سرورهایی است که بزرگ‌ترین شبکهٔ گسترده (WAN – Wide Area Network) در طول تاریخ را می‌سازند. این مجموعهٔ ابزارهای شبکه، سرویس ایمیل، سایت، و انبارهای دیگر معلومات را فراهم می‌کند؛ همهٔ آن‌ها به انترنت متصل هستند و در اختیار همه اشخاصی که به انترنت متصل‌اند، قرار دارند. حتا گفته شده است که انترنت حاوی دانش اجتماع انسانی است.

کل دانش جمع‌آوری‌شده توسط انسان در رسانه‌یی مقناطیسی ذخیره شده است تا مردم آنها را دریافت کرده، یاد بگیرند. همه کتاب‌ها در انترنت نوشته شده و زندگی ما را تحت تأثیر قرار می‌دهند. ما نگران امنیت یا شبکه هستیم، بنابراین باید متوجه باشیم که چه نوع حفاظتی لازم است تا از این حجم باورنکردنی معلومات محافظت کند.

در برخی سازمان‌ها این سیاست‌ها در مورد انترنت شبیه قوانین کشوری در مورد بزرگراه‌ها است؛ پس آیا نوعی پولیس کشوری تجسس می‌کند و همه ابزارهای متصل به انترنت را کنترول می‌نماید؟ پاسخ به این سؤال "نه" است؛ هیچ سازمان متحدی وجود ندارد که مسئول محافظت در انترنت باشد. وظیفهٔ حفاظت و نگهداری در پورت‌های متصل به انترنت، به عهدهٔ کاربران یا اشخاصی است که مسئول انتشار اولیهٔ معلومات هستند. هر وب‌سایت با یک شرکت اتصال انترنت یا شرکت سرویس‌دهندهٔ انترنت (ISP) در ارتباط است. وظیفهٔ شرکت این است که از خرابکاری هکرها در معلومات مهم سایت جلوگیری کند. اما چگونه یکی به‌تنهایی از وب‌سایت، سرور ایمیل (e-mail)، سرور FTP یا منابع دیگری معلومات که از طریق وب قابل دسترسی هستند، محافظت می‌کند؟ جواب فقط یک کلمه است: دیوار آتش (Firewall). تنها هدف این سخت‌افزار اختصاصی، تأمین امنیت در شبکهٔ شماست.

دیوار آتش (Firewall) یک ابزار امنیتی است که در محل اتصال شما به انترنت قرار می‌گیرد و به‌عنوان یک عسکر وفادار متمرکز بر انترنت عمل می‌کند. دیوار آتش همهٔ ترافیک ورودی و خروجی از اتصال شما را زیر نظر می‌گیرد، و طبق قوانین تنظیم‌شده می‌تواند ترافیک را قبول یا رد کند. دیوار آتش قانونی است و در دنیای بی‌قانون وب، یک محافظ است. او در مأموریت حفاظت از منابع شبکهٔ داخلی شما همیشه هوشیار است.

در طی سال‌ها، انترنت معلومات بسیار زیادی را برای کاربران شخصی جمع کرده است. دسترسی به این معلومات آن‌قدر گسترش یافته که به یک عنصر حیاتی برای اشخاص و مشاغل تبدیل‌شده است. با وجود این، قراردادن معلومات در انترنت ممکن است، باعث حمله به معلومات محرمانه و حساس از هر نقطهٔ جهان شود؛ طوری‌که می‌دانید، انترنت یک شبکهٔ جهانی است. به عبارت دیگر، وقتی من از طریق کیبل به انترنت متصل می‌شوم، ممکن است، از اروپا، آسیا و نقاط دیگر جهان مورد حمله قرار بگیرم. دیوار آتش می‌تواند، از کمپیوتر های شخصی و شبکه‌های شرکتی در مقابل نفوذ از طریق انترنت محافظت کند، اما شما باید نحوهٔ عملکرد آن را بدانید تا بتوانید درست از آن استفاده کنید.

این پولیس الکترونیکی ۲۴ ساعته و ۳۶۵ روز در سال، وظیفهٔ بسیار مهمی‌دارد؛ آدم‌های بد را بیرون نگه می‌دارد و به آدم‌های خوب اجازه می‌دهد تا برای انجام کار خود به منابع موردنیاز دسترسی پیدا کنند. این مسأله بر روی کاغذ، مثل قدم‌زدن در پارک ساده است؛ اما در عمل، تنظیم یک دیوار آتش شاید به همین سادگی نباشد.

در برخی موارد، تنظیم بد یا کافی‌نبودن خصوصیت‌های دیوار آتش می‌تواند، بدتر از حالت نبودن آن باشد. در این فصل، به تشریح وظایف دیوار آتش می‌پردازیم تا درک کنید که چگونه کار می‌کند و وظایف خود را چگونه انجام می‌دهد.

۴.۲ سؤالات متداول در مورد دیوار آتش (Firewall)

قبل از این‌که به بررسی عملکرد دیوار آتش بپردازیم، در بخش بعد، از چند سؤال بنیادی در رابطه با دیوار آتش بحث خواهیم کرد.

۴.۲.۱ چه کسی به دیوار آتش نیاز دارد؟

این شاید متداول‌ترین سؤالی باشد که در زمینهٔ امنیت پرسیده می‌شود. اگر قصد اتصال به انترنت را داشته باشید، به دیوار آتش نیاز دارید. فرق نمی‌کند که از خانه متصل می‌شوید ویا شرکت شما می‌خواهد، متصل شود؛ شما به یک دیوار آتش احتاج دارید. گسترش نفوذ سرویس‌های انترنت در خانه و اتصالات همیشه‌روشن (always-on) انترنت، امنیت خانگی را مهم‌تر نیز می‌سازد.

۴.۲.۲ چرا به دیوار آتش (Firewall) احتیاج داریم؟

تقریباً هر روز در مورد تهدیدهای امنیتی، در روزنامه‌ها یا شبکه‌های اجتماعی می‌خوانید ویا در اخبار می‌شنوید: ویروس‌ها، کرم‌ها، حمله‌های DoS، هک‌کردن‌ها، و نقاط ضعف جدید در کمپیوترها؛ مثلاً: SoBig، Blaster، LovSan، SQL Slammer، Code red، NIMDA و MyDoom که همه در اخبار ذکر شده‌اند، حتماً یکی از این نام‌ها را شنیده‌اید، مگر این‌که یک سال نه روزنامه خوانده باشید و نه تلویزیون تماشا کرده باشید ویا عضو هیچ شبکه اجتماعی نباشید.

هکرها آنجا هستند و برای هک‌کردن ما تلاش می‌کنند. غالباً نمی‌دانیم، چه کسانی هستند، اما می‌دانیم که کجا هستند و کجا نمی‌خواهیم باشند (در شبکهٔ ما). همانند دزدان دریایی که دریاها را جستجو می‌کنند، هکرها نیز پهنای انترنت را می‌گردند. شما نمی‌خواهید که آنها وارد شبکهٔ شما شوند و در میان کمپیوترهای متصل به آن به گشت و گذار بپردازند.

می‌دانید که باید از شبکهٔ خود در مقابل مهاجمان دفاع کنید، و یکی از مؤثرترین راه‌ها برای حفاظت از شبکه، نصب یک دیوار آتش است. به‌صورت پیش‌فرض، هر دیوار آتش خوب، از عبور ترافیک بین انترنت و شبکهٔ داخلی جلوگیری می‌کند. این بدان معنا نیست که دیوار آتش همهٔ ترافیک را متوقف می‌کند؛ این هدف اتصال به انترنت است. این بدان معنا است که دیوار آتش (Firewall) فقط به مرورگر وب (Browser) (HTTP پورت ۸۰) اجازهٔ دسترسی به انترنت می‌دهد. دیوار آتش بازرسی کامل پاکِت (SPI) را برای هر پاکِت (Packet) ورودی ممکن می‌سازد.

دلیل دیگر برای داشتن یک دیوار آتش، اجازهٔ همهٔ اتصالات به شبکهٔ شماست؛ نه اینکه نوعی بازرسی پاکِت انجام شود که تشخیص بدهد، آیا حمله‌یی پشت پاکِت‌های ورودی مخفی شده است یا نه. نداشتن یک دیوار آتش باعث می‌شود تا سازمان شما در مقابل حمله کاملاً بی دفاع باشد.

۴.۲.۳ آیا چیز ارزشمندی برای محافظت دارم؟

غالباً این جملات را از مردم می‌شنویم: "من می‌فهمم که اگر چیز ارزشمندی می‌داشتم، قطعاً به یک دیوار آتش نیاز می‌داشتم؛ من جیزی ندارم که یک مهاجم آن را بخواهد، پس چه نیازی به دیوار آتش دارم؟"

شبکه‌ها و منابع آن برای راهی که جامعهٔ ما، عملکرد و شغل را به هم متصل می‌کند، مهم هستند. به عبارت دیگر، این بدان معناست که شبکهٔ شما و عملکرد مؤثر آن، ارزشمند است. بنابراین شبکه‌ها نقش مهمی‌دارند و معنای آن این است که چیز مهمی‌دارید که باید از آن محافظت کنید، همان‌طورکه در زیر به برخی از آنها اشاره شده است:

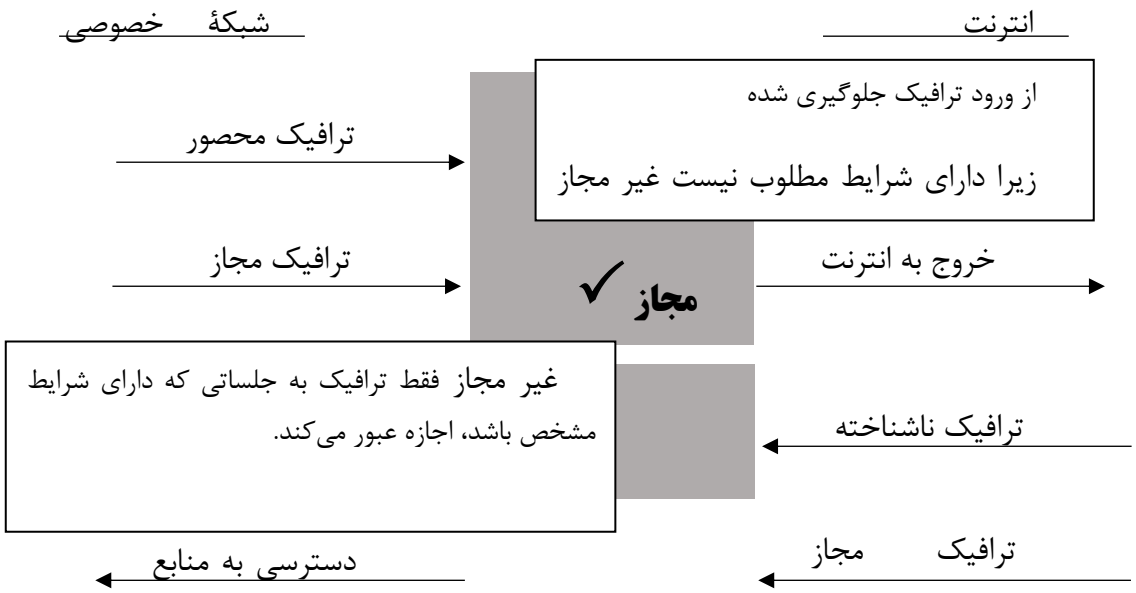
- **مسئولیت پایین‌دست (Downstream liability):** این شاید گام بزرگ بعدی در سیر تکاملی قانون انترنت باشد. شرایط این قانون مربوط به مواقعی است که یک مهاجم، کنترول یک هدف (کمپیوتر شما) را به دست گرفته و به‌وسیلهٔ آن، به شخصی دیگر حمله کرده است. تصور کنید که این کمپیوتر شرکت شما باشد که برای حمله از آن استفاده شده است. ناتوانی شرکت شما در دفاع از سیستم‌های خود، باعث خرابی در یک شبکهٔ دیگر شده است؛ مهاجم از کمپیوتر شما به‌حیث سلاحی در برابر شخص دیگر استفاده کرده است. بنابراین، شرکت شما مسئول خواهد بود، زیرا در وظیفهٔ محافظت از خود در برابر خطرات احتمالی، کوتاهی کرده است – مخصوصاً که دیوار آتشی هم نداشته باشد. تعهد انسان محتاط می‌گوید که باید مراقب باشد.

- **دیتای گم‌شده:** شاید در مورد شرکت‌هایی شنیده باشید که کل دیتای شغلی آنها در حملهٔ یازدهم سپتامبر از بین رفته است و بسیاری از آنها قابل بازگشت نبودند. تصور کنید چه اتفاقی می‌افتد اگر شرکت شما، این از دست‌دادن معلومات را تجربه کند؛ آن‌هم تنها به این دلیل که دیوار آتش نصب نکرده‌اید و یک مهاجم تمام معلومات شما را پاک کرده است؟ چه بلایی سر شغل شما می‌آید؟ آیا راهی برای بازگرداندن همه چیز وجود دارد؟ آیا کل فروش خود را از دست می‌دهید؟
- **افشای معلومات محرمانه:** هر سازمانی دارای معلوماتی است که محرمانه تلقی می‌شود و افشای آنها موجب بروز مسائل مالی، مشکلات قانونی، یا آبروریزی می‌شود. این مشکلات ممکن است ازدست‌رفتن معلومات مشتریان مثل شمارهٔ کارت اعتباری آنها یا طرح‌های محرمانه‌یی که در اختیار شرکت رقیب قرار می‌گیرند. این فهرست بی‌پایان است و هنگامی‌که هک می‌شوید، باید بدترین حالات را در نظر بگیرید. شاید به‌خاطر همین است که جرائم انترنتی منتشر نمی‌شود.
- **ازکارافتادن شبکه:** آیا تا به حال به یک دستگاه ATM یا یک خواروبارفروشی برای دریافت و پرداخت پول با استفاده از کارت اعتباری رفته‌اید؟ شبکه به این دستگاه‌ها امکان می‌دهد که همیشه به‌خوبی کار کنند؛ و درصورتی‌که خوب از آنها محافظت نشود، یک مهاجم می‌تواند باعث از کار افتادن آنها شود. در صورتی‌که این دستگاه‌ها از کار بیفتند، ضرر ناشی از قابل استفاده نبودن آنها بیشتر است.

درنهایت، همهٔ افراد چیز مهمی‌برای حفاظت دارند، و عدم انجام این محافظت برایشان گران تمام می‌شود؛ زمان مهم است، زیرا باید قبل از این‌که اتفاقی بیفتد، دست‌به‌کار شویم. سؤال بعدی این است که "یک دیوار آتش برای محافظت از شبکه چه اقداماتی انجام می‌دهد؟"

۴.۲.۴ یک دیوار آتش چگونه عمل می‌کند؟

با ورود ترافیک به یکی از رابطه‌های دیوار آتش، دیوار آتش آن را بازرسی کرده و قوانین مربوط به ترافیک را بر آن اعمال می‌کند. در واقع، بر اساس قوانین، ترافیک شبکه عمل می‌کند ویا اجازهٔ عبور به آنها می‌دهد. همان‌طور که در شکل ۴ – ۱ مشاهده می‌کنید، یک دیوار آتش، ترافیک ورودی و خروجی را فلتر می‌کند.



شکل ۴-۱ عملکرد دیوار آتش

دیوار آتش مانند ACL (Access Control List)، می‌تواند ترافیک را بر اساس آدرس IP مبدأ و مقصد، پروتوکول، وضعیت اتصال، فلتر کند. به عبارت دیگر، کاربری در شبکهٔ شما یک جلسهٔ FTP را شروع می‌کند. به او اجازهٔ این کار داده می‌شود، زیرا جلسه از داخل شبکه برقرار شده است. به‌طور پیش‌فرض، دیوار آتش همهٔ اتصالات از داخل شبکه به انترنت (خارج) را، مجاز می‌داند.

یک دیوار آتش همچنان می‌تواند درخواست‌های اتصال را با قوانین مخصوص ثبت کند و در صورت لزوم اعلان خطر کند. همچنین، دیوار آتش به شما امکان اجرای ترجمهٔ آدرس شبکه (Network Address Translation – NAT) را از آدرس IP خصوصی به آدرس IP عمومی می‌دهد.

۴.۳ دیوارهای آتش "سیاست‌گذاری امنیت" هستند

چه نوع ترافیکی اجازهٔ عبور به داخل و خارج شبکهٔ شما را دارد؟ چگونه از شبکهٔ خود در مقابل تهاجم دفاع می‌کنید؟ سیاست امنیتی شما چیست؟ چه اتفاقی برای افرادی می‌افتد که سیاست امنیتی را رعایت نمی‌کنند؟ چه کسی مسئول نوشتن و به‌روزکردن سیاست امنیتی است؟

همهٔ این سؤالات مهم هستند و سزاوار پاسخ، داشتن یک شبکه که از طریق دیوار آتش به انترنت متصل است، اولین گام در امنیت است. به دلیل این‌که این کتاب اولین گام‌ها را بیان می‌کند، اینجا جای خوبی برای شروع است، حالا باید بدانید که سیاست‌های امنیتی در اصل چگونه پیاده‌سازی می‌شوند.

آیا این جملهٔ قدیمی را به‌خاطر می‌آوردید "هیچ کاری تمام نمی‌شود مگر این‌که مراحل کاغذبازی طی شده باشد"؟ خوب، هیچ راه امنیتی به پایان نمی‌رسد مگر این‌که گزارش کاملی از قوانین و مقرراتی را که بر امنیت سازمان شما حاکمند، بنویسید. این نسخهٔ نوشتاری از قوانین و مقررات امنیت شما، سیاست امنیتی

نامیده می‌شود. این اسناد "سیاست" در نوع و زاویهٔ دید بسیار متفاوت از یک طرح امنیت هستند، بنابراین اطمینان حاصل کنید که می‌دانید، چه چیزی یک سیاست را از اسناد امنیتی دیگر یک سازمان متفاوت می‌سازد و چه چیزی یک سیاست امنیتی را از طرح‌های امنیتی مجزا می‌سازد؟

مجازات! این درست است، یک سیاست امنیتی مشخص می‌کند که چه چیز مجاز است و تعیین می‌کند که اگر از قوانین سرپیچی کنید، چه مجازاتی در انتظار شما است. اگر از قوانین پیروی نکنید، ممکن است:

۱. اخراج یا معزول شوید.
۲. تنزیل رتبه داده شوید.
۳. تنزیل رتبه داده شده، جریمه شوید.
۴. اخراج، معزول و جریمه شوید.
۵. تنزیل درجه، معزول و جریمه شوید.
۶. همه موارد بالا.

سیاست امنیتی با بیانی واضح و روشن دقیقاً مشخص می‌کند که قانون چیست، چه کسی آن را اجرا می‌کند، و چه اتفاقی می‌افتد، اگر شما آن را نقض کنید. همهٔ این‌ها در مورد پیامدهای عملکرد کاربران است.

چطور یک دیوار آتش می‌تواند سیاست امنیتی باشد؟ یک دیوار آتش با دنبال‌کردن قوانین تنظیم‌شده توسط مهندس شبکهٔا کارمند امنیت معلومات (Information Security Officer – IOS)، وظایف خود را انجام می‌دهد. این قوانین باید به‌خوبی براساس نسخهٔ نوشتاری در اسناد سیاست امنیتی که پیش خود دارید ویا در جعبهٔ دسک فلاپی ۵ اینچی در پشت اتاق سرور، ویا در محلی در دفتر مدیریت که می‌توانید آن را پیدا کنید، تنظیم شوند. این اسناد حاوی معلومات و فهرست قوانین شبکه است. نکتهٔ جالب اینجاست که همهٔ قوانین در اسناد سیاست باید در دیوار آتش تنظیم شوند.

قوانین تنظیم‌شده در دیوار آتش باید با سرتیترهای قوانینی که در سیاست امنیتی سازمان قید شده‌اند، به‌خوبی سازگاری داشته باشند. اگر شما فایل تنظیم دیوار آتش را بررسی کنید، باید چیزی شبیه مثال ۱ – ۵ ببینید که عکسی از تنظیمات یک دیوار آتش Cisco Pix است.

نمونهٔ قوانین دیوار آتش PIX

```
Conduit permit tcp host 216.186.xx.xxx eq smtp any
Conduit permit tcp host 216.186.xx.xxx eq www any
Conduit permit tcp host 216.186.xx.xxx eq pop3 any
Conduit permit tcp host 216.186.xx.xxx eq ftp any
```

عبارات Conduit permit که در مثال ۱ – ۵ می‌بینید، بسیار شبیه برخی عبارات سیاست امنیتی است که مشخص می‌کند، کدام سرویس‌ها به چه نامی‌مجازند، وارد کدام پروتوکول‌های شبکه و مقصدها شوند و چه سرویس‌های مجازند که خارج شوند. این عبارات، طرح امنیتی شبکهٔ شما هستند و سیاست امنیتی آنها را تعریف می‌کنند. امروزه به‌منظور استندردسازی خط تولید سیسکو، Conduitها کم‌کم جای خود را به فهرست کنترول دسترسی (Access control list) داده‌اند.

به‌منظور تشریح بیشتر سیاست دیوار آتش، چند نکتهٔ سیاست امنیتی و چگونگی تنظیم دیوار آتش با آنها را مطرح می‌کنیم:

۱. یک سیاست امنیتی مواردی را که باید در مواجهه با پیشامدها انجام دهیم، بیان می‌کند.
۲. یک سیاست امنیتی دائماً در حال رشد و تغییر است تا نیازهای جدید امنیت برآورده شوند.
۳. یک سیاست امنیتی پارامترهای استفادهٔ قابل قبول و غیر قابل قبول را تعیین می‌کند.

اگر مقایسهٔ نکته‌به‌نکته بین یک سیاست امنیتی با تنظیمات یک دیوار آتش انجام دهید، جدولی مطابق جدول ۴-۱ خواهید دید.

جدول ۴-۱ مقایسهٔ سیاست امنیتی با تنظیمات دیوار آتش

	سیاست امنیتی	تنظیمات دیوار آتش
توانایی پاسخ به پیشامدها	بله	**بله**
رشد و تغیر دایمی	بله	**بله**
تعیین رفتار	بله	**بله**

هدف از این بخش، این نیست که شما را متقاعد سازیم که یک دیوار آتش جایگزینی برای سیاست امنیتی است؛ بلکه هدف این است که شما به امنیت مثل یک فلسفهٔ دربرگیرندهٔ طرح‌ها، سیاست‌ها، و ابزارهای امنیتی فکر کنید. باید بر روی کل سیاست امنیتی تفکر کنید، نه این‌که فقط قسمت‌هایی از آن را برای حفاظت از

شبکهٔ خود به‌کار ببرید. هنگامی‌که آمادهٔ تنظیم دیوار آتش (Firewall) خود هستید و آماده‌اید، قوانینی تنظیم کنید که ترافیک را رد یا قبول کند، باید از سیاست امنیتی به‌حیث نقطهٔ شروع استفاده کنید. دیوار آتش ظهور فزیکی و منطقی سیاست امنیتی شماست.

۴.۴ خلاصهٔ عملکرد دیوار آتش

هر سفر طولانی تنها با یک قدم اول شروع می‌شود. قبل از این‌که در نقاط دیگر امنیت خیلی عمیق شوید، لازم است، بدانید که دیوار آتش چگونه جادوی خود را به انجام می‌رساند.

اکثر دیوارهای آتش (اکثر و نه همه) بر روی SPI (Stateful packet Inspection) تکیه دارند، تا همه بتسه‌های خروجی و واکنش‌ها نسبت به این پاکِت‌ها را ردیابی کنند. ردیابی میزبان‌ها (Host) در شبکه‌یی که پاکِت‌های خروجی را می‌سازند، باعث جلوگیری از ورود پاکِت‌های WAN ناخواسته می‌شود.

به عبارات دیگر، یک دیوار آتش که از SPI استفاده می‌کند، همان‌طورکه در فصل ۳ " بررسی تکنولوژی‌های امنیت" مطرح شد، همه ترافیک خروجی از یک میزان داخلی را بازرسی می‌کند. مکالمه از یک میزبان به خارج را ردیابی می‌کند، و اطمینان حاصل می‌کند که پاسخ داخلی به درخواست، به همان میزبانی برمی‌گردد که همهٔ این‌ها از اول از آنجا شروع شده است.

دو هدف بازرسی بسته (Packet) و فلترکردن پاکِت‌ها، از مسئولیت‌های اصلی یک دیوار آتش هستند، فهرست زیر، رایج‌ترین وظایف و مشخصات دیوار آتش است:

- **سدکردن‌ترافیک ورودی بر اساس آدرس منبع یا مقصد آن:** مسدودکردن ترافیک ناخواستهٔ ورودی، رایج‌ترین مشخصهٔ یک دیوار آتش و دلیل اصلی وجود یک دیوار آتش است: متوقف‌ساختن ترافیک ناخواسته از ورود به شبکهٔ شما. این ترافکیک ناخواسته غالباً از جانب مهاجمان است؛ بنابراین باید مسدود شود.
- **سدکردن‌ترافیک خروجی بر اساس آدرس منبع یا مقصد آن:** بسیاری از دیوارهای آتش می‌توانند ترافیک خروجی از شبکهٔ شما به انترنت را نیز بازرسی کنند. مثلاً شاید بخواهید، از دسترسی کارمندان به سایت‌های نامناسب جلوگیری کنید.
- **سدکردن‌ترافیک بر اساس محتوا:** اکثر دیوارهای آتش پیشرفته می‌توانند، ترافیک شبکه را برای جلوگیری از محتوای غیر قابل پذیرش، بازرسی کنند. مثلاً یک دیوار آتش با یک آنتی‌ویروس یکپارچه شده، می‌تواند، از ورود فایل‌های حاوی ویروس به شبکه جلوگیری کند. دیوارهای آتش دیگری نیز با سرویس‌های ایمیل (e-mail) یکپارچه شده‌اند تا از ورود نامه‌های الکترونیکی غیر قابل پذیرش جلوگیری کنند.
- **دسترسی به منابع داخلی را مقدور می‌سازد:** اگرچه هدف اصلی یک دیوار آتش، جلوگیری از ورود ترافیک ناخواسته است. اما می‌توانید آن را طوری تنظیم کنید که اجازهٔ دسترسی به منابع مشخصی–

همانند یک سرور وب عمومی– را نیز بدهد؛ درحالی‌که از دسترسی به منابع دیگر شبکه از طریق انترنت جلوگیری کند. در بسیاری از موارد، این کار با استفاده از DMZ انجام می‌شود، که در جایی قرار دارد که سرور وب عمومی باید قرار داشته باشد. (در مورد DMZها، در بخش "ملزومات اولیه: زندگی در DMZ" بحث خواهیم کرد.)

- **اجازهٔ اتصالات به شبکهٔ داخلی:** یک راه معمول که کارمندان از طریق آن به یک شبکه متصل می‌شوند، استفاده از VPNها اتصال امن از انترنت به یک شبکهٔ شرکتی را ممکن می‌سازند؛ مثلاً: ارتباطات راه دور و فروشندگان سیار می‌توانند، از طریق VPN به شبکهٔ شرکت خود متصل شوند. برخی از دیوارهای آتشی دارای VPN هستند و چنین اتصالاتی را ساده می‌کنند.
- **گزارش در موردترافیک شبکه و فعالیت‌های دیوار آتش:** در هنگام بازرسی‌ترافیک ورودی و خروجی شبکه به انترنت، این مهم است که بدانیم، دیوار آتش چه می‌کند، چه کسی قصد نفوذ به شبکه را دارد، و چه کسی قصد دسترسی به مطالب غیر مجاز بر روی انترنت را دارد. اکثر دیوارهای آتش دارای یک میکانیزم گزارش‌دهی هستند. یک دیوار آتش خوب می‌تواند، فعالیت‌های syslog یا انواع دیگر آرشیو را نیز ثبت کند. بعد از وقوع یک حمله، بررسی مطالبی که دیوار آتش ثبت می‌کند. یکی از ابزارهای قانونی است که شما در اختیار خواهید داشت.

۴.۵ دیوار آتش در عمل

باید خاطرنشان کنیم که بسیاری از دیوارهای آتش تنها دو انترفیس (Interface) فزیکی دارند، و ۹۹ درصد آنها بر مبنای انترنت است. این انترفیس‌های داخلی (محافظت‌شده) و خارجی (محافظت‌نشده) نامیده می‌شوند و در رابطه با شبکهٔ شما ساخته شده‌اند. بنابراین، در عمل، انترفیس خارجی به انترنت و انترفیس داخلی به شبکهٔ داخلی شما متصل است.

۱. میزبان A یک Apple PowerBook G4 است و یک جستجوگر وب را باز کرده، قصد دارد یک صفحهٔ وب را در سرور www.avoidwork.com ببینید. میزبان A در خواست مربوطه را از طریق دیوار آتش ارسال می‌کند.
۲. دیوار آتش در خواستی را که مبدأ آن میزبان A است و مقصد آن www.avoidwork.com می‌بینید.
۳. دیوار آتش متوجه درخواست خارجی شده و انتظار دارد که پاسخ فقط از سرور وب www.avoidwork.com بیاید.
۴. یک ثبت‌کنندهٔ جلسه در جدول وضعیت جلسات دیوار آتش قرار دارد که مراحل ارتباط را از آغاز تا پایان دنبال می‌کند.
۵. معیارهای اتصال نیز در ثبت‌کنندهٔ جلسه قرار دارد که توسط دیوار آتش برای این اتصال نگهداری می‌شود.

۶. پاسخ به صفحهٔ وب درخواست‌شده توسط میزبان A، توسط سرور وب www.avoidwork.com به میزبان A از طریق دیوار آتش ارسال می‌شود.
۷. دیوار آتش جدول وضعیت جلسهٔ خود را کنترول می‌کند تا ببیند که آیا معیارهای این جلسه با اتصال خارجی همخوانی دارد یا نه. درصورتی‌که همه جزئیات اتصال همخوانی داشته باشند. دیوار آتش به‌ترافیک اجازه خواهد داد.

مسألهٔ آخر در مورد دیوار آتش کامل را در نظر بگیرید. اگر یک دیوار آتش، سابقهٔ وضعیت اتصال را در مورد اتصالات خارجی و داخلی ذخیره کند، احتمال این‌که یک هکر بتواند یک بستهٔ جعلی برای نفوذ به شبکهٔ شما ارسال کند، بسیار کم خواهد شد. هنگامی‌که مهاجمان برای نفوذ به دیوار آتش، سعی در ارسال پاکِت‌هایی می‌کنند، معلومات وضعیت اتصال نادرست یا مفقود، باعث می‌شود که آن جلسه خاتمه داده شود.

بسیاری از دیوارهای آتش برای بررسی این‌که آیا پاکِت‌ها معتبر هستند یا نه، آدرس IP منبع آنها را بررسی می‌کنند. یک مهاجم ممکن است یک حملهٔ IP Spoofing انجام دهد تا با سوءِ استفاده از آدرس‌های IP منبع پاکِت‌هایی که به دیوار آتش ارسال می‌شوند، راه نفوذی برای خود باز کند. اگر دیوار آتش فکر کند که این پاکِت‌ها از جانب منبع معتمدی آر سال شده‌اند، به این دلیل که دارای آدرس IP منبع درست هستند، ممکن است، به آنها اجازهٔ ورود دهد؛ مگر این‌که معیارهای دیگری نقض شود. این یک اصل است که یک تکنالوژی به‌تنهایی نمی‌تواند همه مشکلات امنیتی را حل کند. به علاوه، نیاز است که مدیریت شرکت و سیاست امنیتی را نیز دخیل کنید. دیوارهای آتش سیسکو از ASA (Adaptive Security Alogorithm) به‌عنوان روشی برای افزایش یک شماره به هر جلسهٔ انتقال‌داده‌شده، استفاده می‌کند تا از سوء استفادهٔ احتمالی هکرها از یک جلسه جلوگیری کنند.

۴.۶ نصب یک دیوار آتش

امروزه انتخاب یک دیوار آتش بیار سخت شده است. آن‌ها در انواع طرح‌ها، و مشخصات وجود دارند. من در هنگام طراحی‌ترکیب دیوار آتش برای یک مشتری، اولین چیزی را که می‌خواهم، بدانم، این است که مسئولیت‌های دیوار آتش چه خواهد بود؟

نوع دیوار آتشی که نصب می‌کنید، به نیازمندی‌های حفاظت و مدیریت، مثل اندازهٔ شبکه، و منابعی که قرار است، از آنها محافظت شود، بستگی دارد. دیوارهای آتش معمولاً به‌صورت زیر طبقه‌بندی می‌شوند:

۱. **دیوار آتش شخصی:** یک دیوار آتش شخصی معمولاً قسمتی از یک نرم‌افزار است که در یک کمپیوتر (PC) شخصی نصب می‌شود تا از آن محافظت کند. این نوع دیوارهای آتش معمولاً در کمپیوترهای خانگی با اتصالات باند پهن (broadband) ویا کمندان راه دور نصب می‌شوند. قطعاً هر زمانی‌که شخصی بخواهد یک دیوار آتش نصب کند، ایدهٔ خوبی خواهد بود. سازندگان سیستم‌عامل‌هایی مثل Apple و

Microsoft، با جمع‌آوری دیوارهای آتش شخصی در خود به این نیاز پاسخ داده‌اند. Apple OS X و Windows XP دارای یک دیوار آتش IP هستند.

۲. **دیوار آتش همه‌منظوره (all-in one)**: این نوع دیوار آتش توسط گروه وسیعی از مشترکان باند پهن (کیبل یا DSL) استفاده می‌شود و دارای مزایای یک ابزار است که مشخصات و عملکردهای زیر را دارا می‌باشد: روتر، سویچ اترنت، دسترسی بی‌سیم (Wireless)، و دیوار آتش.

۳. **دیوار آتش دفتری کوچک-تا-متوسط (Small-to-medium)**: این دیوارهای آتش، مثل cisco PIX 501 یا 506، برای حفاظت از دفاتر کاری کوچک طراحی شده‌اند.

۴. **دیوارهای آتش تجاری (enterprise)**: این دیوارهای آتش، مثل cisco PIX 515، برای سازمان‌های بزرگ با هزاران کاربر طراحی شده‌اند؛ درنتیجه، دارای قابلیت‌ها و توانایی اضافه مثل حافظهٔ بیشتر و رابطه‌های بسیار زیاد هستند. همه دیوارهای آتش سیسکو یک نسخهٔ سیستم‌عامل را اجرا می‌کنند که دارای گزارش‌دهی و قابلیت مدیریتی یکسان است. درصورت نیاز به تعداد اتصالات و قابلیت‌های بیشتر، مُدل‌های بزرگتر نصب می‌شود.

معمولاً یک دیوار آتش جایی نصب می‌شود که شبکهٔ شما به انترنت متصل می‌شود. اگر چه سازمان‌های بزرگتر برای ایجاد امنیت بیشتر، دیوارهای آتش بین بخش‌های مختلف شبکهٔ داخلی نیز نصب می‌کنند؛ اما اکثر دیوارهای آتش برای بازرسی‌ترافیک بین شبکهٔ داخلی و انترنت نصب می‌شوند. مثلاً اگر یک سازمان بزرگ به شرکای کاری اجازهٔ اتصال مستقیم به شبکه را بدهد، معمولاً می‌توان یک دیوار آتش پیدا کرد که مشخص می‌کند، شرکا چه کارهایی می‌توانند، در داخل شبکه انجام دهند. این قراردادن یک دیوار آتش داخلی قطعاً تکنیک خوبی به‌حساب می‌آید.

مهم نیست چه نوع دیوار آتشی به‌کار می‌برید، شما باید فلترهایی را برای پیاده‌سازی سیاست‌های امنیتی تعریف کنید.

۴.۷ تعیین سیاست دسترسی به داخل

با عبورترافیک از یک دیوار آتش، این‌ترافیک با قوانینی تعریف‌شده در دیوار آتش (Firewall) سنجیده می‌شود. برای این‌که ۹۹ درصد شبکه‌ها از آدرس IP خصوصی در داخل شبکه استفاده می‌کنند. می‌توانید، انتظار داشته باشید که تقریباً همه دیوارهای آتش (Network Address Translation) NAT استفاده می‌کنند.

پاکت‌هایی که بنا به درخواست صادرشده از کمپیوترهای شخصی (کاربران) از انترنت وارد می‌شوند، آدرسشان، رابط خارجی دیوار آتش است. دیوار آتش از NAT استفاده کرده و وضعیت درخواست‌های کاربر داخلی را بررسی می‌کند. دیوار آتش با استفاده از NAT، به صورت داینمیک شمارهٔ پورت‌ها را در اختیار انترفیس خارجی قرار می‌دهد. بدین‌ترتیب به چندین کاربر اجازهٔ استفاده از یک آدرس IP داده می‌شود و درخواست‌های آنها با کمک NAT به انترنت می‌رود. استفاده از یک آدرس IP و شمارهٔ پورت‌های (ports)

مختلف برای‌ترجمهٔ آدرس پورت (Port Address Translation PAT) نامیده می‌شوند. همچنین این تغییرات در گاه، تصمیم‌گیری در مورد انتخاب پورت را برای یک مهاجم مشکل می‌سازد.

اگر همه ترافیک LAN شما مقصدش انترنت باشد، سیاست دسترسی ساده‌یی به داخل طراحی خواهد داشت. دیوار آتش فقط به ترافیکی اجازهٔ ورود می‌دهد که پاسخ به درخواستی از میزبان‌های LAN داخلی باشند. همان‌طورکه قبلاً مطرح شد، دیوار آتش همه درخواست‌های خارجی را در جدول وضعیت دنبال می‌کند.

هرچند، در بعضی مواقع، به یک درخواست به‌خصوص، از بیرون باید اجازه داده شود. توجه کنید که من نگفتم، این فکر خوبی است یا شما باید آن کار را کنید.

اجازهٔ دسترسی مستقیم از انترنت (خارج)، از طریق دیوار آتش بسیار خطرناک است، اما تکنیک متداولی است. در این نوع عیارسازی، کلید امنیت این است که انواع ترافیک و شمارهٔ پورت‌های مجاز را دقیقاً مشخص کنید، به‌حیث مثال، اجازه به IP از هر کجای شبکهٔ داخلی کار مناسبی نیست؛ مثلاً: شما باید به ترافیک internet HTTP (پورت 80) اجازهٔ ورود به سرور وب (آدرس‌های IP: 10.10.10.10) را بدهید، این تنها به ترافیک HTTP پورت 80 اجازهٔ ورود از انترنت به سرور وب را می‌دهد. آیا فکر می‌کنید که باید کار دیگری انجام دهید.

البته که باید انجام دهید، اگر به مُدل لایه‌یی امنیت برای محافظت از شبکهٔ خود اعتقاد پیدا کرده‌اید. به این دلیل که بسیاری از نقاط ضعف و حمله‌ها از جانب HTTP و پورت 80 است، دیوار آتش نمی‌تواند، بسیاری از آنها را تشخیص دهد، زیرا شما به همهٔ این ترافیک اجازهٔ عبور داده‌اید.

یک تکنیک توصیه‌شده این است که لایه‌های امنیت به‌صورت یک دیوار آتش شخصی، IDS (Intrusion Detection System)، و نرم‌افزار ضد ویروس، اضافه کنید، هچنن قبل از پیاده‌سازی این تنظیمات، اطمینان حاصل کنید که عناوین سیاست امنیتی شما بهترین تکنیک ممکن است و همه مراحل مورد نیاز برای نگهداری امنیت در آن طی شده است. اگر شما یک سیاست امنیتی نداشته باشید، این بهترین وقت برای شروع نوشتن آن است.

۴.۸ تعیین سیاست دسترسی به خارج

همه دیوارهای آتش، ترافیک به دیوار آتش را بازرسی می‌کنند، اما دیوار آتشی که خوب نصب و طراحی شده باشد، ترافیک خروجی کاربر را نیز بازرسی می‌کند.

مبحثی را که پیش از این در مورد سرورهای Proxy و چگونگی استفاده از آنها برای کنترول و بازرسی ترافیک خروجی از شبکه مطرح کردیم، به یاد آورید؛ آن‌ها مثال‌های خوبی از ابزاری بودند که یک سیاست دسترسی به خارج را تعیین می‌کند.

به علاوه، مبحثی را که در مورد قراردادن یک دیوار آتش بین شبکهٔ خود و اتصالاتی که به شرکای کاری شما متصل هستند مطرح کردیم، به یاد آورید که این نوع استفاده و عیارسازی دیوار آتش،ت رافیک خروجی از شبکهٔ شما را کنترول و بازرسی می‌کند.

همچنان ممکن است بخواهید که از دیوار آتش اصلی خود برای کنترول آدرس‌های IP خروجی استفاده کنید؛ مخصوصاً که شما باید فقط به آدرس‌های IPیی اجازهٔ خروج دهید که در شبکهٔ داخلی شما وجود دارند. درنتیجه، از سوءِاستفاده (spoofing) آدرس‌های IP جلوگیری می‌کنید.

شاید مکان‌های مشخصی نیز در انترنت وجود داشته باشند که نمی‌خواهید، کاربران شما وارد آنها شوند. ممکن است شما بخواهید، آن‌ها فقط اجازهٔ ورود به مکان‌های مشخصی را داشته باشند و به‌صورت پیش‌فرض از دسترسی آنها به آدرس‌های دیگر جلوگیری شود.

در بخش بعد به بررسی یکی دیگر از وجوه دیوار آتش و امنیت شبکه، یعنی DMZ (Demilitarized Zone) می‌پردازیم.

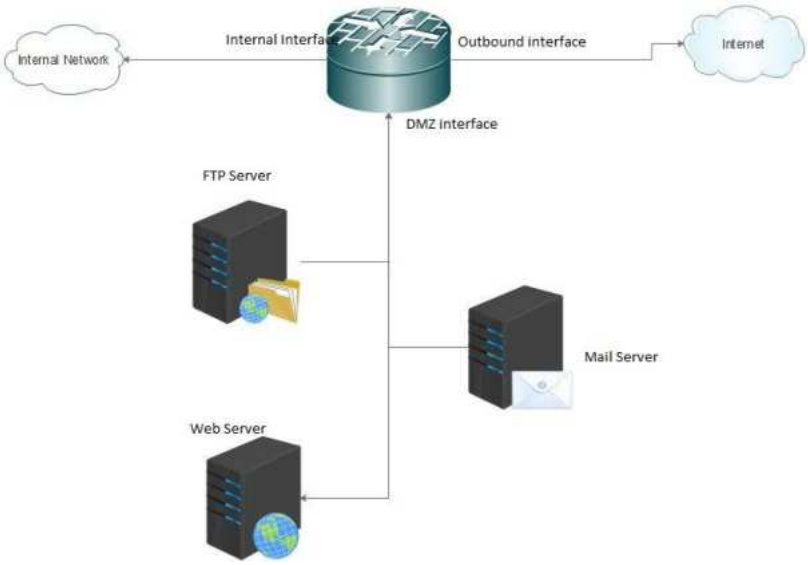
۴.۹ ملزومات اولیهٔ زندگی در DMZ

DMZ (Demilitarized Zone) یک اصطلاح در ارتش است و به منطقهٔ بین دو دشمن گفته می‌شود. شاید یکی از DMZهای شناخته‌شده در جهان، DMZ بین کوریای شمالی و جنوبی باشد که آن دو را از هم جدا می‌کند؛ زیرا از زمان جنگ کوریا، آن‌ها هنوز قرارداد صلح پایداری امضا نکرده‌اند. شاید این مطلب نظامی به نظرتان جالب برسد، اما این چگونه به امنیت شبکهٔ شما و دیوار آتش مربوط می‌شود؟

اتصال سرورهای وب، ایمیل، و FTP به انترنت می‌تواند خطرناک باشد و در برخی موارد این کار توصیه نمی‌شود. اگر سایت شرکت شما روی میزبان خودش قرار دارد و داری سرورهای ایمیل خود است، شما باید از یک دیوار آتش به دو رابط (خارجی و داخلی) استفاده کنید؛ دیوار آتشی که دارای قوانین انتقال برای هدایت ترافیک داخلی به سرورهای درست در شبکهٔ خصوصی شما باشد. این کار به نظر بسیار امن می‌رسد، اما درصورتی‌که یک هکر با استعداد در کمین شما نشسته باشد، می‌تواند فاجعه‌آمیز باشد. مدتی پیش عده‌یی از انسان‌های هوشمند دور هم جمع شده، گفتند که "بیا یک رابط سوم بدیوار آتش اضافه کنیم و آن را DMZ بنامیم." افزودن رابط سوم به یک دیوار آتش استندرد، ساخت سرورها و سرویس‌های (email, www و...) قابل دسترسی در انترنت را ساده‌تر و امن‌تر ساخت.

ارسال مستقیم ترافیک از انترنت به شبکهٔ خصوصی، بسیار ایدهٔ بدی است. این ایده آنقدر بد است که برخی سازمان‌ها حتا به آن فکر هم نمی‌کنند. اگر قصد داشته باشید، در بیرون خانهٔ خود کمپیوتر بفروشید، نمی‌خواهید، همه مردم برای خرید کمپیوتر وارد خانهٔتان شوند؛ آیا می‌خواهید؟ مطمئناً نمی‌خواهید، شما می‌خواهید، یک فروشگاه کوچک در گاراژ یا در جلوی ایوان درست کنید، تا از توجه مردمی‌که نمی‌شناسید، به داخل منزل و فضولی آنها در کلکسیون کتاب‌هایتان یا رفتن آنها بر سر یخچال شما و درست‌کردن ساندویچ جلوگیری کنید.

DMZ یک رابط است که بین قسمت قابل اعتماد (شبکهٔ شرکت شما) و قسمت غیر قابل اعتماد (انترنت) شبکه قرار می‌گیرد و با اجرای یک سری از قوانین اتصال، در داخل دیوار آتش یک جداسازی فزیکی در بین دو شبکه ایجاد می‌کند. چند جداسازی فزیکی یک DMZ جداسازی شده‌اند و مستقیماً به شبکهٔ داخلی شما متصل نیستد (شکل ۲۲)



شکل ۴-۲ عملکرد و کارایی DMZ

در شکل ۲۲، بخش متصل به رابط DMZ مکانی است که سرورهای ایمیل، وب، و FTP را در خود جای داده است. قوانینی که به رابط DMZ اعمال شده‌اند، از ورود ترافیک انترنت به بخش متصل‌شده به آن جلوگیری می‌کنند.

بزرگ‌ترین مزیت یک DMZ این است که همه درخواست‌های انترنتی ناآشنا به سرورهای روی DMZ را جدا کرده، به آنها اجازهٔ ورورد به شبکهٔ داخلی شما را نمی‌دهد. با این وجود، نصب یک دیوار آتش با DMZ مزایای دیگری نیز دارد که به شما امکان می‌دهد، در مورد فعالیت‌هایی که در شبکه انجام می‌شود، بیشتر بدانید، و این موجب افزایش امنیت خواهد شد:

۱. بازرسی‌ترافیک DMZ؛
۲. قراردادن یک IDS (Intrusion Detection System) در DMZ؛
۳. محدودکردن به‌روزرسانی‌های روتری (Routing) به سه رابط؛
۴. قراردادن DNS در DMZ.

در این بخش DMZ را معرفی کردیم و مثال‌های متعددی را در مورد استفاده از آن ذکر کردیم. بررسی‌های مورد زیرین، ملزومات یک DMZ را بررسی می‌کند و به این پرسش پاسخ می‌دهد که چرا باید در یک شبکه با معیارهای خاص یک DMZ استفاده شود؟

خلاصهٔ فصل چهارم

در این فصل در مورد دنیای دیوار آتش و نقش آن در امنیت یک شبکه بحث کردیم. همه، به ارزش این ابزارها اعتقاد ندارند و ما در این فصل سعی کردیم به پرسش‌های این اشخاص نفی‌کننده، پاسخ دهیم و آنها را متقاعد کنیم که نادرست فکر می‌کنند. با بیان حقایق بنیادی در مورد این‌که دیوار آتش ظهور سیاست امنیتی شرکت است و گسترش بحث پیرامون جنبه‌های مثبت فنی دیوار آتش، دلایل بیشتری بر اهمیت این ابزار آوردیم.

همچنان در این فصل چگونگی عملکرد دیوار آتش، کی و کجا باید آنها را به کار برد، و چگونگی طراحی سیاست‌های دسترسی لازم برای تعریف دسترسی به شبکه را بیان کردیم. افزون بر آن در این فصل، رابط DMZ را به‌حیث یک تکامل در دیوار آتش معرفی کردیم و گفتیم که چگونه یک مکان ویژه برای سرورهای انترنت مختلف ایجاد می‌کند. این فصل شامل چندین بررسی موردی بود که به‌صورت خلاصه دیوار آتش و محدودیت‌های آن را در عمل نشان می‌داد.

سوالات و فعالیت فصل چهارم

۱. چه کسی به دیوار آتش احتاج دارد؟

۲. چرا به دیوار آتش احتاج داریم؟

۳. آیا به دیوار آتش احتاج داریم؟

۴. چطور یک دیوار آتش باعث توسعهٔ یک سیاست امنیتی می‌شود؟

۵. نام جدولی که در یک دیوار آتش قرار دارد و اتصالات را ردیابی می‌کند چیست؟

۶. DMZ چه کاری را انجام می‌دهد؟

۷. چهار مزیت DMZ را بیان کنید.

۸. آیا دیوار آتش می‌تواند، سیاست‌های رمز عبور را اجرا کند یا از استفادهٔ بی‌مورد کاربران از رمز جلوگیری کند؟

فعالیت

نحوهٔ عیارسازی یک دیوار آتش CISCO ASA را در نرم‌افزار GNS3 انجام دهید.

فصل پنجم

شبکه‌های خصوصی مجازی

هدف کلی: محصلان با Virtual Private Network (VPN) آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. مفهوم VPN تشریح کنند.
۲. مزایا و اهداف VPN را بیان کنند.
۳. استراتیژی‌های استفاده از VPN را توضیح دهند.
۴. مفاهیم IPSec را توضیح دهند.
۵. مفهوم tunneling را توضیح دهند.

VPN ها یکی از مهمترین راه حل موجود برای کاهش هزینه‌های باند می‌باشد. برای اتصال به یک شبکهٔ خصوصی از راه دور و از طریق یک شبکهٔ عمومی لازم است یک شبکهٔ خصوصی مجازی (VPN) ایجاد گردد که این اتصال از طریق یک تونل رمزنگاری‌شده بین کلاینت VPN و شبکل خصوصی شما صورت می‌پذیرد.

در این فصل با مفهوم VPN یا شبکه‌های خصوصی مجازی آشنا می‌شویم، که دربرگیرندهٔ موضوعاتی چون مزایا، اهداف VPN و استراتیژی‌های به‌کارگیری از، VPN، مفهوم IPSec و مهفوم Tunneling می‌باشد.

۵.۱ شبکهٔ خصوصی مجازی (Virtual Private Network-VPN)

در ابتدا لازم است که دو مفهوم شبکه‌های خصوصی (Private Network) و شبکه‌های عمومی (Public Network) را معرفی نماییم. زمانی‌که شما سیستم‌های کمپیوتری داخل منزل یا دفتر کارتان را به صورت LAN به هم متصل می‌کنید در حقیقت یک شبکهٔ خصوصی (Private Network) ایجاد کرده‌اید. سیستم‌های داخل شبکهٔ خصوصی می‌توانند به راحتی همدیگر را دیده و با هم ارتباط برقرار کنند اما این سیستم‌ها از بیرون شبکهٔ خصوصی شما (مثلاً از طریق انترنت) قابل دستیابی نیستند. سیستم‌های کمپیوتری داخل یک شبکهٔ خصوصی می‌توانند هر IP Address دلخواه شما (مثلاً ۱۹۲.۱۶۸.۰.۱) را داشته باشند زیرا این IP Addressها فقط داخل شبکهٔ خصوصی شما تعریف شده‌اند و خارج از شبکهٔ خصوصی شما معنا ندارند. به این IP Addressها Private IP Address گفته می‌شود.

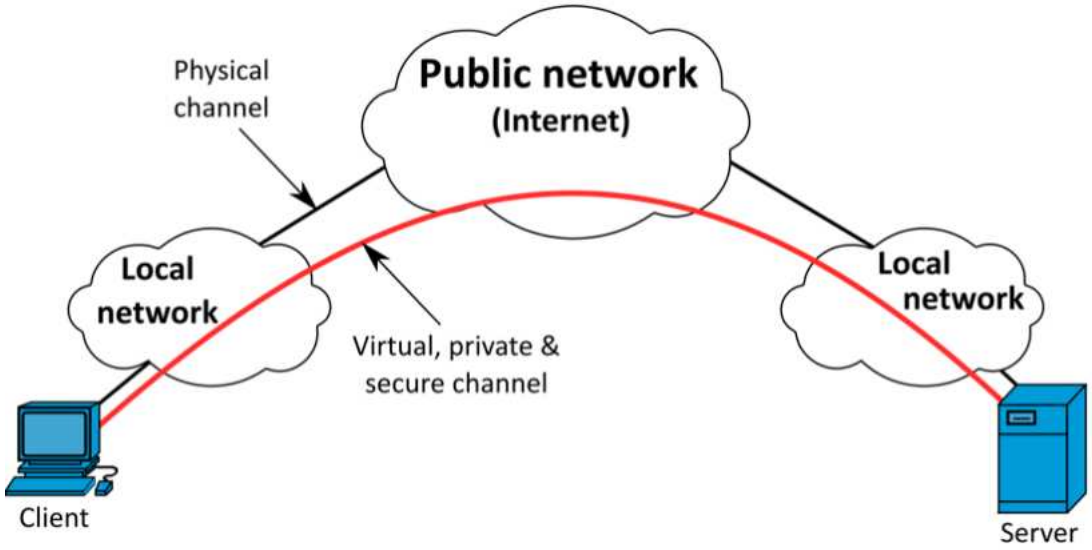
اما شبکهٔ عمومی (Public Network) به سیستم‌های متعلق به شما محدود نمی‌شود. در حقیقت شبکهٔ جهانی انترنت اصلی‌ترین شبکهٔ عمومی است. سیستم‌های متصل به انترنت باید IP Address یکتای مختص به خود را داشته باشند که توسط RIR به آنها فروخته شده است. این IP Addressها کاملاً یکتا و عمومی‌اند. منظور از آدرس آی‌پی عمومی (Public IP Address) این است که این IP Address در انترنت تعریف شده و از طریق آن می‌توان به سیستم مورد نظر دسترسی مستقیم داشت.

حال که با مفهوم شبکهٔ خصوصی و شبکهٔ عمومی آشنا شدید، لازم است بدانید که گاهی لازم است از خارج از یک شبکهٔ خصوصی و از طریق یک شبکهٔ عمومی (مثل انترنت) به سیستم‌های داخل شبکهٔ خصوصی دسترسی داشته باشید. مثلاً فرض کنید که می‌خواهید از خانه به فکس شرکت و یا فایل‌های به اشتراک گذاشته شده در شبکهٔ داخلی شرکت دسترسی داشته باشید. یا فرض کنید که می‌خواهید از خارج از محیط آموزشی، به اسناد و پایان‌نامه‌های موجود در شبکهٔ داخلی محیط آموزشی دسترسی پیدا کنید. یا فرض کنید که فایروال نصب‌شده روی سرور سایت شما قسمی تنظیم شده است که تنها از داخل شرکت اجازهٔ دسترسی به سرور را می‌دهد و شما نیاز دارید که از بیرون شرکت به آن دسترسی پیدا کنید.

برای اتصال به یک شبکهٔ خصوصی از راه دور و از طریق یک شبکهٔ عمومی لازم است یک شبکهٔ خصوصی مجازی (VPN) ایجاد کنید.

پس VPN عبارت از اتصال به یک شبکهٔ خاص از راه دور و از طریق یک شبکهٔ عمومی می‌باشد.

این اتصال از طریق یک تونل رمزنگاری‌شده بین کلاینت VPN و شبکهٔ خصوصی شما صورت می‌پذیرد. شما با واردکردن یک نام کاربری و کلمهٔ عبور و یا واردکردن یک Certificate در نرم‌افزار کلاینت VPN می‌توانید یک تونل امن به شبکهٔ خصوصی مورد نظرتان باز کنید.



شکل ۵-۱ تونل امن ایجادشده بین استفاده‌کننده و شبکهٔ خصوصی

۵.۲ مقایسه: VPNها به شکلی امن با LAN ارتباط برقرار می‌کنند

شبکهٔ شما (LAN) شهری از تعقل، سفارش‌ها، با خدمات اقیانوس غیر قابل پیش‌بینی به نام انترنت است. شما هزاران شهر و جزیرهٔ دیگر را در این اقیانوس می‌شناسید؛ وقتی می‌خواهید، از جزیره‌ها به جزیرهٔ دیگر سفر کنید، بر روی یک کشتی نشسته، چشم به وب‌سایت هدف می‌دوزید.

اکنون سوار بر آن کشتی (TCP/IP)، در حال سفر در اقیانوس (انترنت) هستند که به چیزی در یک جزیره برسید (LAN) که نوع خدمات ارائه می‌دهد. این موضوع بی‌معنا نیست، اکنون چند نفر دیگر را در کشتی می‌بینید؟ اگر مشغول خواندن آخرین اخبار فاکس‌نیوز باشید، نداشتن حریم خصوصی مهم نیست. اما اگر وارد سایت شرکت شخصی خود شوید، آنگاه نداشتن امنیت مشکل‌ساز خواهد بود.

چون مشغول سفر در اقیانوس جهانی به نام انترنت هستید، هیچ کنترولی بر کیبل‌ها، فایبرها، روترها یا سویچ‌های تشکیل‌دهندهٔ آن ندارید. هیچ تضمینی به هیچ شکل وجود ندارد. به‌عبارت‌دیگر، شاید بتوانید، به سایت یا سرور دیگر متصل شوید، اما تضمینی وجود ندارد. به یاد داشته باشید که اتصال به انترنت یک لطف است، نه یک حق. عدم کنترول بر انترنت، یعنی آسیب‌پذیری امنیتی و این مشکل هنگام ارتباط با شبکه‌های خصوصی از طریق یک منبع عمومی‌مانند انترنت، جدی‌تر می‌شود.

شما به‌عنوان شخصی که جزیرهٔ خود را با یک جزیره مرتبط می‌کند، مسئول این ارتباط هستید و شما را رهنمایی می‌کنیم که یک جزیرهٔ تازه بخرید. جزیرهٔ شما تصمیم می‌گیرد که پلی به جزیرهٔ دیگر بزند تا راهی

ایمن‌تر، سریع‌تر و مستقیم‌تری برای افرادی که در بین آن سفر می‌کنند، مهیا شود. حتا اگر در جزیرهٔ نزدیک باشند، بازهم احداث پل گران خواهد بود؛ اما نیاز به راهی مطمئن و قابل قبول آن قدر زیاد است که به‌هرحال این کار را می‌کنید. این حالت شبکه داشتن یک WAN است. پل‌ها (خطوط شخصی) از اقیانوس (انترنت) جدا هستند، اما با LANها ارتباط برقرار می‌کنند. بسیاری از شرکت‌ها از این روش استفاده می‌کنند، زیرا نیاز به امنیت و قابلیت اعتماد ارتباط از راه دور با محل کار، آن را لازم می‌کند.

جزیرهٔ شما می‌خواهد، با جزیرهٔ دیگری که بسیار دورتر است، ارتباط برقرار کند؛ اما این بار هزینهٔ احداث پل بسیار خواهد بود. می‌دانید که اگر فواصل زیاد باشد، هزینه‌ها بالا خواهد رفت؛ اما نیاز همچنان وجود دارد.

بسیاری از شرکت‌ها مایل‌اند که IT، کار آنها را تکمیل کند و درحالی‌که برای برخی این کار مناسب است، اغلب شرکت‌ها باید تغییر عقیده دهند و برعکس فکر کنند. روش کار شرکت باید زیرساخت‌های IT یک شرکت را تعیین کند. این‌یک حقیقت اساسی است، زیرا شرکت‌ها به هدف داشتن یک بخش بزرگ شبکه یا IT، کار نمی‌کنند. دههٔ ۹۰ تمام‌شده است و متأسفانه حقیقت به‌شکل مُدل‌های تجاری اثبات‌شده، بازگشته است.

هنوز نمی‌دانید، VPNها در کجای این مقایسه جای دارند؟ می‌دانید که به امنیت بیشتر نیاز دارید و اولین گزینه ساختن یک پل بود که بسیار گران است. می‌توانید برای یک سفر ایمن و شخصی، از یک زیردریایی استفاده کنید. زیردریایی در یک مقیاس کامل برای VPN است؛ زیرا VPNها مثل زیردریایی‌ها خواص زیر را دارند:

۱. سریع هستند.
۲. قابل حمل هستند.
۳. شمارا از دید دیگران پنهان می‌کنند.
۴. پس از اولین استفاده، هزینه‌های اضافی آنها بسیار کم است.
۵. هنگام سفر از شما محافظت می‌کند.
۶. PDAهای مطلع از VPN، آخرین ورودهای VPN به بازار هستند.
۷. نرم‌افزار Cisco VoIP Softphone در یک VPN به‌خوبی کارمی‌کند و PC شمارا به یک تلفون ایمن تبدیل می‌کند.

شاید داشتن یک زیردریایی کار راحتا نباشد اما مطمئناً این مقایسه را به‌خوبی درک می‌کنید. انواع مختلف استفاده از VPN وجود دارد و ما در بخش بعدی، سه نوع مختلف VPN را بررسی می‌کنیم. یک مقایسهٔ خوب دیگر می‌تواند، مفهوم پورتال‌های Stargate باشد. شما باید نشانه‌ها را در هر دو سمت داشته باشید. (SA برای VPN)، و برای سمت دیگری که روشن است، باید یک Stargate داشته باشید تا بتوانید تونل فرافضایی (تونل VPN) را داشته باشید.

۵.۳ نمای کلی از VPN

یک شبکهٔ مجازی شخصی (VPN) یک ارتباط شبکه‌یی رمزنگاری‌شده است که از یک تونل امن بین دونقطه، از طریق انترنت یا دیگر شبکه‌ها مثل WAN استفاده می‌کند. در یک VPN، ارتباط از طریق dialup با کاربران راه دور با خطوط اجاره‌یی (Lease-line) یا ارتباطات Frame Relay با سایت‌های راه دور، جایگزین ارتباط محلی با یک ISP، و دیگر خدمات دهندگان (POP) می‌شود. افزایش بیش از اندازهٔ ارتباطات انترنتی در خانه‌ها و دفاتر دورافتاده، استفاده از دسترسی ارزان‌تر به انترنت را جذاب می‌کند. همان‌طورکه گفته شد، پس از سرمایه‌گذاری اولیه در VPNها، هزینهٔ اضافه‌کردن سایت‌ها یا کاربران بیشتر به حد اقل می‌رسد.

کاربران دور شبکه به شما امکان می‌دهد تا به‌شکل امن و قابل‌اعتماد، با استفاده از انترنت به‌عنوان وسیلهٔ ارتباط، با LAN خصوصی شما رابطه برقرار کند. یک VPN برای پوشش کاربران بیشتر و مکان‌های متفاوت رشد کرده و بهتر از یک خط اجرایی عمل می‌کند. درواقع مقیاس‌پذیری یک ویژگی عمده است که VPNها نسبت به دیگر خطوط دارند. برخلاف خطوط اجاره‌یی (Leased-line) که در آنها هزینه نسبت به فاصله افزایش می‌یابد، مکان جغرافیایی هر دفتر در خلق یک VPN بسیار کمی‌دارد.

می‌توان VPN رمزنگاری‌شده‌یی داشت که برای امنیت به نوع دیگری از رمزنگاری (مثل VPNهای MPLS) وابسته است. تنها تحت شرایط خاص این VPNها راه‌حل مناسب برای شبکهٔ شما هستند. بهترین حالت این است که شما را وادار کند، همواره‌ترافیک عبوری از VPN را، رمزنگاری کنید. انجام‌ندادن این کار ممکن است، خیلی فاجعه‌بار باشد و مسئولیت آن فقط به عهدهٔ شماست.

یک VPN باعث می‌شود تا یک شبکهٔ داخلی از طریق رمزنگاری IPSec، به‌طور امن در انترنت یا دیگر شبکه‌ها گسترش‌یافته، تجارت الکترونیک و ارتباط با شبکه‌های خارجی و کارمندان متحرک را آسان کرده، به شرکای تجاری، تأمین‌کنندگان و مشتریان خدمات دهد. سه نوع مختلف VPN وجود دارند:

۱. **VPNهای دسترسی از راه دور (Remote Access VPNs):** به کاربران شخصی مرتبط از راه dial-up امکان می‌دهد تا از طریق انترنت یا دیگر شبکه‌های عمومی، به یک سایت مرکزی مرتبط شوند. این نوع VPN، یک ارتباط کاربر به LAN است و کارمندانی که نیاز دارند در یک حوزه با LAN مرتبط باشند، می‌توانند، از این امکانات استفاده کنند. سیستم‌های آنها از یک نرم‌افزار ویژهٔ کاربر VPN استفاده می‌کند، که ارتباط فوری را بین آنها و LAN شرکت فراهم می‌نماید. معمولاً شرکتی که می‌خواهد، یک VPN بزرگ دسترسی از راه دور داشته باشد، با استفاده از یک ISP، یک ارتباط dial-up به کاربران خود می‌دهد؛ سپس این کاربران برای دسترسی به انترنت از یک شمارهٔ رایگان استفاده کرده، از نرم‌افزار VPN خود برای دسترسی به LAN شرکت استفاده می‌کنند. مثالی از شرکتی که به این نوع VPN نیاز دارد، می‌تواند شرکت بزرگی با صدها فروشنده باشد. VPNهای دسترسی از راه دور را گاهی اوقات VPNهای نرم‌افزار امنیتی (مبتنی بر نرم‌افزار)، شبکه‌های خصوصی مجازی dial-up (VPDN) ویا VPNهای تلفنی می‌گویند. کاربران برای استفاده از خط تلفون محلی، هزینهٔ ثابت بسیار کم می‌پردازند

و دیگر نیاز به پرداخت هزینه‌های راه دور ویا تماس مستقیم با دفتر شرکت ندارند. کاربر می‌تواند برای ایجاد یک تونل VPN در انترنت از یک ISP محلی استفاده کند. CFOها هزینه‌های کوچک و ثابت را به هزینه‌های زیاد راه دور ترجیح می‌دهد.

۲. **VPNهای سایت‌به‌سایت (Site-to-Site VPNs)** - برای ارتقای LAN فعلی شرکت و گسترش آن به ساختمان‌ها و سایت‌های دیگر از طریق استفادهٔ تجهیزات اختصاصی استفاده می‌شود، تا کارمندان شاغل در این مکان‌ها بتوانند، از خدمات شبکه‌یی مشابه استفاده کنند. این نوع VPNها به‌طور فعال همواره متصل هستند و گاهی به آنها VPNهای سخت‌افزاری (مبتنی بر سخت‌افزار)، شبکهٔ داخلی، یا VPNهای LAN به LAN گفته می‌شود.

همهٔ این VPNها، عملکرد، اعتماد، کیفیت خدمات و امنیت برای محیط‌های معمول WAN با استفاده از ISP کم‌هزینه، و انعطاف‌پذیری نسبت به دیگر خدمات‌دهندگان را فراهم می‌کنند، شکل ۱-۷ سه نوع مختلف VPN را نشان می‌دهد.

تکنالوژی VPN برای ارائهٔ لایهٔ امنیتی بیشتر و کنترول دسترسی به معلومات مالی برای کاربران خاص ویا اطمینان از این‌که معلومات حساس و محرمانه به‌شکل امن ارسال می‌شوند، قابل‌استفاده است. دراین‌صورت، VPNها می‌توانند رمزنگاری شده، امنیت‌ترافیک سیستم‌های حساس را بیشتر کنند. بخش بعدی، جایگاه VPNها و مزایای خاص آن را بررسی می‌کند.

۵.۴ مزایا و اهداف VPN ها

یک VPN با طراحی خوب می‌تواند، منفعت زیادی برای یک شرکت داشته باشد. برخی از مزایای استفاده از VPN در شبکه عبارتند از:

۱. قبل از اختراع تکنالوژی VPN کارمندان در مکان‌های دور مجبور بودند، برای دسترسی به شبکهٔ شرکت خود، از خطوط تلفون راه دور استفاده کنند. شما می‌خواهید، با جایگزین‌شدن خطوط راه دور با ارتباط محلی و انترنت از طریق استفاده از یک VPN، هزینه‌های ارتباطی خود را کاهش دهید. باتوجه به تعداد کارمندان در یک حوزه، همین کار به‌تنهایی می‌تواند، صرفه‌جویی زیادی را به همراه داشته باشد، برای بسیاری از شرکت‌های کوچک‌تر بااعتبار مالی کمتر، راه‌حل VPN یک راه‌حل عملی است.
۲. شما می‌توانید، بهره‌وری کاربران خود را، با ارائهٔ دسترسی امن به منابع شبکه، بدون توجه به مکان جغرافیایی آنان، افزایش دهید.
۳. شما می‌خواهید، هزینه‌های عملکرد مربوط به ارتباطات با اتصال WAN اختصاص‌یافته و جایگزین‌کردن آن‌ها با ارتباطات انترنت مستقیم، مثل انواع تجاری با پهنای باند بالا، از طریق سایت‌های راه دوری را که به روش یک VPN سایت‌به‌سایت متصل می‌شوند، کاهش دهید.
۴. شما می‌خواهید، نقشهٔ سایت خود را با اضافه‌کردن VPNها در تمام شبکه، ساده‌تر کنید.

۵. نیازهای پهنای باند شما منطقی‌اند، زیرا سایت‌ها نیازمند ارتباط با شبکه هستند. با از استفاده از VPN، بازگشت سرمایهٔ سریع‌تری نسبت به WAN خواهید داشت.
۶. شما می‌خواهید، در استفاده از کمپیوتر همراه، ارتباط از راه دور و شبکه‌های دفاتر کاری، تجارت الکترونیکی آسان‌تر و ارتباط بیرون شبکه‌یی با شرکای تجاری، دستیابی انترنتی تأمین‌کنندگان و مشتریان انعطاف‌پذیری داشته باشید؛ و دستیابی درون‌شبکه‌یی و بیرون شبکه‌یی با استفاده از یک ارتباط تکی و امن میسر باشد.
۷. شما می‌خواهید، هزینه‌های دفتر کاری خود را با داشتن کاربرانی که فقط سه روز در هفته به محل کارمی‌آیند و مابقی را در خانه کارمی‌کنند، کاهش دهید. کاربران خانگی معمولاً کارایی بالاتر و استرس کمتری دارند.

قبل از استفاده از یک VPN باید زمان زیادی را برای درک آنچه می‌خواهید، به آن دست‌یابید، اختصاص دهید. در طول این کار، قبل از انتخاب یک راه‌حل یا سخت‌افزار و نرم‌افزار باید مهم‌ترین ویژگی‌ها را در نظر بگیریم. امنیت که بعداً توضیح داده خواهد شد، یکی از مهم‌ترین ویژگی‌های شماست.

۵.۵ استراتیژی‌های به‌کارگیری VPN

این استراتیژی‌ها بسیار متنوع‌اند، زیرا هر تولیدکننده‌یی، VPN ویژهٔ خود را دارد. برخی از آنها خدماتی هستند که تولیدکنندگان ادعا می‌کنند و برخی دیگر، همان‌طورکه در فصل شش گفته شد، نگرانی‌های امنیتی به وجود می‌آورند. چون هیچ استندرد قابل‌قبولی در این زمینه وجود ندارد، بسیاری شرکت‌ها راه‌حل ویژهٔ خود را ارائه می‌دهند. این بخش، برخی مؤلفه‌های بالقوهٔ موجود در سیسکو را بررسی کرده، چگونگی استفاده از وسایل مثل دیوارهای آتش (Firewalls) را برای رسیدن به نقش یک VPN کامل شرح می‌دهد:

۱. **دیوارهای آتش یا (Firewalls):** اگر تا قبل از خواندن فصل 5، دیوار آتش نداشتید، احتمالاً حالا دارید. دیوارای آتش برای امنیت شبکهٔ شما حیاتی‌اند. امروزه، همه دیوارهای آتش سیسکو،ترکیب VPNها با شناسایی بسته و مشروط (SPI) را پشتیبانی می‌کنند. راه‌حل‌ها از VPNهای استندرد سایت‌به‌سایت که بر IKE اثر دارند، گرفته، استفاده از استندرد رمزنگاری DES، 56 بیت، DES سه‌گانهٔ 168 بیت ویا رمزنگاری استندرد پیشرفتهٔ AES، رمزنگاری می‌کند. این دیوارهای آتش که یک تکنالوژی جالب هستند، ترجمهٔ آدرس شبکهٔ پویا، فلترکردن بستهٔ شبکه، دیوار آتش و قابلیت‌های انجام VPN را در یک سخت‌افزار ترکیب می‌کنند. این وسیله به‌جای استفاده از Cisco IOS، از یک سیستم‌عامل به‌شدت جریان‌مند استفاده می‌کند، که با تمرکز بر روی IP، بسیاری از پروتوکول‌ها را برای ارتقای عملکرد کنترول می‌کند.
۲. **روترهای سازگار با VPN:** روترهای سیسکو می‌توانند، برای استفادهٔ VPNها ارتقا داده شوند. این ارتقا، بسته به نوع روتر، شکل‌های مختلفی دارد: IOS، حافظه، ویا سخت‌افزار VPN اختصاص‌یافته. شما می‌توانید، برخی ویژگی‌های منحصربه‌فرد از نظر اندازه‌پذیری، روتری، امنیت و کیفیت خدمات را داشته باشید.

۳. **متمرکز کنندهٔ VPN:** با به‌کارگیری پیشرفته‌ترین رمزنگاری و تکنیک‌های تأیید اعتبار موجود، متمرکزکننده‌های Cisco VPN به‌طور مشخص برای ایجاد VPNهای دسترسی از راه دور ساخته می‌شوند، که عملکرد، اندازه‌پذیری و دسترسی بالا را فراهم کرده، شامل مؤلفه‌هایی به نام ماژول‌های پردازشگر و رمزنگاری اندازه‌پذیر (Scalable Encryption Processing – SEP) می‌شود، که مهندسان شبکه را قادر می‌سازد تا ظرفیت و تکامل را به آسانی افزاش دهند. متمرکزکننده‌های VPN برای کنترول ملزومات VPN ساخته‌شده، و برای مُدل‌های هر چیزی، از شرکت‌های کوچک با کاربران راه دوری از 100 تا 10000 نفر همزمان، مناسب هستند.

۴. **نرم‌افزار کاربر:** این نرم‌افزار به‌سادگی راه‌اندازی شده، کارمی‌کند، تونل‌های رمزنگاری‌شده سرتاسر امنی را برای وسایل VPN که در اینجا فهرست شده‌اند، فراهم می‌کند. این طراحی ظریف، یعنی نرم‌افزار سازگار با IPSec می‌تواند، برای استفاده‌های وسیع تنظیم شود و اتصالات اولیه، نیاز کمی به دخالت کاربر دارد. این نرم‌افزار برای سیستم‌عامل‌های زیر موجود است: ویندوز 95، 98، ME، NT.4.0، 2000، XP، Linux (Intel)، (Ultra Spaev – 32 it)، MAC OSX 10X.

بسته به نوع VPN (دسترسی از راه دور ویا سایت‌به‌سایت)، شما باید از مؤلفه‌های سخت‌افزاری خاص برای ساخت VPN خود استفاده کنید. اما موارد زیر را هم در نظر بگیرید:

۱. **قابلیت مدیریت:** این قابلیت از VPN، مقدار تلاش لازم برای حفظ ارتباط شبکه را نشان می‌دهد؛ به‌ویژه مجلهٔ PC این قابلیت را از طریق عوامل سهولت کاربرد برای گزینه‌های مدیریتی محلی و راه دور شامل این‌که یک نرم‌افزار مبتنی بر جستجوگر یا دسترسی خط فرمان مورد استفاده است، تعریف می‌کند.

۲. **قابلیت اعتماد:** مسلماً اگر نرم‌افزار VPN در دسترس نباشد، بهره‌وری و احتمالاً پول خود را از دست داده‌اید. هنگام انتخاب یک راه حل برای مقایسه، آخرین آمار را درخواست کنید.

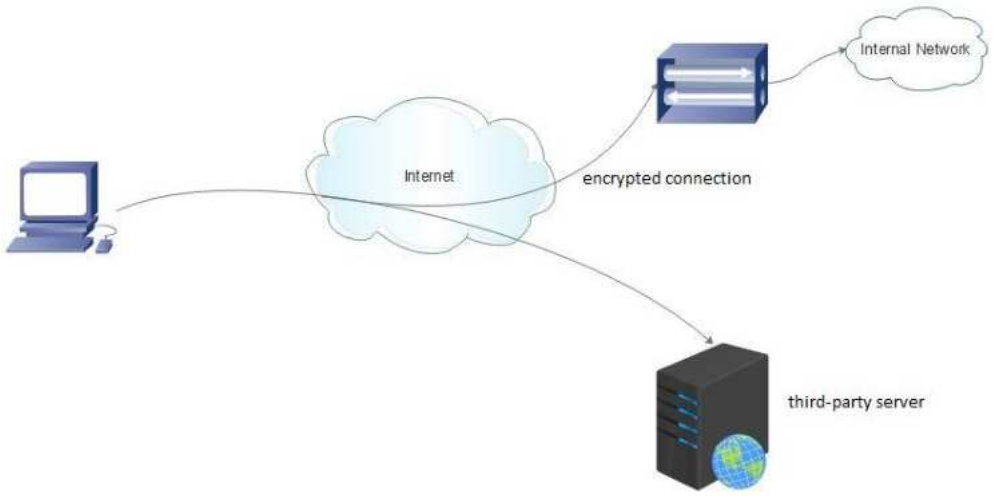
۳. **اندازه‌پذیری:** با رشد کار یک شرکت، نیازهای IT آن هم افزایش می‌یابد. برای رشد سریع و مقرون به‌صرفهٔ زیرساخت VPN، انتخاب راه‌حلی که اندازه‌پذیر باشد، مهم است. آخرین کاری که یک مدیر IT می‌خواهد طراحی و جایگزینی زیرساخت VPN به دلیل یک گلوگاه در پتانسیل رشد آن است. هنگام انتخاب وسیله‌یی درست برای ارائه خدمات VPN به شبکهٔ خود، باید از محدودیت‌های مطلع باشید؛ مثلاً: یک IOS روتر می‌تواند، VPNها را پایان دهد (terminate)، اما این فرایندی دستی است که باید تنظیم شود و نیازمند درک عمیق‌تری نسبت به زمانی است که از یک PIX Firewall با تنظیمات VPN در GUI استفاده می‌کنید. متمرکزکننده VPN سیسکو نیز وجود دارد که به‌عنوان یک GUI قدرتمند، PIX یا IOS را خنثی کرده، بسیاری از سیاست‌های VPN را مدیریت می‌کند. این متمرکزکننده، ساختارهای قابل درکی را برای تنظیم این سیاست‌های مختلف ارائه داده، به کاربران مختلف با قدرت‌های مختلف در یک گروه، امکان کار در شبکه را می‌دهد. من معمولاً وقتی از متمرکزکننده

استفاده می‌کنم که مشتری، پرسنل محدودی دارد و نیازهای سیاست VPN مختلفی را می‌طلبد. IOS با PIX، با دشواری بیشتری برای این نیاز خاص تنظیم و مدیریت می‌شود. اندازه‌پذیری را نیز فراموش نکنید.

۵.۶ تونل‌زنی دوگانه

بسیاری از کاربران VPN پشت دیوار آتش هستند و تنها از طریق VPN به منابع دسترسی دارند. VPN های معمولی به کاربران اجازهٔ دسترسی به منابع شبکه از محل خود را درحالی‌که در آن واحد با VPN شرکت خود در ارتباط هستند، نمی‌دهند. این مورد، وقتی‌که کاربران باید از طریق یک VPN به یک سیستم دسترسی داشته و با یک چاپگر (Printer) شبکهٔ محلی پرینت بگیرند، مشکل‌ساز می‌شود. برای اصلاح این مشکل یک ویژگی با عنوان تونل دوگانه (Split Tunneling) ارائه می‌شود.

تونل‌زدن دوگانه وقتی رخ می‌دهد که یک کاربر VPN از راه دور ویا یک سایت در زمانی‌که با یک VPN خصوصی در تماس است، بتواند، به یک شبکهٔ عمومی متصل شده، ترافیک شبکهٔ عمومی را از داخل تونل خارج کند. البته این همیشه بهترین ویژگی نیست، زیرا ممکن است که به یک مهاجم امکان تسلیم‌کردن کمپیوتری را که به هر دو شبکه متصل است، بدهد.



شکل ۵-۲ نمایی از عملکرد تونل‌زنی دوگانه

۵.۷ نمای کلی از VPNهای IPSec

IPSec یک استندرد واقعی برای ایجاد VPN ها در صنعت شبکه شده است. چندین تولیدکننده از آن استفاده کرده و چون قانون IETF، IPSec را در یک RFC تعریف کرده است؛ همخوانی بین تولیدکنندگان، IPSec را به بهترین گزینه برای ساخت VPNها تبدیل می‌کند. IPSec ابزاری استندرد برای تأیید اعتبار و خدمات رمزنگاری بین اعضا و رقبا ارائه می‌دهد. برای اهداف این بحث، اعضای IPSec وسایلی هستند که هر انتهای یک تونل VPN را تشکیل می‌دهند. IPSec به‌عنوان لایحهٔ شبکه‌یی مُدل مرجع OSI عمل کرده،

پشتیبانی و تأیید اعتبار پاکِت‌های IP بین وسایل IPSec (اعضا)، از جمله روترها و دیوارهای آتش سیسکو را انجام می‌دهد. IPSec خدمات امنیت شبکهٔ زیر را انجام می‌دهد:

۱. **مخفی‌ماندن داده (Data Cofidentiality):** فرستندهٔ IPSec می‌تواند، پاکِت‌ها را پیش از ارسال به شبکه رمزنگاری کند. اگر یک هکر نتواند، داده‌ها را بخواند، نمی‌تواند، از آنها استفاده کند.
۲. **یکپارچگی داده (Data Integrity):** گیرندهٔ IPSec در نقطهٔ پایانی، همه پاکِت‌های فرستاده‌شده توسط IPSec فرستندهٔ تأییدشده اعتبار می‌کند، تا مطمئن شود که داده‌ها در طول انتقال تغییر نیافته‌اند.
۳. **تأیید اعتبار منشأ داده (Data Origin Authentication):** گیرندهٔ IPSec می‌تواند، منبع پاکِت‌های IPSec ارسالی را تصدیق کند. این سرویس به سرویس یکپارچگی داده بستگی دارد.
۴. **ضد پاسخ (Anti-reply):** گیرندهٔ IPSec می‌تواند، پاکِت‌های پاسخ‌داده‌شده را شناسایی و باز گرداند.

IPSec از داده‌های حساس که در شبکه‌های ناامن حرکت می‌کنند، محافظت می‌کند، و خدمات امنیتی IPSec در لایهٔ شبکه‌یی ارائه می‌شود، بنابراین شما مجبور نیستید، برنامه‌ها، PCها، یا ایستگاه‌های کاری شخصی را تنظیم کنید. این مزیت بسیار مقرون‌به‌صرفه است. به‌جای ارائهٔ خدمات امنیتی که نیازی به راه‌اندازی آن و ایجاد امنیت در هر برنامه ویا هر کمپیوتر وجود ندارد، می‌توانید، به‌راحتا زیرساخت‌های شبکه را به‌گونه‌یی تغییر دهید که خدمات امنیتی لازم ایجاد شود. این مزیت IPSec باعث می‌شود تا در شبکه‌های متوسط، بزرگ و درحال‌رشد که ارتباط امن بین بسیاری از تجهیزات را می‌طلبد، بتوان از آن استفاده کرد.

IPSec ویژگی‌های امنیتی پیشرفته‌یی مثل الگوریتم‌های رمزنگاری بهتر و تأیید اعتبار کامل‌تر را ارائه می‌دهد. شبکه‌های شرکتی متصل به انترنت، با IPSec دسترسی و انعطاف‌پذیری را فراهم می‌کنند. با تکنالوژی IPSec، مشتریان می‌توانند، VPNهای در انترنت، با پشتیبانی رمزنگاری در برابر شنود یا دیگر حملات که وارد ارتباطات خصوصی می‌شوند، بسازند.

تنها سیستم‌های سازگار با IPSec می‌توانند، از این پروتوکول سود ببرند. همچنین همه وسیله‌ها باید از یک کلید رایج استفاده کنند و دیوار آتش هر شبکه باید چیدمان امنیتی مشابه داشته باشد.

IPSec خدمات تأیید اعتبار (Authentication) و رمزنگاری (Encryption) را برای محافظت از نفوذ و تغییر غیر قانونی داده‌ها در شبکه یا هنگام انتقال معلومات در یک شبکهٔ محافظت‌نشده مثل انترنت، ارائه می‌دهد. IPSec می‌تواند، داده‌ها را بین تجهیزات مختلف رمزنگاری کند؛ از جمله:

۱. روتر به روتر؛
۲. دیوار آتش به روتر؛
۳. دیوار آتش به دیوار آتش؛

۴. کاربر به روتر؛
۵. کاربر به دیوار آتش؛
۶. کاربر به متمرکزکنندهٔ VPN؛
۷. کاربر به سرور.

IPSec چارچوبی از استندردهای آزاد است که توسط IETF تعریف شده است. IPSec امنیت انتقال حساس در شبکه‌های محافظت‌نشده مثل انترنت را فراهم می‌کند.

۵.۸ معتبر سازی و یکپارچگی داده

برای ایجاد اعتماد، تأیید اعتبار هویت در نقطهٔ پایانی، VPN و نیز کاربران فرستنده ترافیک از VPN را شناسایی می‌کنند. یک نقطهٔ پایانی می‌تواند، یک کاربر VPN، متمرکزکنندهٔ VPN، دیوار آتش یا روتر باشد. تأیید اعتبار یک فرایند IPSec است که پس از رمزنگاری و قبل از رمزگشایی هنگام دریافت رخ می‌دهد. این کار در IPSec برای تضمین این‌که هم فرستنده و هم گیرنده واقعاً آنچه ادعا می‌کنند هستند، ضروری است. با IPSec، هر عضو باید با یک کلید از پیش تعیین‌شده (که معمولاً توافقی است) و یک فهرست ایستا از اعضای معتبر، به‌طور دستی تنظیم شود و یک جدول بزرگ داخل روتر بسازد که منابع حافظه را پر می‌کند.

یکپارچگی داده، عملکرد دیگری در IPSec است. یکپارچگی یعنی بسته‌یی که گیرنده دریافت می‌کند در طول انتقال تغییر نکرده است. این کار از طریق استفاده از الگوریتم یک‌طرفهٔ Hash انجام می‌شود. این الگوریتم معادل یک حاصل جمع رمزنگاری‌شده است. پس از این‌که سمت فرستنده، یک بسته را رمزنگاری و معتبر می‌کند، یک Hash یک‌طرفه بر روی تمام بسته اجرا می‌شود. این Hash از این نگاه جالب است که نتیجهٔ آن بدون توجه به ورودی، همیشه اندازه‌یی ثابت دارد. این‌یک میکانیزم امنیتی دیگر است، چون هکرها نمی‌تواند، اندازهٔ فیلد ورودی را بدانند. Hash یک‌طرفه، یک فیلد رمزدار می‌سازد که ضمیمهٔ پیغام می‌شود. هنگام دریافت، مقدار Hash یک‌طرفه از بسته جدا می‌شود و سمت گیرنده، Hash مربوط به خود را اجرا می‌کند. چون Hash بر روی متغیرهای داخل بسته مثل زمان ارسال‌شده، تعداد بایت‌ها و غیره اجرا می‌شود. مقدار Hash باید یکسان باشد، یعنی بسته تغییر نکرده است. اگر مقادیر متفاوت باشد، یعنی بسته دستکاری‌شده و IPSec در پارامترهای امنیتی خود تجدید نظر می‌کند.

۵.۹ تونل‌زنی دیتا

تونل‌زنی چیزی است که VPN برای ایجاز یک شبکهٔ خصوصی در انترنت، بر آن متکی است. اصولاً این فرایند، گرفتن یک بسته از داده و جاسازی آن در بستهٔ دیگر، قبل از ارسال در شبکه است. شبکه باید برای ورود و خروج از شبکه، پروتوکول بستهٔ بیرونی را بشناسد. تونل‌زنی برای فعالیت، سه پروتوکول نیاز دارد:

پروتوکول مسافر (Passenger Protocol): بستهٔ اصلی داده، معمولاً یک IP است که باید در یک VPN رمزنگاری شود. برای این کار پروتوکول‌هایی مثل IPX یا NetBEUI باید استفاده شود.

پروتوکول کپسوله‌کننده (Encapsulated Protocol):

پروتوکولی (T2TP, PPTP, L2F, IPSec, GRE) که دورهٔ دادهٔ اصلی قرار می‌گیرد (یعنی کپسول‌شدن). IPSec استندرد اصلی است که در این مرحله به‌عنوان پروتوکول کپسول‌شدن استفاده‌شده و اجازه می‌دهد، تمام بستهٔ مسافر، رمزنگاری و پشتیبانی شود. IPSec باید برای عملکرد مناسب، در هر سمت تونل پشتیبانی شود. پروتوکول کپسول‌کننده، اغلب رمزنگاری داده را انجام می‌دهد. همان‌طورکه می‌بینید، پروتوکول‌های مثل IPX و NetBEUI که معمولاً در انترنت ارسال نمی‌شوند، از این طریق می‌توانند، به‌شکل این منتقل شوند ویا می‌توانید، بسته‌یی به‌کار ببرید که از آدرس IP خصوصی داخل بسته‌یی استفاده می‌کند که آدرس IP منحصربه‌فرد جهانی را برای گسترش یک شبکهٔ خصوصی در انترنت به کارمی‌برد. تکنیک‌هایی‌که این پروتوکول‌ها را می‌سازند، با استفاده از GRE و IPSec کارمی‌کند.

پروتوکول حامل (Carrier Protocol): پروتوکولی که شبکه استفاده می‌کند و در آن معلومات سفر می‌کنند. بستهٔ اصلی پروتوکول مسافر، داخل پروتوکول کپسول‌کننده، کپسول‌شده و داخل پروتوکول حامل برای انتقال در شبکهٔ عمومی‌قرار می‌گیرد.

تونل‌زنی با VPN به‌خوبی کارمی‌کند، زیرا می‌توانید، از پروتوکول‌هایی استفاده کنید که در انترنت داخل یک پاکِت IP پشتیبانی نشده، ولی همچنان به‌شکل امن قابل ارسال هستند. در ابتدای انتقال با تونل VPN، یک بسته از داده‌ها از LAN مبدأ، با معلومات جدیدی کپسوله می‌شود، که باعث می‌گردد، شبکه‌های میانی آن را شناسایی کرده، تحویل بگیرند. پس از این کار و تکمیل انتقال، سرایند (Header) پروتوکول تونل‌زنی بازشده و بستهٔ اصلی برای تحویل، به LAN مقصد منتقل می‌شود.

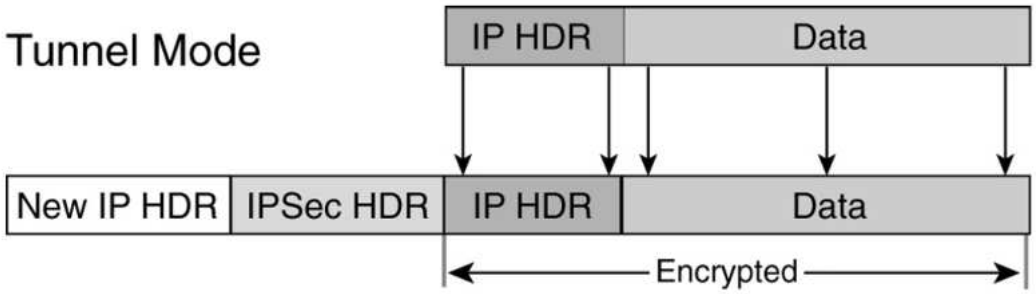
اگرچه تونل‌زنی باعث می‌شود، داده‌ها در شبکه‌های دیگر منتقل شوند، این کار به‌تنهایی حریم خصوصی ایجاد نمی‌کند. برای ایمن‌سازی انتقال تونلی در برابر تداخل و دستکاری، همه ترافیک VPNها رمزگشایی می‌شود. به‌علاوه، VPNها معمولاً ویژگی‌های دیگری مثل دیوار آتش در مرزهای بیرونی دارند. در VPNهای سایت‌به‌سایت، پروتوکول کپسوله‌کردن معمولاً IPSec یا GRE (Generic Routing Encapsulation) است. GRE شامل معلوماتی در مورد نوع بسته‌یی که کپسوله می‌شود و ارتباط بین کاربر و سرور است. تفاوت، به سطح امنیتی لازم برای ارتباط بسته‌گیر دارد و IPSec دارای عملکرد و امنیت که بیشتر نسبت به GRE است. IPSec می‌تواند، پاکِت‌های IP را تونل زده، رمزنگاری کند، درحالی‌که GRE می‌تواند، پاکِت‌های IP و غیر IP را تونل بزند. وقتی باید سیستم‌های غیر IP (مثل IPX) را از طریق تونل ارسال کنید، IPSec و GRE باید باهم به کار روند.

۵.۱۰ حالت‌های رمزنگاری

IPSec دو حالت رمزنگاری دارد: تونل و حمل. هر حالت از نظر عملکرد و میزان اضافه‌شده بالاسری و بستهٔ مسافر متفاوت است. این حالت‌های مختلف به‌طور خلاصه به این‌صورت هستند که تونل، سرایند بسته و محتویات هر بسته را رمزنگاری می‌کند، درحالی‌که، حمل فقط محتویات را رمزنگاری می‌کند.

۵.۱۰.۱ حالت تونل

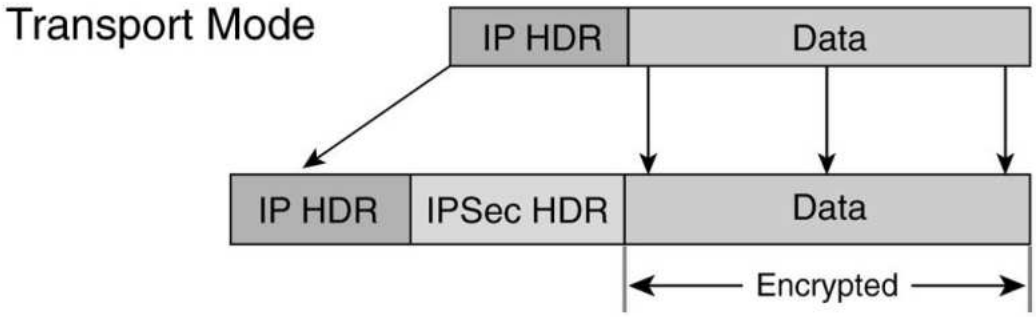
این یک راه عالی است که از طریق آن، IPSec بین دو PIX Firewall (یا هر دروازهٔ امنیتی دیگر) که در یک شبکهٔ ناامن مثل انترنت به یکدیگر متصل‌اند، به کار گرفته می‌شود. همه بحث‌های مربوط به IPSec در مورد حالت تونل خواهد بود. این حالت تمام بستهٔ IP را کپسوله و محافظت می‌کند. چون این حالت پاکِت‌ها را برای انتقال موفق و کپسوله و پنهان می‌کند، روتر رمزنگاری به‌خودی‌خود IP آدرس‌های را که در این سرایندهای جدید استفاده می‌شوند، مالک خواهد شد. حالت تونل با ESP یا AH یا هر دو قابل استفاده است. استفاده از این حالت منجر به افزایش حجم بسته تا ۲۰ بایت مربوط به سرایند IP خواهد شد. یک سرایند IP جدید باید برای بسته‌یی با سرایند جدید همانند شکل ۲۴ اضافه شود.



شکل ۵-۳ حالت تونل

۵.۱۰.۲ حالت حمل

این نوع استفاده از IPSec معمولاً برای ایجاد تأیید اعتبار کاربران راه دور VPN ویندوز ۲۰۰۰ با L2TP انجام می‌شود. این مفهوم در فصل ۵ بررسی شد بنابراین این فصل بر روی IPSec و حالت تونل متمرکز می‌شود. در این حالت، IPSec تمام بسته را رمزنگاری کرده، یک سرایند IP جدید در بسته می‌نویسد که معلومات مبدأ و مرجع اصلی را پنهان می‌کند. حالت تونل به این دلیل که تمام بسته و نه‌فقط محتویات آن رمزنگاری می‌شود، از حالت حمل ایمن‌تر است (شکل ۵-۴)



شکل ۵-۴ حالت حمل

۵.۱۱ پروتوکول‌های IPSec

IPSec از سه پروتوکول مکمل استفاده می‌کند که وقتی باهم استفاده می‌شوند، چارچوب استندرد و ایمنی تشکیل می‌دهند که برای VPNها ایده‌آل است. در اینجا سه پروتوکول شرح داده‌شده در استانداردهای IPSec آمده است:

پروتوکول مدیریت کلید مشارکتی امنیت انترنت (Internet Security Association-key Management Protocol-ISAKMP): که فاز تصمیم‌گیری ارتباط IPSec برای ایجاد VPN را شرح می‌دهد ???Oakley. روش ایجاد یک تبادل کلید معتبر را تعریف می‌کند. این روش حالت‌های مختلف داشته و می‌تواند، از طریق الگوریتم‌هایی مثل Diffie Hellman، مواد ایجاد کلید را فراهم کند. در این پروتوکول، تبادل کلید انترنتی وجود دارد که چارچوبی را برای تصمیم‌گیری پارامترهای امنیتی (مثل SA طول عمر، نوع رمزنگاری و غیره) و دقت کلیدها را ایجاد می‌کند.

پروتوکول امنیتی کپسول‌شده (Encapsulate Security Protoco –ESP) – پنهان بودن داده و محافظت به همراه تأیید اعتبار و خدمات شناسایی پاسخ را ارائه می‌دهد. ESP داده‌های کاربر را به‌طور کامل کپسوله می‌کند. ESP به‌تنهایی به همراه AH استفاده می‌شود. ESP با استفاده از پروتوکول DCP بر روی پورت‌های ۵۰ و ۵۱ اجراشده و در RFC، ۲۴۰۶ ثبت می‌شود.

سرایند تأیید اعتبار (Authentication Header-AH): خدمات تأیید اعتبار و ضد پاسخ را (به شکل اختیار) ارائه می‌دهد. AH خدمات محدود سرایند IP و سرایند توسعه‌یافته را ارائه می‌دهد؛ اما رمزنگاری داده از طریق اعمال یک Hash یک‌طرفه و ایجاد خلاصهٔ پیغامی از بسته را انجام نمی‌دهد. AH داخل داده‌هایی که باید پشتیبانی شوند (مثل یک داده‌نگار IP کامل) گنجانده می‌شود. AH می‌تواند، به‌تنهایی ویا به ASP استفاده شود. این پروتوکول توسط ESP جایگزین شده و غیر قابل استفاده محسوب می‌شود.

خلاصهٔ فصل پنجم

این فصل VPN و مزایایی را که برای شبکه به ارمغان می‌آورد، بررسی کرد. مهم‌ترین ویژگی استفاده از VPN، کاهش هزینه و مقرون به صرفه بودن آن است. کاهش هزینه‌های پهنای باند VPNها را یکی از مهم‌ترین راه‌حل‌های موجود کرده است. این فصل روی بهترین VPN موجود، یعنی VPNهای مبتنی بر IPsec متمرکزشده است. برای درک چگونگی محافظت VPNها از دیتا، این فصل سطوح، فازها و انواع فرایندهایی را که در رمزنگاری پاکِت دیتا در VPN مبتنی بر IPsec دخیل هستند، بررسی کرد.

سوالات فصل پنجم

۱. آیا می‌توان VPNهای رمزنگاری‌شده داشت؟

۲. سه نوع مختلف VPN کدامند؟

۳. سه ویژگی VPN را نام‌برده و شرح دهید که سازمان شما چگونه می‌تواند، از هر کدام سود ببرد؟

۴. متمرکزکننده‌های VPN برای کاربران بسیاری طراحی می‌شوند، تعداد و زمان استفاده را شرح دهید.

۵. آیا نرم‌افزار کاربردی VPN برای کمپیوتر ها، سیستم‌عامل قدرتمند جدید Apple یعنی، MAX OS X را پشتیبانی می کند؟

۶. تونل‌زنی دوگانه (Split Tunneling) چه موقع رخ می‌دهد؟

۷. در ارتباط با جریان داده‌ها، تأیید اعتبار در ایمن‌سازی آن چه نقشی ایفا می کند؟

۸. هنگام تونل‌زنی داده‌ها در IPsec، سه پروتوکولی که در فرایند ایفای نقش می کنند، کدامند؟

۹. در VPNهای سایت‌به‌سایت، دو پروتوکول جاسازی مختلف کدامند و تفاوت آنها چیست؟

فصل ششم

سیستم‌های شناسایی نفوذ

هدف کلی: محصلان با Intrusion Detection System(IDS) آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. سیستم‌های شناسایی حمله یا (IDS) را تعریف کنند.
۲. اهمیت IDS را در امنیت شبکه شرح دهند.
۳. نحوهٔ کارکرد IDS را توضیح دهند.

IDS یک سیستم محافظتی بوده که ترافیک شبکه را با جزئیات بیشتر نسبت به فایروال تحلیل می‌کنند. در این فصل با یکی از جدیدترین تکنالوژی‌های امنیتی یعنی سیستم شناسایی حمله (IDS) آشنا خواهیم شد که روی موضوعاتی چون انواع مختلف سیستم شناسایی حمله (IDS) و اهمیت آن همچنین عملکردهای اصلی سیستم شناسایی حمله و کارکرد آن و روش‌های مختلف برای شناسایی انواع حملات آن بحث خواهیم نمود.

۶.۱ چرا از (IDS) در شبکه‌های کمپیوتری استفاده می‌کنیم؟

سیستم‌های شناسایی نفوذ (IDS) نرم‌افزار و یا سیستم‌های مبتنی بر سخت‌افزار هستند که ورودی‌های شبکه و Host خود را بر اساس مجموعه‌یی از قوانین از پیش تعریف‌شده شناسایی می‌کنند. IDS های فعال تلاش می‌کنند تا با اقدامات مقابله‌یی که قبلاً در سیستم IDS برنامه‌ریزی شده‌اند از حملات جلوگیری کنند و یا حد اقل در هنگام حمله به مدیران مربوطه هشدار دهند.

نظر به دلایل ذیل از IDS در شبکه‌های کمپیوتری استفاده می‌کنیم:

- یک IDS نصب می‌کنید تا از ارتباط انترنتی شخص و آنهایی که می‌خواهند، از دیوار آتش (Firewall) شما رد شوند، مراقبت کنید.
- بر اساس نوع بسته و ارتباط و فعالیت‌هایی که این ارتباطات انجام می‌دهند، به IDS می‌گویید که به دنبال چه حملاتی باشد.
- به IDS می‌گویید که هر موقع چنین حملاتی پیش آمد، با یک e-Mail شما را مطلع کند.
- Uber Haxor پشت در کمپیوتر شما می‌آید، پورت‌ها (ports) را اسکن می‌کند (که خیلی هم عجیب نیست، چون کار خیلی واضحی می‌خواهد، انجام دهد) و اولین 1000 پورت Tcp را اسکن می‌کند.
- IDS در می‌یابد که اتصال‌ترتیبی همۀ پورت‌ها را امتحان می‌کند، پایگاه‌های دادۀ آن‌ها را کنترول می‌کند و به دنبال رفتاری مطابق آنچه شما برایش تعریف کرده‌اید، می‌گردد که چطور با port scan برخورد کند.
- IDS همزمان هم تلاش می‌کند، شما را مطلع کند و هم به شما e-Mail بفرستد.
- ناگهان، اسکن‌شدن پورت‌ها افزایش می‌یابد و از اطراف یک منبع دیگر هم این کار شروع می‌شود.
- IDS از این موضوع هم شما را مطلع می‌کند.

حالا IDS شما از هر لحاظ آماده است. شبکۀ شما را بیست‌وچار ساعته مراقبت می‌کند و در اولین لحظه و اولین نشانه از هرگونه خطر شما را مطلع می‌کند.

تا اینجا همه چیز خوب است، تا به حال هیچ نقصی در این سیستم دیده نشده است.

اول این‌که، IDS در آن واحد فقط یک رابط (Interface) را می‌تواند، مراقبت کند.

دوم این‌که، IDS فقط شرایطی را که شما تعیین کنید، مورد مراقبت قرار می‌دهد و برای حملات "double-reverse Twinkie" برنامه‌ریزی نشده است و اگر چنین حمله‌یی رخ می‌دهد، شما را مطلع نمی‌کند.

در آخر این‌که، یک IDS می‌تواند شریک هکرها شود. می‌گویید، ناممکن است؟ چند بار تا به حال شده که وقتی آژیر دزدگیر ماشین شما به صدا در می‌آید، نیمه‌شب از خواب بلند شده، ماشین خود را نگاه کنید. همین وضعیت برای IDS هم پیش می‌آید، اگر «پیجر» شما پر از پیام‌هایی شود که از طرف IDS فرستاده شده، آنگاه فکر می‌کنید که همهٔ پیام‌ها اشتباه بوده و در این بین ممکن است که پیام‌های واقعی را از دست بدهید.

رمز به‌کارگیری موفق یک IDS، تنظیم دقیق آن است. IDS ابتدا باید در یک آزمایشگاه امتحان شود و مشخص گردد که در یک ترافیک معمولی آیا IDS اخطار می‌دهد یا خیر و آنگاه باید حساسیت IDS را کم کنیم، لازم است شرایطی فراهم شود که در برابر هر اتفاقی اعلام خطر نکند. اغلب افراد انتظار دارند، از کوچکترین اتفاقی با خبر باشند که این واقع‌گرایانه نیست، IDSها کامل نیستند و گاهی به اشتباه، تهدیدها را نادیده می‌گیرند. بیایید، نگاهی به ملزومات شناسایی حملات بیندازیم.

۶.۲ مفهوم IDS

IDS مخفف عبارت Intrusion Detection System به‌معنای سیستم کشف نفوذ می‌باشد، به‌منظور نظارت بر تمامی‌فعالیت‌های ورودی و خروجی شبکه و شناسایی هرگونه فعالیت مشکوک طراحی شده است. این فعالیت‌های مشکوک ممکن است، نشان‌دهندهٔ یک حمله به سیستم یا شبکه توسط شخصی که در تلاش است تا سیستم امنیتی را در هم بشکند، باشد. IDS یک سیستم مانیتورینگ غیر فعال (Passive) در نظر گرفته می‌شود، زیرا عملکرد اصلی یک IDS هشدار در مورد فعالیت‌های مشکوک در حال وقوع است و در متوقف‌کردن آن‌ها نقشی ایفا نمی‌کند. اساساً یک IDS ترافیک شبکه و دیتای شما را مورد بررسی قرار می‌دهد و حملات، موارد سوءِاستفاده و سایر نقاط آسیب‌پذیری را شناسایی می‌کند. IDSها می‌توانند، رویدادهای مشکوک را به چندین روش اطلاع‌رسانی کنند که شامل نمایش یک آلارم، درج در بخش رویدادها (Logs) یا حتا برقراری ارتباط (مثل تماس تلفنی) با مدیر سیستم می‌باشد. در برخی از موارد IDSها درخواست عیارسازی مجدد سیستم به‌منظور کاهش نفوذهای مشکوک را مطرح می‌کنند. یکی از کاربردهای IDS تشخیص‌ترافیک نامتعارف درحال‌ورود به شبکه و گزارش آن به مدیر سیستم است. IDS به‌طور خاص به دنبال فعالیت‌های مشکوک و رویدادهایی می‌باشد که ممکن است، از اثرات ویروس‌ها، کرم‌ها و هکرها باشند. این امر به‌وسیلهٔ جستجو در امضاهای نفوذ (گزارش‌های ذخیره‌شده از جزئیات ورود به سیستم) یا امضاهای حمله (Attack Signatures) که کرم‌ها و ویروس‌های گوناگونی را شناسایی می‌کنند، انجام می‌شود. اصلاح IDS گسترهٔ وسیعی از محصولات متنوع را در بر می‌گیرد. یک راهکار IDS می‌تواند، در قالب یک نرم‌افزار متن باز (Open Source) رایگان ویا به‌صورت یک نرم‌افزار امنیتی گران‌قیمت برای فروش ارائه شود. علاوه بر این برخی از IDS ها شامل برنامه‌های نرم‌افزاری و سخت‌افزاری می‌باشند که در نقاط مختلف از شبکه نصب شده، مورد استفاده قرار می‌گیرند.

IDS یک سیستم محافظتی است که خراب‌کاری‌های در حال وقوع روی شبکه را شناسایی می‌کند.

روش کار به‌این‌صورت است که با استفاده از تشخیص نفوذی که شامل مراحل جمع‌آوری معلومات، پویش پورت‌ها، به‌دست‌آوری کنترول کمپیوترها و نهایتاً هک‌کردن می‌باشد، می‌تواند، نفوذ خراب‌کاری‌ها را گزارش دهد و کنترول کند.

از قابلیت‌های دیگر IDS، امکان تشخیص ترافیک غیر متعارف از بیرون به داخل شبکه و اعلام آن به مدیر شبکه ویا بستن ارتباط‌های مشکوک و مظنون می‌باشد. ابزار IDS قابلیت تشخیص حملات از طرف کاربران داخلی و کاربران خارجی را دارد.

برخلاف نظر عمومی‌که معتقدند، هر نرم‌افزاری را می‌توان به‌جای IDS استفاده کرد، دستگاه‌های امنیتی زیر نمی‌توانند، به‌حیث IDS مورد استفاده قرار گیرند:

۱. سیستم‌هایی که برای ثبت وقایع شبکه مورد استفاده قرار می‌گیرند؛ مانند: دستگاه‌هایی که برای تشخیص آسیب‌پذیری در جهت ازکارانداختن سرویس ویا حملات مورد استفاده قرار می‌گیرند.
۲. ابزارهای ارزیابی آسیب‌پذیری که خطاها ویا ضعف در تنظیمات را گزارش می‌دهند.
۳. نرم افزارهای ضدویروس که برای تشخیص انواع کرم‌ها، ویروس‌ها و به‌طورکلی نرم‌افزارهای خطرناك تهیه شده‌اند.
۴. دیوار آتش (Firewall)
۵. میکانیزم‌های امنیتی مانند SSL، VPN و Radius و....

۶.۳ آیا IDS همان فایروال است؟

پاسخ این سؤال منفی است. به‌طور معمول IDS با فایروال اشتباه گرفته شده ویا به‌حیث یک جانشین برای آن در نظر گرفته می‌شود. درحالی‌که هریک به‌صورت مجزا به امنیت شبکه مربوط می‌باشند. فایروال نفوذها را به‌منظور جلوگیری از وقوع آنها جستجو می‌کند و دسترسی بین شبکه‌ها را به‌منظور توقف نفوذها محدود می‌کند، اما در مورد حملات درون شبکه اطلاع‌رسانی نمی‌کند. IDS یک نفوذ مشکوک را شناسایی می‌کند و اگر نفوذ انجام شد، به وسیلهٔ آلارم اطلاع‌رسانی می‌کند. همچنین IDSها حملاتی را که از درون یک سیستم آغاز می‌شوند، نیز مورد بررسی قرار می‌دهند. محافظت‌کننده‌های نفوذ به سیستم که مبتنی بر شبکه می‌باشند، می‌توانند، پاکِت‌هایی را که توسط قوانین (rule) سادهٔ فایروال نادیده گرفته می‌شوند، نیز شناسایی کنند. در حقیقت IDS جایگزینی برای یک فایروال یا یک آنتی‌ویروس قوی نیست. IDS می‌بایست به‌صورت ترکیبی با محصولات امنیتی مثل فایروال و آنتی‌ویروس در نظر گرفته شود تا بتوانند، به‌صورت یک مجموعه، امنیت شبکه را افزایش دهند. به‌طور کل می‌توان تفاوت IDS و فایروال را در این دانست که IDS با جزئیات بیشتری نسبت به فایروال‌ترافیک شبکه را مورد بررسی قرار می‌دهد و بر خلاف فایروال که تنها ترافیک ورودی و خروجی را ارزیابی می‌کند، IDS ها ترافیک‌های درون سیستم را نیز مورد بررسی قرار می‌دهند.

به دلایل زیر دیوارهای آتش نمی‌توانند، امنیت شبکه را به‌طور کامل تأمین کنند:

۱. چون تمام دسترسی‌ها به انترنت فقط از طریق دیوار آتش نیست.
۲. تمام تهدیدات خارج از دیوار آتش نیستند.
۳. امنیت کمتر در برابر حملاتی که توسط نرم‌افزارهای مختلف به معلومات و دیتای سازمان می‌شود، مانند Active، Java Applet، Virus Programs.

۶.۴ ملزومات اولیهٔ شناسایی حمله

همه شبکه‌ها برای اشتراک‌گذاری اطلاعات طراحی می‌شوند و تنها بخش کوچکی از این طراحی به امنیت آن اختصاص دارد. بسیاری از تجارت‌ها از شبکه‌های مبتنی بر IP، مثل انترنت استفاده می‌کنند تا دفاتر، کارگران و شرکای راه دور خود را وارد محیط‌های شبکه‌های مطمئن داخل شرکت خود کنند. انترنت هر روز بزرگ و بزرگتر می‌شود و نقاط بیشتری را به یکدیگر متصل می‌کند. هر چه انترنت مطمئن‌تر شود، شرکت‌ها راحت‌تر می‌توانند عملکرد خود را به اشترا ک بگذارند. واضح‌ترین مثال وابستگی همه چیز به ما HTML است؛ اگرچه این امر تعامل را افزایش می‌دهد، عملکردهای جاری را راحت می‌کند، هزینه‌ها را کاهش می‌دهد و مزایای رفاهی را افزایش می‌دهد، در عین حال خطر و قیمت بالایی نیز دارد.

دسترسی آسان به انترنت، آن را به ابزار تجاری قوی و درعین‌حال به یک خطر بزرگ تبدیل کرده است، انترنت برای ارتباط و اشتراک طراحی شد، نه برای محافظت و ایمن‌سازی پرتال‌ها و سایت‌هایی که کاربران، مشتریان سایت‌ها و شرکای تجاری راه دور را وارد شبکه‌های مطمئن داخلی می‌کنند، مهاجمانی را که قصد سوءِ استفاده دارند، نیز ممکن است، به داخل شبکه راه دهند.

سؤال این است که این ارتباطات پراهمیت چگونه باید از یک واسطهٔ (Medium) ناامن مثل انترنت در امان باشند؟ این کتاب ابزارهای متخلفی را برای افزایش امنیت این منابع از طریق افزایش لایه‌های امنیتی معرفی کرده است. رایج‌ترین لایه‌های امنیتی در یک شبکه، یک بستهٔ روتر انترنتی و یک دیوار آتش مناسب هستند. اما سازمان شما هم یک سرور e-mail و هم یک وب‌سرور دارد که برای عملکرد، از طریق انترنت قابل دسترسی می‌باشند. شما نمی‌توانید، این ترافیک را ببینید چون تجارت شما به آن وابسته است. همچنین می‌دانیم که با رشد انترنت، حملات نیز رشده کرده و حرفه‌یی‌تر شده؛ اما سطح دانش لازم برای انجام این حملات کاهش یافته است.

نه روتر و نه دیوار آتش نمی‌توانند، بگویند که پاکِت‌های www در واقعیت شامل یک خطر یا حمله هستند یا خیر. متأسفانه بسیاری مردم به این تجهیزات اعتماد می‌کنند که در زمینهٔ شناسایی گاهی دچار کمبود می‌شوند. شاید سازمان شما یک مسئول سیستم حرفه‌یی دارد که می‌تواند، با فرایندها و سیاست امنیتی، سرورهای تجاری حیاتی و مهم را در برابر حملات، ایمن‌سازی می‌کند. هیچ یک از راه‌حل‌های امنیتی که تاکنون اشاره شد، نیاز به شناسایی حملات و هجوم‌ها را مدنظر قرار نداده‌اند.

در اصطلاحات انترنتی، شناسایی تهاجم هنوز جوان است. تحقیقات در دهۀ ۱۹۸۰ با تلاش‌ها و نوشته‌های Anderson و Denning آغاز شد. در دهۀ ۸۰ دولت ابتدا از عملکردهای پایه‌یی IDS استفاده کرد که بعدها ARPANET نامگذاری شد. پس از آن، اعضای پروژۀ Haystack لابراتوارهای Haystack را به‌حیث یک اقدام تجاری در زمینۀ ایجاد شناسایی تهاجم مبتنی بر میزبان (Host) تشکیل دادند. شناسایی تهاجم مبتنی بر شبکه، در دهۀ ۹۰ با تحقیقات Todd Heberlein در این زمینه همراه بود. تا آن هنگام، سازمان‌های بسیاری در حال ایجاد ابزارهای IDS بودند، نظیر لابراتوارهای Haystack و SAIC. سیستم سنجش خودکار امنیت (ASIM) نیروی هوایی امریکا و تیمی‌که این راه‌حل را تشکیل داد، در سال ۱۹۹۴ گروه Wheel را تشکیل دادند.

این موضوع به بحث ما مربوط است زیرا در سال ۱۹۹۴، سیسکو گروه Wheel را خرید و این کار هستۀ IDS سرویس‌های امنیتی را شکل داد.

انگیزۀ یک مهاجم، چه چالش فکری باشد، چه جاسوسی، سیاسی، مالی ویا حتا ایجاد مزاحمت، به هر حال شبکۀ شما مورد حمله قرار گرفته است. نظارت این حملات نه‌تنها کاری معقول است، بلکه در برخی موارد یک ضرورت تجاری نیز هست. در اوایل دهۀ ۹۰ محصولات جدید کم‌کم به این جنبۀ امنیت شبکه پرداختند: سیستم شناسایی تهاجم (IDS). یک مثال IDS یک سسیتم اخطار برای شبکۀ شما است. شبکه محافظت می‌شود اما بدون وجود IDS شما هرگز متوجه نخواهید شد که آیا قصدی برای حمله به شبکۀ شما وجود داشته یا خیر. هدف شناسایی تهاجم، کنترول بخش‌های شبکه و شناسایی رفتارهای غیرمعمول، فعالیت‌های نامناسب و حملات ویا متوقف‌کردن این حملات حتا ارائۀ اطلاعاتی برای دستگیری و مجازات مهاجمان می‌باشد.

IDS در بخش‌های مختلفی در یک شبکه قابل اجرا است. در کل، دو شکل اساسی IDS به‌کار می‌رود؛ IDS مبتنی بر شبکه و مبتنی بر میزبان، هر دو نوع، تکنیک‌های مختلفی برای شناسایی و جلوگیری از فعالیت‌های مشکوک ارائه می‌دهند و هر دو استراتژی‌هایی برای ارتقای لایه‌های امنیتی فراهم می‌کنند.

NIDS (Network-Based Intrusion Detection System): این سیستم به‌طور مستقیم بر روی شبکه ساکن شده، تمام‌ترافیکی را که از شبکه عبور می‌کند، مراقبت می‌کند. NIDS هم برای ترافیک‌های ورودی و خروجی، و هم برای ترافیک بین میزبان‌ها و اجزای شبکه‌های داخلی مؤثر هستند. NIDSها معمولاً در جلو و پشت دیوارهای آتش و پورت‌های VPN قرار گرفته، اثربخشی این تجهیزات امنیتی را سنجیده و به آنها برای عمل‌بخشیدن به امنیت شبکه تعامل می‌کنند.

HIDS (Host-Based Intrusion Detection system): این سیستم‌ها عملکردهای نرم‌افزاری تخصصی هستند که بر روی کمپیوتر (سرور) نصب می‌شوند تا تمامی ترافیک ارتباطی ورودی و خروجی از آن را مراقبت کرده، سیستم فایل را از لحاظ تغییرات، نظارت کنند. HIDS در سرورهای

قابل‌دسترسی از طریق انترنت و سیستم‌های حیاتی مثل سرورهای وب e-mail به شدت مؤثرند، زیرا علمکردها را در مبدأ مراقبت کرده، از آنها محافظت می‌کنند.

NIDS و HIDS برای دفاع چند لایهٔ مؤثر و قرار گرفتن در دید و کنترول ارتباطات یک سازمان، باید همواره باهم استفاده شوند. IDS ها برای سیستم‌های امنیتی سازمان حالت کنترول و تعادلی اثربخش فراهم کرده، اثربخشی کلی هزینه‌های صرف‌شده برای امنیت را بالا می‌برند، بخش بعدی قابلیت‌های کلی یک IDS را بررسی می‌کند.

۶.۵ نگاهی بر عملکرد IDS

IDSهایی که در بازار امروز موجودند، قابلیت‌ها و ویژگی‌های فراوانی دارند، هنگام ارزیابی یک IDS برای سازمان خود، قابلیت‌های زیر را جدا از موارد مرسوم باید در نظر بگیرید:

ارتباط متقابل وقایع: وقتی یک IDS در یک شبکهٔ شلوغ با IDSهای چندگانه نصب می‌شود، قابلیت ایجاد ارتباط بین وقایع (حملات) برای اطیمنان از این‌که شبکه‌های شما امن هستند، ضروری می‌باشند. در نظر داشته باشید که یک حمله می‌تواند از اجزای چندگانه استفاده کند و وقتی یک میزبان تأمین شد، از آن برای حمله به دیگری استفاده می‌شود. همین‌طور تا آخر، بدون این ایجاد ارتباط بین وقایع، آن حمله سردرگمی زیادی فراهم کرده، برای برطرف‌کردن علت آن، زمان و منابع بسیار زیادی باید صرف شود. ایجاد ارتباط به مدیر IDS امکان می‌دهد تا حمله را به سرعت ردیابی کرده، وقایعی را که در حسگرهای چندگانه در زیر شبکه‌های مختلف نصب شده‌اند، ویا حتا در مکان‌های جغرافیایی متفاوت و در دوره‌های زمانی پیشتر وجود دارند، با یکدیگر مرتبط کنند.

مدیریت حسگر متمرکز: داشتن یک IDS که بتواند وقایع را با یکدیگر مرتبط کند، مهم است و مدیریت همه IDSها از طریق مدیریت متمرکز نیز بسیار حیاتی است. درواقع، هر وسیله (سرور – روتر – دیوار آتش) فهرست وقایع را ایجاد می‌کنند؛ اما این فهرست‌ها به‌ندرت حتا کنترول می‌شوند. بنابراین داشتن یک قالب مدیریت متمرکز که بتواند در حسگرهای مختلف، کنترول پاسخ و ایجاد ارتباط بین وقایع را داشته باشد، و قابلیت ارائهٔ گزارش جامع در مورد امنیت شبکهٔ شما را داشته باشد، برای موفقیت شما ضروری است.

شخصی‌سازی علائم: عملکردهای ویژهٔ تجاری ویا شرکت، نرم‌افزارهای آبدیت‌شده، سیستم عامل‌های جدید، ویروس‌ها و هکرهای باهوش، همواره به دنبال کشف آسیب‌پذیری‌های جدید هستند. همیشه بین کشف یک آسیب‌پذیری جدید و ارائهٔ یک نشانهٔ (signature) جدید توسط تولیدکنندگان IDS که بتوانند حمله‌یی را که از آن آسیب‌پذیری سوءِاستفاده کرده است، شناسایی کنند، تأخیر وجود دارد. بنابراین، یک IDS باید به سازندگان و مدیران امکان خلق علامت‌های حمله را برای ماقبل با هرگونه آسیب‌پذیری بدهد.

حذف اشتباهات نادیده‌گرفته‌شده: همانند هرگونه سیستم عامل دیگر (مثل ویندوز) که هنگام انتشار تمام ویژگی‌های آن فعال شده است، تجهیزات IDS نیز چنین هستند، به عبارت دیگر، هنگام استفاده برای

اولین بار بیش از حد حساس هستند و درنتیجه موجب ترس، عدم اطمینان و شک (FUD – Fear, uncertainty, and doubt) در مورد امنیت شبکهٔ شما می‌شوند. بنابراین بهتر است بدانید که هر IDS خوب باید بتواند، این ایجاد ترس‌های بی مورد را حذف کند. البته باید دقت کنید که فقط به‌شرطی باید تشخیص‌های اشتباه را حذف کنید که مطمئن هستید، و در این صورت هم باز بیست‌وچار ساعت منتظر بمانید.

به‌کارگیری مبتنی بر استندرد: یک جنبهٔ مهم به‌کارگیری هر تکنولوژی، انتخاب عملکردی می‌باشد که مبتنی بر استندردهاست، بسیاری از تولیدکنندگان محصولاتی ایجاد می‌کنند که خدمات امنیتی فوق‌العاده‌یی را ارائه می‌دهند؛ اما تعداد کمی از محصولات با یکدیگر همخوانی دارند ویا چارچوبی برای کابردهای آینده ارائه می‌دهند. IDS هم از این قاعده مستثنا نیست و استندردهای کمی در حال حاضر موجود هستند. از آنجایی که مهم‌ترین جنبهٔ یکپارچگی IDS و مدیریت آن، قابلیت‌های گزارش‌دهی آن است، استندردی بر اساس دیتابیس آسیب‌پذیری و خطرات رایج (CVE) به وجود آمده است. بانک بر اساس دیتابیس CVE، آسیب‌پذیری‌ها را به‌شکل یک سیستم مرجع طبقه‌بندی و گروه‌بندی می‌کند. سازگاری CVE برای IDS مهم است، زیرا قابلیت‌های گزارش‌دهی ارائه می‌دهد که فراتر از توانایی‌های گزارش‌دهی رایج IDS است. با یکپارچگی IDSهای سازگار با CVE، سازمان‌ها می‌توانند، از دیگر ابزارهای سازگار CVE، مثل ابزارهای ارزیابی آسیب‌پذیری (VA) که برای ارتقای دقت و حساسیت گزارش خطر است، استفاده کنند. CVE از پذیرش روزافزون برخوردار است و به روشی استندرد برای گزارش‌دهی و تقسیم‌بندی و طبقه‌بندی خطرات امنیتی تبدیل شده است.

عملکرد جلوگیری از حمله: جلوگیری از حمله لزوماً قابلیت پاسخ فعال به حمله و جلوگیری از آن و جلوگیری از ترافیک ناخواسته می‌باشد. عبارت جلوگیری از حمله اخیراً موجب سردرگمی‌هایی شده و اغلب به‌حیث یک تکنالوژی رقابتی در شناسایی حمله به بازار عرضه می‌شود؛ اما عکس این قضیه صحت دارد: در بازار امروز یک IDS باید از قابلیت پاسخ فعال به تهدیدهای مشکوک برخوردار باشد.

تطبیق امضاها: این قابلیت تمام ترافیک عبور از شبکه را چک کرده، هر پاکِت یا مجموعه‌یی از پاکِت‌ها را با الگوهای حمله (امضاها) مطابقت می‌دهد. سپس IDS به هر حمله به‌شکل فعال یا غیر فعال پاسخ می‌دهد. این پاسخ می‌تواند یک اخطار SNMP، ارسال یک e-mail اخطاری ویا متوقف‌کردن حمله‌کننده باشد (که جلوگیری از حمله نیز گفته می‌شود).

شناسایی نامحسوس: سناسایی نامحسوس به IDS امکان می‌دهد تا یک خط پایه از الگوهای ترافیکی و جریانات اطلاعاتی معمول ایجاد کند و هرگاه مرزهای عادی شکسته شدند (مثلاً یک پروتوکول جدید بر روی شبکه شناسایی شد)، پاسخ دهد. این نوع شناسایی هنگامی به حد اکثر اثربخشی می‌رسد که با رمزگشایی پروتوکول همراه باشد. ازاین‌طریق، IDS رفتارهای طبیعی مورد نظر را می‌شناسد و اگر دستوری یا درخواستی غیرعادی دریافت شود، واکنشی نشان می‌دهد. همیشه در مورد IDSها و این واقعیت که آنها می‌توانند،

هرچیزی را مورد نظارت قرار دهند، یک سوءتفاهم وجود داشه است. این تصور درست نیست، داشتن یک IDS به‌حیث یک لایه در برنامهٔ امنیتی، ایدهٔ خوبی است؛ اما وابستگی به آن به‌حیث تنها راه‌حل، ایدهٔ خوبی نیست.

نفوذ به مجموعهٔ اقدامات غیر قانونی که صحت و محرمانگی یا دسترسی به یک منبع را به خطر می‌اندازد، اطلاق می‌گردد. نفوذها می‌توانند، به دو دستهٔ داخلی و خارجی تقسیم شوند. نفوذهای خارجی به آن دسته نفوذهایی گفته می‌شود که توسط افراد مجاز یا غیر مجاز از خارج شبکه به درون شبکهٔ داخلی صورت می‌گیرد و نفوذهای داخلی توسط افراد مجاز در سیستم و شبکهٔ داخلی، از درون خود شبکه انجام می‌پذیرد. نفوذگرها عموماً از عیوب نرم‌افزاری، شکستن کلمات رمز، شنود میزان تردد در شبکه و نقاط ضعف طراحی در شبکه، سرویس‌ها یا کمپیوتر های شبکه برای نفوذ به سیستم‌ها و شبکه‌های رایانه‌یی بهره می‌برند.

به‌منظور مقابله با نفوذگران به سیستم‌ها و شبکه‌های رایانه‌یی، روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ ایجاد گردیده‌است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکهٔ رایانه‌یی را بر عهده دارد. روش‌های تشخیص مورد استفاده در سیستم‌های تشخیص نفوذ، به دو دسته تقسیم می‌شوند:

۱. روش تشخیص رفتار غیر عادی (anomaly detection)؛
۲. روش تشخیص سوءِ استفاده یا تشخیص مبتنی بر امضا (misuse detection).

۶.۶ روش تشخیص رفتار غیر عادی

در این روش، یک نما از رفتار عادی ایجاد می‌شود. یک ناهنجاری ممکن است نشان دهندهٔ یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه‌های عصبی، تکنیک‌های یادگیری ماشین و حتا سیستم‌های ایمنی زیستی استفاده می‌شود. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آنها پیدا کرد. رفتارهایی که از این الگوها پیروی می‌کنند، عادی بوده، رویدادهایی که انحراف بیش از حدمعمول آماری از این الگوها دارند، به‌حیث رفتار غیر عادی تشخیص داده می‌شوند. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استندرد انحراف از آمار عادی به وقوع می‌پیوندد، غیر عادی فرض می‌شود. به‌حیث مثال اگر کاربری به‌جای یک یا دو بار ورود و خروج عادی به سیستم در طول روز، بیست بار این کار را انجام دهد، یا رایانه‌یی که در ساعت ۲:۰۰بعد از نیمه شب مورد استفاده قرار گرفته، درحالی‌که قرار نبوده، کمپیوتر فوق پس از ساعت اداری روشن باشد. هر یک از این موارد می‌توانند، به‌حیث یک رفتار غیر عادی در نظر گرفته شوند.

۶.۷ روش تشخیص سوء استفاده یا تشخیص مبتنی بر امضا

در این تکنیک که معمولاً با نام تشخیص مبتنی بر امضا شناخته شده‌است، الگوهای نفوذ از پیش ساخته‌شده (امضا) به‌صورت قانون نگهداری می‌شوند. طوری‌که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته،

درصورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می‌شود. در این روش‌ها، معمولاً تشخیص‌دهنده دارای دیتابیسی از امضاها یا الگوهای حمله‌است و سعی می‌کند با بررسی ترافیک شبکه، الگوهای مشابه با آنچه را که در دیتابیس خود نگهداری می‌کند، بیابد. این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته‌شده می‌باشند و درصورت بروز حملات جدید در سطح شبکه، نمی‌توانند، آن‌ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سیستم تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آنها عیناً به سیستم داده شده‌است.

۶.۸ معماری سیستم‌های تشخیص نفوذ

معماری‌های مختلف سیستم تشخیص نفوذ عبارتند از:

۱. سیستم تشخیص نفوذ مبتنی‌برمیزبان (HIDS)؛
۲. سیستم تشخیص نفوذ مبتنی‌برشبکه (NIDS)؛
۳. سیستم تشخیص نفوذ توزیع‌شده (DIDS).

۶.۸.۱ سیستم شناسایی حملات شبکه‌یی (NIDS)

سیستم‌های شناسایی حملات شبکه‌یی، همهٔ پاکِت‌ها در یک قسمت شبکه را دریافت می‌کنند. این کار مثل سیستم حسگر پاکِت است، اما تفاوت پس از دریافت ویا حس‌شدن پاکِت مشخص می‌شود. NIDSها براساس مفهوم شنود، بنا شده‌اند و به دو شکل مختلف می‌توان آنها را به‌کار گرفت. این روش‌ها برای مقابله با سویچ‌های LAN و نیز برای چگونگی ایزوله‌کردن ترافیک توسط آنها طراحی شده است. یک IDS باید تا حد ممکن بتواند، بخش زیادی از ترافیک را ببیند تا بتواند، مؤثر باشد. دو روش متفاوت NIDS به شرح زیرند:

- **شنود داخل خط (Inline wiretap)**: این روش دریافت پاکِت‌ها، یک شنود فزیکی بین دو وسیله از شبکه قرار می‌دهد، NIDS به این شنود وصل می‌شود.
- **انعکاس پورت (Port mirroring):** بسته به نوع سویچی که استفاده می‌کنید، انعکاس پورت که به چرخش پورت (port spanning) نیز معروف است، می‌تواند، یک راه‌حل انعطاف‌پذیر باشد. این تکنیک به سویچ فرمان می‌دهد که از هر پاکِتی که مثلاً قرار است، به پورتی (Port) که دیوار آتش (Firewall) شما به آن متصل است، فرستاده شوند، یک کاپی به پورت دیگر ارسال کند. NIDS به این پورت انعکاس متصل است.

بعد از این‌که NIDS پاکِت‌ها را می‌خواند، پاکِت‌ها به روش‌های متخلفی تحلیل می‌شوند، که این، به نوع NIDS مورد استفاده بستگی دارد. برخی NIDSها با مقایسهٔ پاکِت با نشانه‌های حمله‌یی که در دیتابیس خود دارند، به دنبال یک اثر انگشت یا رد پا می‌گردند؛ درحالی‌که دیگر سیستم‌ها به دنبال فعالیت غیرمعمول هستند که می‌تواند، نشانگر شروع یک حمله باشد. یکی از مزایای NIDS این است که به محض نصب، غیر قابل ردیابی بوده، نامرئی می‌شود.

مواردی مربوط به سرعت و تغیرپذیری وجود دارند که هنوز صنعت IDS با آن دست و پنجه نرم می‌کند. NIDSها با افزایش سرعت شبکه‌ها و ورود GigEthernet به شبکه‌ها در هر اندازه‌یی، در مقیاس‌بندی به مشکل برخورده‌اند، به‌زودی سرعت‌های بالای ده گیگابایت استفاده خواهند شد. البته NIDSها باید هر پاکِت را دریافت کرده، تمام اجزای آن را تحلیل کند. این موضوع باعث می‌شود که سرعت بالا مشکلی باشد که هنوز حل نشده است؛ افزون‌براین، به‌روزرسانی امضاهای حمله هنوز به جایی نرسیده که بتواند جدیدترین حملات را شناسی کند. واضح است که فروشندگان IDS و چگونگی به‌روزرسانی امضا توسط آنها، بسیار دورتر از جایی هستند که انتی‌ویروس‌ها رسیده‌اند. اخیراً سیسکو یک ماژول برای سویچ ۶۰۰۰catalyst روانهٔ بازار کرده است که شناسایی حملهٔ شبکه‌یی را به‌طور مستقیم در سویچ به‌کار می‌گیرد که هنگام گرفتن پاکِت‌ها دقت را افزایش می‌دهد.

نصب و به‌کارگیری NIDS به‌طور کامل به طراحی فعلی شبکه و معماری‌تان در هر نقطه بستگی دارد. هرچه اجزای شبکه بیشتر باشد، تعداد مکان‌های قرارگیری NIDSها معمولاً بهتر تعیین می‌شود.

جاگذاری معمول NIDSها به آنها این مکان را می‌دهد تا در محیط پیرامون شبکه مثل دو سمت دیوار آتش (سمت داخلی و خارجی)، نزدیک به سرور و روی لینک‌های شبکه‌های شریک تجاری بیشترین اثربخشی را داشته باشند، این جایگذاری به سازمان امکان می‌دهد تا اثربخشی واقعی روترهای پیش اسکن‌کننده و دیوار آتش را بسنجند. این لینک‌ها بهتر است، پنهای باندهای کمی‌داشته باشند (سرعت‌های IT)، به گونه‌یی که یک IDS بتواند ترافیک را مدیریت کند. این کار سنجش خوبی از کنترول‌ها و بالانس‌ها ارائه داده و برای سازمان‌های مطلع از امنیت که در آنها سرورها در پشت دیوار آتش به انترنت دسترسی دارند، ایده‌آل است. یک نکتهٔ باارزش دیگر، همخوانی با بدنه و استخوان‌بندی WAN است. یک مشکل رایج هک‌کردن شبکهٔ اصلی شرکت از نقاط دور از شبکه است. چون لینک‌های WAN پهنای باند کمی دارند، NIDS می‌تواند، بسیار سودمند باشد.

یک عمل امنیتی خوب می‌گوید که هنگام درنظرگرفتن یک راه‌حل IDS، هر دو NIDS داخلی و خارجی باید استفاده شوند. این، NIDSها را قادر می‌سازد تا حملات را از تهدیدهای داخلی و تهدیدهای انترنتی کنترول کند. داشتن دو NIDS کمی عجیب به نظر می‌رسد، اما به یاد داشته باشید که به لحاظ آماری اکثریت حملات از منابع داخلی هستند. نادیده‌گرفتن هریک از این دو مکان، اثربخشی IDS را کاهش می‌دهد.

۶.۸.۲ سیستم شناسایی حملهٔ مبتنی بر میزبان (HIDS)

سیستم‌های شناسی حملهٔ مبتنی بر میزبان (HIDS)، حمله‌های انجام‌شده به سمت یک میزبان مشخص را کنترول و شناسایی کرده، به فعالیت سیستم و کاربر پاسخ می‌دهند. برخلاف NIDSها، HIDSها بر روی میزبانی مثل وب یا سرور e-mail که باید کنترول شود، نصب می‌شود. HIDS، فهرست رویدادها و آزمایشی‌های میزبان را کنترول می‌کند، درحالی‌که یک NIDS پاکِت را کنترول می‌کند. به‌جای تلاش برای

شناسایی محتوای پاکِت‌ها در برابر امضاهای حمله، روش HIDS تلاش می‌کند که الگوهای شناخته‌شدهٔ کاربران لوکال و راه دوری را که مشغول به کارهای ممنوع و غیر قانونی هستند، شناسایی کند.

NIDS با پاکِت‌های ردوبدل‌شده از میزبان و به سمت میزبان در یک شبکه سروکار دارد، درحالی‌که HIDS ها با آنچه در خود میزبان رخ می‌دهد، از طریق کنترول و فعالیت لاگ‌ها (Log) سروکار دارد. یک NIDS همانند یک مسئول پارکینگ است که مراقب تمامی موترها در روی پارکینگ و خروجی از آن است؛ درحالی‌که HIDS بیشتر شبیه یک کارمند است که فقط به فضایی که شما موتر خود را در آن پارک کرده‌اید، توجه دارد.

HIDS بیشتر مانند یک نرم‌افزار آنتی‌ویروس عمل می‌کند (البته جایگزین آنها نیست) و دارای قابلیت‌های بسیار زیادی است که سطح امنیتی را افزایش می‌دهد. HIDS برای مقابله با تهدیدهای امنیتی علیه میزبان (Host) بهترین گزینه است، چون می‌تواند، به علمکردهای خاص کاربران پاسخ داده، آن‌ها را کنترول کند و همین‌طور دسترسی به فایل‌های روی سرور را نیز تحت نظر دارد. اغلب تهدیدهای کمپیوتری از منابع بسیاری مثل کارمندان ناراضی یا جاسوسانی از داخل سازمان ایجاد می‌شود. HIDS ها سرورها را با فراهم‌کردن اطلاعاتی مربوط به موارد زیر کنترول می‌کنند:

- تلاش‌های تهاجمی و رفتارهای مشکوک کاربران حقیقی؛
- اسکن میزبان‌ها برای اطمینان از این‌که با عملکردهای امنیتی سازگاری دارند.
- مدیریت سیاست تجهیزات و متمرکزسازی، تأمین دیتای قانونی، تحلیل آماری و پیشتیبانی شواهد و در مواقع خاص، تا اندازه‌یی کنترول دسترسی. معمولاً ابزارهای جدیدتر تمام این ویژگی‌ها را ارائه می‌دهند.

به‌کارگیری HIDS بسیار ساده است. این برنامه‌یی است که بر روی یک سرور مقیم می‌شود و تغییرات سیستم فایل، تغییرات Registry، پورت‌های باز، برنامه‌های درحال‌اجرا، و تمام ترافیک و ورودی و خروجی به میزبان خود را مراقبت می‌کند. معمولاً فارم‌های سرور (server farms) کاندیدهای خوبی برای HIDS هستند.

در جایی که میزبان‌های چندگانه مدنظرند، HIDS باید به‌گونه‌یی تنظیم شود که به یک کنسول مدیریت متمرکز گزارش دهد تا ارتباط متقابل وقایع و گزارش‌دهی کامل را فراهم کند. انتخاب‌ها و گزینه‌های معمول برای HIDS و به‌کارگیری آنها، سرورهای وب، سرورهای فایل ویا هرگونه سرور کاربری دیگر است که ارتباط منابع شبکه‌یی با انترنت عمومی را میسر می‌کند.

۶.۸.۳ سیستم تشخیص نفوذ توزیع‌شده (DIDS)

این سیستم‌ها از چندین NIDS یا HIDS یا ترکیبی از این دو نوع همراه یک ایستگاه مدیریت مرکزی تشکیل شده است. بدین‌صورت که هر IDS که در شبکه موجود است، گزارش‌های خود را برای ایستگاه

مدیریت مرکزی ارسال می‌کند. ایستگاه مرکزی وظیفهٔ بررسی گزارش‌های رسیده و آگاه‌سازی مسئول امنیت سیستم را بر عهده دارد. این ایستگاه مرکزی همچنان وظیفهٔ به‌روزرسانی پایگاه قوانین تشخیص هر یک از IDS های موجود در شبکه را بر عهده دارد. اطلاعات در ایستگاه مدیریت مرکزی ذخیره می‌شود. شبکه بین «ان‌آی‌دی‌اس‌ها» با سیستم مدیریت مرکزی می‌تواند، خصوصی باشد یا این‌که از زیرساخت موجود برای ارسال داده‌ها استفاده شود. وقتی از شبکهٔ موجود برای ارسال داده‌های مدیریتی استفاده شود، امنیت‌های اضافی به‌وسیلهٔ رمزنگاری یا فناوری شبکه‌های خصوصی مجازی (VPN) حاصل می‌گردد.

برای تشخیص خطرات و حملات احتمالی باید سیستم خود را در برابر تقاضاهایی که سرویس‌های نامناسب درخواست می‌کنند، مورد بررسی قرار دهید. این بررسی‌ها در تشخیص حملات واقعی به ما کمک می‌کند. باتوجه به انواع راه‌هایی که نفوذگران برای دسترسی به سیستم‌ها استفاده می‌کنند، نگاهی اجمالی به روش‌های آسیب‌رسانی و نفوذ می‌اندازیم.

- **استفاده از آسیب‌پذیری‌های معروف**: در اکثر موارد حمله به معنای تلاش برای استفاده از نقص یا ایجاد آن در سیستم امنیتی یك سازمان اطلاق می‌شود و این یکی از راه‌های نفوذگری در شبکه می‌باشد. اغلب خود سازمان ممکن است، از ابزاری برای امن‌ساختن شبکه استفاده کند که کار حمله‌کننده را آسان می‌سازد. به بیان واضح‌تر این‌که ابزارهای امنیتی نیز خود دارای نواقص و حفره‌های امنیتی می‌باشد که اختیارات بیشتری را به نفوذگر می‌دهد. این نرم‌افزارها اغلب مانند شمشیر دولبه عمل می‌کنند و مورد استفادهٔ هر دو گروه کاربران و حمله‌کنندگان قرارمی‌گیرد؛ مانند: نرم‌افزارهای کنترول صحت و یکپارچگی فایل یا نرم‌افزارهایی که جهت تست آسیب‌پذیری شبکه مورد استفاده قرارمی‌گیرند. چك‌کردن یکپارچگی فایل‌ها با استفاده از روش‌های سیستمی و با قابلیت ادغام روش‌های مختلف با یکدیگر و با ابزارهایی نظیر anti-SATAN یا Courtney امکان‌پذیر می‌باشد.
- **ترافیك خروجی غیر معمول**: یك نفوذگر با استفاده از تعداد زیادی Exploit و حتا نفوذهای ناموفق سعی در به‌دست‌آوردن کنترول کمپیوتر مقصد دارد. این عملیات نفوذگرانه، ترافیك معمول شبکه را افزایش می‌دهد و نشانهٔ وقوع یك حمله در آینده می‌باشد. هر ابزار تست آسیب‌پذیری می‌بایست قابلیت تشخیص فعالیت‌های مشکوك و غیر متعارف را داشته باشد و با ارائهٔ گزارش، اعلام خطر لازم را به مدیر شبکه بدهد.
- **حد تکرار برای کمك به تشخیص فعالیت‌های واقعی و مشکوك**: فعالیت‌های شبکه به‌وسیلهٔ دریافت و کنترول بعضی پارامترها قابل شناسایی است؛ مانند: User Profile یا از Session State.
- **زمان بین تکرار فعالیت‌ها:** پارامتری برای تشخیص زمان سپری‌شده بین دو واقعهٔ متوالی؛ مثلاً: وقتی بخواهید، با نام کاربری اشتباه وارد سیستم شوید، سه تلاش برای ورود با نام غلط بین فاصلهٔ زمانی ۲ دقیقه یك فعالیت مشکوك به نظر می‌رسد.

اشتباه در تایپ ویا جواب‌هایی که در یک Session ایجاد می‌شود.

پروتوکول‌ها وسرویس‌های شبکه به‌صورت کاملاً دقیقی مستند شده‌اند و از ابزارهای نرم‌افزاری خاص استفاده می‌کنند. هرگونه ناهماهنگی با قالب شناخته شده (مثل اشتباه در تایپ یک دستور) ممکن است معلوماتی برای شناسایی سرویس‌هایی که می‌توانند، مورد حملهٔ یک نفوذگر قرار بگیرند، باشد. اگر امکان Audit در سیستم فعال شده باشد، مثل Send Mail Relaying، توالی ارتباط Log به‌صورت معمولی و قابل پیش‌بینی اتفاق می‌افتد. هرچند که اگر در Log دریافت‌شده دستورات غیر مجاز دیده شود، ممکن است، نتیجهٔ موارد اشتباه غیر عمدی ویا سعی در Spoofing باشد. (Spoofing بدین معناست که نفوذگر آدرس خود را به آدرسی که برای سیستم شناخته‌شده است، تغییر داده و به این ترتیب به سیستم نفوذ می‌کند.)

تست تلاش‌های مخرب ممکن است، شامل موارد زیر باشد:

۱. شناسایی تلاش‌های متعدد برای جبران خطاهای تایپی و تکرار دستورات؛
۲. تشخیص خطاهای مکرر برای یافتن پروتوکول‌ها که بدنبال یك تلاش موفق انجام می‌شود.
۳. تشخیص خطا و یادگیری در جهت شناسایی نرم‌افزارها ویا سیستم‌عامل‌های موجود در سایت مقصد.
۴. ناهماهنگی در جهت ارسال و دریافت معلومات: هرگونه ناهماهنگی ترافیکی در Packet ها یا یك Session نشانه‌یی از یك حملهٔ پنهانی است. بررسی آدرس مبداء و مقصد (به‌صورت ورودی یا خروجی) می‌تواند جهت Packet را تشخیص بدهد. روند برقراری یك session با تشخیص اولین پیام ارسال‌شده شناسایی می‌شود. یك درخواست برای دریافت یك سرویس از شبکهٔ محلی به‌صورت یك session ورودی است و پروسهٔ فعال‌کردن یك سرویس بر پایهٔ Web از یك شبکهٔ محلی یك session خروجی است.

۶.۹ حملات چگونه شناسایی می‌شوند؟

هر فروشنده و تولیدکنندهٔ IDS اصطلاحات علمی ویژهٔ خود را دارد که در شرح چگونگی عملکرد IDS خود، FUD را به درد سر می‌اندازد. این امر مستلزم نگاهی دقیق به روش‌هایی است که هر IDS خوب باید به کار گیرد.

یک IDS روش به‌کارگیری ویژه‌یی از TCP/IP دارد که به آن امکان می‌دهد، پاکِت‌ها را جمع‌آوری کرده، سپس برای تحلیل، آن‌ها را مجدداً بازسازی (Reassemble) کند. ردیابی پاکِت‌ها به تنهایی کافی نیست. یک IDS باید آنها را آزمایش کند و این کار را به روش‌های گوناگون انجام می‌دهد که در بخش‌های بعد گفته خواهد شد.

۶.۹.۱ بازسازی مجدد جریان ارتباطی

یک IDS می‌تواند، جریان پاکِت‌ها را در هر جلسهٔ (session) ارتباطی بازسازی کرده، آنچه را که در واقعیت رخ می‌دهد، تحلیل کند. این فرایند حیاتی است، زیرا IDS را قادر می‌سازد تا وقایع را کنار یکدیگر

قرار داده، ارتباط متقابل مناسبی را برای ایستگاه مدیریت فراهم کند. این امر آنجا حیاتی‌تر می‌شود که مطالعات دریافته‌اند که دلیل اصلی کرم‌های انترنتی (worm) از جایی شروع می‌شود که کارمندان Laptopهای خود را به شبکهٔ کاربران متصل کرده، آن‌ها را آلوده می‌کنند و سپس آنها را به شبکهٔ شرکت می‌برند. بدتر این‌که کارمندان یک تونل VPN در شرکت درست می‌کنند و کنترول‌کننده‌های امنیتی کرم‌ها را دور می‌زنند. دلیل اصلی این است که کارمند، PC دفتر کار خود را از دیوار آتش (Firewall) عبور داده، و وارد شبکهٔ شرکت می‌شود؛ آن‌هم با یک کمپیوتر آلوده. چقدر خوب است که روی لپتاپ (Laptop)، HIDS داشته باشیم تا از این کار جلوگیری کنیم.

۶.۹.۲ تحلیل پروتوکول

حملات از روش‌های تغییر پروتوکول اطلاعات برای موفقیت خود استفاده می‌کنند. به‌حیث مثال، روش Ping of Death موفق است، زیرا اندازهٔ پاکِت را تغییر می‌دهد و از طریق مطابقت پروتوکول این کار قابل شناسایی است. یک IDS سیستم مطابقتی دارد که پاکِت‌های غیرمطمئن را علامت‌گذاری می‌کند. این می‌تواند، شامل پاکِت‌های معتبری باشد که به‌شدت قطعه‌قطعه (fragment) شده‌اند که بار دیگر ثابت می‌کند، بازسازی جریان ارتباطی، مهم است.

جنبهٔ مهم تطبیق پروتوکول این است که برنامهٔ کاربردی هم می‌تواند، تطبیق داده شود که از این طریق IDS، برنامهٔ کابردی غیرمناسب و رفتار پروتوکول را شناسایی می‌کند. به‌حیث مثال، حمله WinNuke از NetBIOS (یک پروتوکول معتبر) استفاده می‌کند. اما اطلاعات خارج از محدوده‌یی را اضافه می‌کند که معتبر هستند؛ اما فقط برای حمله استفاده می‌شوند.

۶.۹.۳ شناسایی نا محسوس

این نوع شناسایی همچون فراگیری فلترهای SPAM است، زیرا یک دورهٔ فراگیری توسط یک IDS، آن را قادر می‌سازد تا سطح پایهٔ فعالیت‌های عادی را تعیین کند. البته این سطح عادی برای هر شبکه متفاوت است، تفکر نهفته در این روش، سنجش و تعیین یک خط پایهٔ آماری از جمله فعالیت فایل، تعداد ورودی‌های کاربر، استفاده از CPU، فعالیت disk و غیره است. پس از ایجاد این خط پایه، IDS برای شناسایی فعالیت ناشناس و مشکوک مورد استفاده قرار می‌گیرد؛ مثلاً: فرض کنید که در حال کنترول فعالیت هستید و IDS شما به این نتیجه می‌رسید که هر روز صبح چندین میزبان از شبکهٔ شما بسیار فعال می‌شوند. شاید در ابتدا متوجه نشوید که چه اتفاقی می‌افتد؛ اما به شما اخطار داده می‌شود که این موضوع را بررسی کنید.

۶.۹.۴ همخوانی الگو/امضا

ایجاد همخوانی بین این دو، رایج‌ترین روش شناسایی حملات است و بدان معناست که IDS باید قادر باشد، هرگونه تکنیک هجومی را بشناسد تا بتواند، مؤثر باشد. یک IDS دیتابیس بزرگی شامل هزاران امضا دارد که آن را قادر می‌سازد تا امضاها (حملات) را با الگوهای خود تطبیق دهند.

مثلاً بسیاری IDSها برای کنترول سوء استفاده، مثل مشاهدهٔ سایت‌های قمار و یا سایت‌های غیر اخلاقی از محل کار، به کار می‌روند. شناسایی این نوع سوءِ استفاده به یک کلمهٔ کلیدی (Keywords) بستگی دارد. اما یک موضوع دیگر را در نظر بگیرید که در آن شخصی برای بررسی و ردیابی شبکهٔ شما از ICMP استفاده می‌کند. پاکِت‌ها شامل نشانه‌های خاصی هستند که قابل تطبیق‌اند.

این نوع شناسایی حمله در سطحی کوچکتر از تحلیل پروتوکول ویا شناسایی نامحسوس صورت می‌گیرد. درنتیجه، رویدادهای خاصی شناسایی می‌شوند که مثلاً نشان‌دهندهٔ این هستند که یک کشف رمز رخ داده است. یکی از الگوهایی که دارای سطح تطابق بسیار بالایی است و مکرراً مورد تطابق قرار می‌گیرد، هنگامی‌است که یک مهاجم مطمئن است که به سطح دسترسی ریشه‌یی یک میزبان دست یافته است. میزبان این‌گونه پاسخ می‌دهد که دسترسی رشته‌یی در پاکِت‌های حاصل‌شده به مهاجم باز پس فرستاده می‌شود و برای کلمهٔ ریشه‌یی مورد بازرسی قرار می‌گیرد. این مثال بسیار ساده شده است. اما آنچه را که یک IDS به دنبال آن است (یعنی همان تطابق‌ها)، به‌خوبی نشان می‌دهد.

۶.۹.۵ تحلیل لاگ (LOG)

IDSها می‌توانند، از وسایل متخلفی لاگ دریافت کنند و برای وقایع امنیتی مربوطه، آن‌ها را بررسی کنند. مثلاً NIDS به راحتی می‌تواند، تمام پروتوکول‌های لایه‌های عملکردی را که توسط یک دستگاه مورد استفاده قرار می‌گیرند، ثبت و گزارش کند. سیتم‌های لاگ‌گیری وقایع (SNMP WinNT Event, UNIX syslog, TRAPS و غیره) می‌توانند، این وقایع را با دیگر وقایع داخل شبکه مرتبط کنند. تحلیل لاگ نه‌تنها داشتن قابلیت مرتبط‌کردن syslog ها با دیگر وقایع بلکه یعنی داشتن میکانیزمی برای ثبت پاکِت‌هایی که IDS ها را برای به صدا در آوردن زنگ خطر نشانه گرفته‌اند.

- **گرفتن پاکِت‌های مختلف:** حسگر IDS پاکِتی را که موجب هدف‌گیری زنگ خطر شده، می‌گیرد. این کار موجب می‌شود تا محتویات پاکِت مورد تحلیل قرار گیرند. یک IDS را می‌توان به‌گونه‌یی تنظیم کرد که پاکِت‌های بیشتر ویا حتا جلسهٔ ارتباطی (session) را جمع‌آوری کند. این امر در درک این‌که چگونه یک امضا، لاگ درست را از نادرست تشخیص می‌دهد، بسیار مهم است.
- **بازسازی جلسهٔ ارتباطی:** اغلب یک IDS برای یک پاکِت، تنها یک پاکِت شروع به هشداردادن می‌کند، اما آن پاکِت یک رویداد است که زنگ خطر را هدف قرار داده است. قابلیت بازسازی تمام جلسهٔ ارتباطی در شناسایی تمام حمله بسیار پر اهیمت است و به حذف پیام‌های اشتباه کمک می‌کند. زیرا اینجا شما تصویر بهتری از آنچه رخ داده است، در دست دارید. گزارش‌ها مهم هستند، زیرا ابزار آنچه را که زنگ خطر را به صدا در آورده، فراهم می‌کنند. گام بعدی‌ترکیب این روش‌ها است تا امنیت شبکه افزایش یابد.

۶.۹.۶ ترکیب روش‌ها

مهاجمان همواره در حال ارتقای توانایی‌های خود هستند و این، شناسایی آنها را همواره دشوار می‌کند. برای مقابله با این مشکل، IDS همواره در حال تکامل است و در شناسایی خود از طریق ترکیب روش‌های شناسایی، باهوش‌تر و بهتر می‌شود؛ مثلاً: یک IDS ممکن است، توانایی‌ترکیب روش‌های تطبیق الگوی متبنی بر امضاها، تحلیل پروتوکول و شناسایی نامحسوس را داشته باشد. این قابلیت استفاده از روش‌های چندگانهٔ شناسایی حمله، شکل دیگری از راه همواره در حال تکامل IDS برای رشد و ارتقای خود است.

۶.۱۰ جلوگیری از حمله

سیستم جلوگیری از حمله (Intrusion Prevention System – IPS)، از یک حمله در زودترین زمان ممکن جلوگیری می‌کنند. IPS با یک IDS کار می‌کند و تولیدکنندگان برای تولید یک IDS با قابلیت IPS، این دو فناوری را با هم‌ترکیب کرده‌اند، برای جلوگیری از حمله، دو تکنیک استفاده می‌شود:

- **قیچی‌کردن (snipping): IDS** را قادر می‌سازد تا یک حملهٔ مشکوک را از طریق پاکِت Reset، TCP ویا پیام غیر قابل دسترسی ICMP قطع کند.
- **گریختن (Shunning): IDS** را قادر می‌سازد تا روتر (Router) یا دیوار آتش (Firewall) شما را به‌طور خودکار تنظیم کند تا از ترافیک بر اساس آنچه شناسایی شده، جلوگیری کند و بدین‌ترتیب از ارتباط اجتناب کند. هرچه IDS پیشرفته‌تر می‌شود، این نوع اجتناب هم حرفه‌یی‌تر می‌شود و به کلمهٔ قفل‌کردن (Blocking) تبدیل می‌شود که در آن یک IDS با یک روتر یا یک دیوار آتش تماس می‌گیرد و یک فهرست کنترول دسترسی (ACL) می‌سازد تا IP آدرس‌های مهاجم را ببیند.

۶.۱۱ عملکردها و پاسخ‌های IPS

همان‌طورکه تا اینجا گفته شد، یک IDS برای جلوگیری از حملات شناسایی‌شده، کارهای مختلفی انجام می‌دهد. مؤثرین راه‌ها شامل قیچی‌کردن و اجتناب‌کردن می‌باشند. IDS می‌تواند، قیچی‌کردن خود را انجام دهد؛ اما اجتناب‌کردن به کمک دستگاه‌های دیگر نیاز دارد. حسگرهای IDS باید به یک کنسول مرکزی گزارش دهند که آن نیز به نوبهٔ خود واکنش‌هایی نشان می‌دهند. در ادامه، چند عملکرد که یک IDS می‌تواند، در پاسخ به یک حمله انجام دهد، آمده است.

- **قیچی تنظیمات دیوار آتش یا روتر:** یک IDS درحالی‌که اجتناب آن فعال است می‌تواند به گونه‌یی دیوار آتش یا روتر را تنظیم کند که آدرس IP مهاجم را فلتر کند؛ اما مهاجم همچنان می‌تواند، از طریق آدرس دیگری حمله کند. دیوارهای آتش نقاط کنترول را برای تغییر تنظیمات از پروتوکول کنترول فعالیت‌های مشکوک (SAMP)، حمایت می‌کنند. هر نقطهٔ کنترول (Check point) استندرد OPSEC ویژهٔ خود را برای تغییر تنظیمات دیوار آتش دارد تا بتواند، آدرس IP مهاجم را قفل کند.

- **ارسال یک دام SNMP:** این کار IDS را بری ارسال یک دیتالاگر (دام/SNMP) به یک کنسول مدیریتی مثل HP open view،،Tivoli، Cabletron Spectrum و غیره تنظیم می‌کند.
- **تشکیل و ایجاد گزارش:** یک IDS می‌تواند، به بخش گزارش وقایع ویندوز، سرور syslog یک پیجر و امثال آن را گزارش دهد ویا حتا یک e-mail ارسال کند.

وقتی‌که یک حمله یا نفوذ شناسایی شد، IDS سرپرست شبکه را مطلع می‌سازد. مرحلهٔ بعدی کار می‌تواند، بر عهدهٔ سرپرست شبکه یا خود IDS باشد که از بررسی‌های به‌عمل‌آمده نتیجه‌گیری کرده، اقدام متقابل را انجام دهد؛ مانند جلوگیری از عملکرد یک قسمت بخصوص برای پایان‌بخشیدن به Sessionهای مشکوک یا تهیهٔ نسخهٔ پشتیبان از سیستم برای حفاظت از معلومات، ویا انتقال ارتباط به یک سیستم گمراه‌کننده مانند Honeypot و چیزهای دیگر که بر اساس سیاست‌های (Policy) شبکه قابل اجرا باشد. درحقیقت IDS یکی از عناصر سیاست‌های امنیتی شبکه است. در بین وظایف مختلف IDS، شناسایی نفوذگر از اساسی‌ترین آنهاست. حتا ممکن است، در مراجع قانونی از نتایج و گزارشات حوادثی‌که IDS اعلام می‌کند، استفاده نمود، و از حملاتی‌که در آینده اتفاق خواهد افتاد، با اعمال وصله‌های امنیتی مناسب، از حمله به یک کمپیوتر بخصوص ویا یک منبع شبکه جلوگیری کرد.

شناسایی نفوذ ممکن است گاهی اوقات زنگ خطر اشتباهی را به صدا در آورد. برای مثال نتیجه خراب کارکردن یک کارت شبکه و یا ارسال شرح یک حمله و یا اثر یک نفوذ ازطریق Email.

ساختار و معماری سیستم تشخیص نفوذ:

سیستم تشخیص نفوذ یک هسته مرکزی دارد و یک تشخیص دهنده (موتور تشخیص) است که مسئولیت تشخیص نفوذ را دارد. این سنسور یک مکانیزم تصمیم گیری بر اساس نوع نفوذ دارد.

این سنسور معلومات خام را از سه منبع دریافت می‌کند.

۱. از معلومات موجود در بانك اطلاعلتی خود IDS.
۲. فایل ثبت وقایع سیستم (syslog).
۳. آثار ترافیك عبوری و دیده بانی شبکه.

فایل ثبت وقایع سیستم (syslog) ممکن است، به‌طور مثال معلومات پیکربندی سیستم و دسترسی‌های کاربران باشد. این معلومات اساس تصمیم‌گیری‌های بعدی میکانیزم سنسور خواهد بود. این سنسور با یک Event Generator که مسئول جمع‌آوری معلومات است، با هم کار می‌کنند. (شکل ۴) قوانین جمع‌آوری معلومات که به‌وسیلهٔ سیاست‌های Event generator مشخص می‌شود، تعیین‌کنندهٔ نوع فلترینگ از روی حوادث و معلومات ثبت‌شده است.

Event Generator، مثل سیستم‌عامل یا شبکه یا یک برنامهٔ اجرایی، تولیدکنندهٔ Policyهایی هستند که ممکن است، یک واقعهٔ ایجادشده در سیستم‌عامل یا Packetهای شبکه را ثبت کنند. این مجموعه به همراه معلومات Policy می‌تواند، در یک سیستم محافظت‌شده یا خارج از شبکه قرار داده شود. در بعضی شرایط خاص هیچ محل مشخصی به‌حیث محل حفظ معلومات ایجاد نمی‌شود؛ مثل وقتی‌که معلومات جمع‌آوری‌شده از وقایع مستقیماً به یک سیستم آنالیز ارسال می‌شود.

وظیفهٔ سنسور فلترکردن معلومات است و حذف‌کردن هر دادهٔ غیر مرتبط که از طرف منابع دریافت معلومات می‌رسد. تحلیل‌کننده برای دستیابی به این هدف از Policyهای موجود استفاده می‌کند. تحلیلگر نکاتی مانند اثر و نتیجهٔ حمله، پرو فایل رفتارهای نورمال و صحیح و پارامترهای موردنیاز مثل Threshold ها را بررسی می‌کند. علاوه بر همهٔ این‌ها بانک معلوماتی که پارامترهای پیکربندی IDS را در خود نگه می‌دارد، روش‌های مختلف ارتباطی را ایجاد می‌کنند. سنسور یا گیرنده هم بانک معلوماتی خاص خود را دارد، که شامل تاریخچهٔ پویایی از نفوذهای پیچیده بوده یا باتوجه به تعدد حمله مورد تحلیل قرارگرفته است. سیستم تشخیص نفوذ می‌تواند، به‌صورت متمرکز مثل برقراری یک فایروال فزیکی یا به‌صورت غیر متمرکز انجام شود. یک IDS غیر متمرکز شامل تعداد زیادی سیستم تشخیص نفوذ در یک شبکهٔ بزرگ است که هرکدام از آنها با هم در ارتباط هستند. سیستم‌های پیچیده‌تر از ساختاری پیروی می‌کنند که ماژول‌های مشابه برنامه‌های خوداجرایی دارند که روی هر کمپیوتر اجرا می‌شوند. عملکرد این سیستم جایگزین، مونیتور و فلترکردن تمام فعالیت‌های مرتبط با یک بخش محافظت‌شده است که بتواند، یک آنالیز دقیق و پاسخ متناسب از شبکه دریافت کند. یکی از قسمت‌های بسیار مهم IDS برنامه‌یی است که به سرور آنالیزکننده گزارش می‌دهد، DIDS (Database IDS) و دارای ابزار آنالیز پیچیده‌تری است که حملات غیر متمرکز را نیز شناسایی می‌کند. دلیل دیگری که وجود دارد مربوط به قابلیت حمل و انتقال در چند منطقهٔ فزیکی است. افزون‌براین عامل جایگزین مشخص برای تشخیص و شناسایی اثر حمله‌های شناخته‌شده می‌باشد. یک راه‌حل ساختاری چندبرنامه‌یی که در سال ۱۹۹۴ ایجاد شد.

AAFID یا Autonomous Agent for Intrusion Detection است (شکل ۵). این ساختار از یک جایگزین استفاده می‌کند که بخش ویژه‌یی از رفتار سیستم را در زمان خاص دیده‌بانی می‌کند. به‌طور مثال یک جایگزین می‌تواند، تعداد دفعاتی را که به سیستم Telnet شده تشخیص داده، درصورتی‌که این عدد منطقی به نظر نرسد، آن را گزارش کند. یک جایگزین همچنین قابلیت ایجاد زنگ خطر در زمان وقوع یک حادثهٔ مشکوک را دارد. جایگزین‌ها می‌توانند، مشابه‌سازی شوند و به سیستم دیگر منتقل گردند. غیر از جایگزین‌ها، سیستم می‌تواند، رابطهایی برای دیده‌بانی کل فعالیت‌های یک کمپیوتر بخصوص داشته باشد. این رابطها همیشه نتایج عملیات خود را به یک مونیتور مشخص ارسال می‌کنند. سیستم‌های مانیتور معلومات را از نقاط مختلف و مشخص شبکه دریافت می‌کنند و این بدین معناست که می‌توانند، معلومات غیرمتمرکز را بهم ارتباط دهند و نتیجه‌گیری نهایی را انجام دهند. به انضمام این‌که ممکن است، فلترهایی گذاشته شود تا دیتای تولیدشده را به‌صورت انتخابی دریافت نماید.

مقابله با نفوذ، نیاز به یک سیستم ترکیبی دام‌گذاری و تله‌اندازی دارد که هردوی این پروسه‌ها باید با بررسی و دقت انجام شود. از کارهای دیگری که باید انجام داد، تغییردادن جهت توجه هکر است. هر دو سیستم واقعی و مجازی (Honeypot) به دام‌اندازی هکر به‌طور دائمی مانیتور (Monitor) می‌شوند و دیتای تولیدشده توسط سیستم شناسایی نفوذ (IDS) برای شناسایی نحوهٔ عملکرد حمله، به دقت بررسی می‌شود که این مهمترین وظیفهٔ یک IDS جهت شناسایی حملات ویا نفوذهای احتمالی می‌باشد.

باز هم تأکید می‌کنیم که فقط وقتی به یک IDS اجازه دهید که وسایل شبکهٔ شما را تنظیم کرده، تغییر دهد که برای مدتی طولانی خودتان به‌شکل دستی و کامل مشغول کنترول و تنظیم آن بوده‌اید.

۶.۱۲ محصولات IDS

سیستم‌های IDS فراوانی وجود دارند که خود موجب سردرگمی‌می‌شوند، زیرا در زمینهٔ استندردهایی که عملکردهای آنها را شامل شود، کار زیادی انجام نشده است. مقایسهٔ این محصولات دشوار است زیرا کلمات، معانی، ویژگی‌ها و عملکردها هنوز به سطحی نرسیده‌اند که یک مقایسهٔ مؤثر بین آنها بتوان انجام داد؛ اما بسیاری محصولات بر اساس کارهای انجام‌شده توسط Open sourceها در رأس این محصولات، snort قرار گرفته است.

۶.۱۳ Snort

در اینجا، آنچه را که در سایت در مورد snort آمده، می‌خوانیم:

Snort یک سیستم شناسایی حملهٔ اوپن‌سورس است که می‌تواند، تحلیل همزمان ترافیک و لاگ پاکِت‌ها و شبکه‌های IP را انجام دهد. این سیستم می‌تواند، تحلیل پروتوکول، جستجو و مطابقت محتوا و شناسایی انواع حمله‌ها و تهدیدات را انجام دهد؛ از جمله buffer overflow، port scan، حمله‌های CGI، SMB probes، ردیابی OS و کارهای دیگر.

Snort از زبان قوانین انعطاف‌پذیر برای شرح ترافیکی که باید جمع‌آوری کرده یا عبور دهد. Snort قابلیت هشدارهای همزمان را هم دارد که به همراه سیستم هشدار برای syslog، یک فایل مشخص‌شده از طرف کاربر، یک سوکت UNIX، یا پیغام Popup ویندوز برای کاربری که از samba's smbclient استفاده می‌کند، عمل می‌کند.

Snort سه کاربرد اصلی دارد؛ می‌تواند، به‌حیث یک تحلیلگر پاکِت مثل tcmpdump (۱)، پاکِت لاگر (که برای رفع ترافیک شبکه مفید است)، یا به‌حیث سیستم تحلیل حملهٔ شبکه استفاده شود.

۶.۱۴ محدودیت‌های IDS

IDS یک تکنالوژی روبه‌تکامل است و محدودیت‌های قابل کنترولی در کنار مزیت‌های آن وجود دارد. یک IDS باید در کنار دیوارهای آتش و روترها استفاده شود. Bugها یا تنظیم‌های اشتباه اغلب منجر به مشکلاتی در این تجهیزات می‌شوند؛ اما مفاهیم آنها اثبات‌شده و دقیق است. برخی محدودیت‌ها به شرح زیرند:

- **HIDS در برابر NIDS:** شاید این یک مشکل نباشد؛ اما هر دو باید با یکدیگر کار کنند تا امنیت شبکه را تضمین کنند، چون هر یک نقش‌های متفاوتی ایفا می‌کنند.
- **الگوهای حمله:** محصولات IDS همواره در مورد نشانه‌های حملهٔ جدید آپدیت نیستند.
- **شناسایی‌های اشتباه:** گاهی ترافیک عادی به اشتباه شناسایی می‌شود.
- **محدودیت‌های منبع:** NIDS در مکان‌های مرکزی شبکه می‌نشینند و باید بتوانند، اطلاعات تولیدشده توسط هزاران دستگاه را تحلیل و ذخیره‌سازی کنند. به وضوح این کار به‌طور کامل انجام نمی‌شود و باید از میان‌بُرها استفاده شود.
- **حالت درازمدت:** یک مشکل معمول «اسکن آهسته» است که در مُدل سیستم را بسیار آهسته اسکن می‌کند. IDS نمی‌تواند، آن همه اطلاعات را در آن زمان طولانی ذخیره کند، بنابراین نمی‌تواند، دیتا را کاملاً مطابقت دهد.
- **نابینایی حسگر:** IDS ها بر روی کمپیوترهای معمولی ساخته شده‌اند که قابلیت‌های ویژه‌یی ندارند. بنابراین می‌توان ارتباط آنها را پُر کرده، آن‌ها را کور کرد و بدین‌وسیله آنها را از ثبت پاکِت‌های مورد نظر باز داشت. به‌حیث مثال، ابزار nmap که یک اسکنر پورت اوپن‌سورس است، دارای ویژگی معروف به decoy scans است که باعث می‌شود، nmap با استفاده از آدرس IP های جعل‌شده، هزاران اسکن را ارسال کند. بنابراین کشف این‌که کدام آدرس واقعی و کدام یک جعلی است، برای مدیر دشوار می‌شود. به‌هرحال، این دو موضوع، دیتای جعلی را حفظ می‌کنند. اگر مهاجم مشکوک باشد و به او شک شود، دیتا هنوز باقی مانده است.
- **محدودیت‌های ذخیره‌سازی:** وقتی یک مهاجم می‌خواهد، حسگر را کور کند، ممکن است، هدف پرکردن دیتابیس حسگر یا سخت‌افزار را داشته باشد. این باعث می‌شود که حسگر وقایع را پاک کرده یا دیگر ذخیره نکند.
- **عدم ارائهٔ سرویس:** یک IDS بسیار پیچیده است، زیرا تمام TCP/IP را به‌کار می‌گیرد. درنتیجه، IDS در برابر حمله آسیب‌پذیر است؛ مهاجمان می‌توانند به راحتی و به‌شکل رایگان همان IDS را دانلود کنند و سپس سعی کنند، پاکِت‌هایی را که IDS را از کار می‌اندازد، پیدا کنند. در طول حمله، مهاجم IDS را از کار انداخته و مخفیانه حمله را ادامه می‌دهد.
- **قطعه‌قطع کردن:** عمل شکستن پاکِت‌های بزرگ به پاکِت‌های کوچکتر را می‌گویند. دریافت‌کنندهٔ TCP/IP پاکِت‌های دیتای آنها را مجدداً به هم وصل می‌کند. اغلب IDS ها نمی‌توانند پاکِت‌های IP

را بازسازی کنند. ابزارهای ساده‌یی وجود دارند که می‌توانند به‌شکل خودکار برای فرار از IDS، حملات را قطعه‌قطعه کنند.

- **تغییر الگویا فرار از آن:** بسیاری NIDS ها به تطبیق وابسته‌اند. متن‌های حمله، الگوهای مشهوری دارند، بنابراین داشتن یک دیتابیس از آنها، شناسایی را آسان می‌کند؛ اما با تغییر متن، به راحتی می‌توان از آن فرار کرد.
- ابزارهای ارزیابی IDS: انواع ابزارها به‌طور رایگان برای آزمایش دقت و کارایی IDS موجودند. دوتا از معروف‌ترین آنها Snot و Stick هستند. این ابزارها هزاران حمله را برای IDS شبیه‌سازی می‌کنند. یک مهاجم می‌تواند، از این برای پنهان‌کردن حمله یا کورکردن IDS استفاده کند.

این محدودیت‌ها به این معنا است که اسفاده از IDS فایده‌ای ندارد. هک کردن آنقدر همه گیر است ابزارهای حمله آندر در دسترس‌اند که کار شناسایی IDS را دشوار می‌کند. اگر IDS به درستی مدیریت و استفاده شود، امنیت هر شبکه‌ای را ارتقا می‌دهد. یک سیاست امنیتی برای استفادهٔ موفق از IDS حیاتی است. شاید نتوان گفت که وسایلی که توسط سیستم امنیتی شما محافظت می‌شوند با ارزش هستند و کسانی که در محافظت از انها نقش دارند، از همان سیاست‌های استفاده می‌کنند که می‌توانند، خود اشتباهاتی مرگبار باشند.

خلاصهٔ فصل ششم

در این فصل یکی از جدیدترین تکنالوژی‌های امنیتی یعنی سیستم شناسایی حمله معرفی شد. این فصل با بررسی انواع مختلف سیستم شناسایی حمله آغاز شد. سیستم شناسایی حملهٔ مبتنی‌برمیزبان که بر روی سرور کار می‌کند و سیستم شناسایی حملهٔ مبتنی‌برشبکه که بر روی شبکه کار می‌کند. همچنان در این فصل عملکردهای اصلی سیستم شناسایی حمله بررسی شد. پروتوکول‌ها و روش‌های مختلفی برای شناسایی انواع حملات وجود دارد که در این فصل چند روش به‌صورت مختصر معرفی شد. پس از آن با معرفی انواع محصولات سیستم شناسایی حمله و همچنین محدودیت‌هایی که سیستم شناسایی حمله دارد، مباحث این فصل به اتمام رسید.

سوالات فصل ششم

۱. اولین IDS تجاری چه موقع و توسط چه کسی ارائه شد؟

۲. دو نوع IDS کدامند و آیا به‌طور جداگانه استفاده می‌شوند یا باهم استفاده می‌شوند؟

۳. NIDS را تعریف کنید و بگویید، چطور و در کدام بخش شبکه مؤثرند.

۴. HIDS را تعریف کنید و بگویید، چطور و در کجای شبکه مؤثرند؟

۵. شناسایی نامحسوس در کجا مؤثر است و چرا؟

۶. کدام روش شناسایی حمله رفتار عملکردی را نیز تغییر می‌دهد؟

۷. هر یک از دو روشی را که برای جلوگیری از حمله استفاده می‌شوند، نام برده، تعریف کنید؟

۸. سه مورد از مهمترین محدودیت‌های IDS را نام ببرید و دلیل انتخاب خود را بگویید؟

فصل هفتم

سیستم‌های جلوگیری از نفوذ

هدف کلی: محصلان با Intrusion Prevention System(IPS) آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. سیستم‌های جلوگیری از نفوذ یا (IPS) را تعریف کنند.
۲. اهمیت IPS را در امنیت شبکه شرح دهند.
۳. نحوۀ کارکرد IPS را بیان کنند.

IPS یک وسیلهٔ امنیتی است که بر فعالیت‌های یک شبکه و یا سیستم نظارت کرده تا رفتارهای ناخواسته و مخرب را شناسایی نموده و از ادامهٔ فعالیت آن‌ها جلوگیری می‌کند. در این فصل راجع به اهمیت IPS در امنیت شبکه‌های کمپیوتری آشنا خواهیم شد که روی موضوعاتی چون نحوهٔ کارکرد IPS، تفاوت عمده بین IPS و IDS عیارسازی یک IPS به‌صورت عملی در شبکه بحث خواهیم نمود.

۷.۱ IPS – یک راهکار امنیتی فعال

IPS مخفف عبارت Intrusion Prevention System به‌معنای سیستم ممانعت از نفوذ است، مرحلهٔ بالاتری از تکنالوژی‌های امنیتی است که قابلیت فراهم‌سازی امنیت در تمام سطوح سیستم از هستهٔ سیستم‌عامل گرفته تا پاکت‌های شبکه (پاکِت‌های داده ارسالی یا دریافتی در شبکه) را دارا می‌باشد. IPS سیاست‌ها و قوانینی را برای ترافیک شبکه حین اعلام آلارم یک IDS هنگام رویارویی با ترافیک مشکوک تعریف می‌کند؛ اما این اجازه را نیز به مدیر سیستم می‌دهد که بتواند، عملکرد لازم را تعیین کند. هنگامی‌که IDS یک حملهٔ بالقوه را اطلاع‌رسانی می‌کند، IPS تلاش می‌کند تا آن را متوقف کند. IPS همچنان این ظرفیت را دارد که بتواند، امضاهای نفوذ شناخته‌شده در سیستم را متوقف کند. باتوجه به تفکر ترکیب IDS و فایروال به‌منظور محافظت می‌توان گفت که IPS نسل پیشرفتهٔ IDS می‌باشد. در حال حاضر دو نوع IPS وجود دارد. این دو مورد شامل سیستم‌های ممانعت از نفوذ میزبان‌محور (host-based intrusion prevention systems) و سیستم‌های ممانعت از نفوذ شبکه‌محور (network-based intrusion prevention systems) می‌شوند.

۷.۲ تفاوت میان IPS و IDS چیست؟

IDS بیشتر شبیه یک دزدگیر عمل می‌کند. IDS قسمت‌هایی از شبکه را که به نظر می‌رسد، کسی به آن صدمه زده، کشف می‌کند و سپس اخطار می‌دهد. بدیهی است که این اخطار بعد ویا در حین آسیب به دستگاه صورت می‌گیرد. اکنون زمان آن رسیده که شما از صدمات، پیش‌تر جلوگیری نموده، سیستم را اصلاح کنید.

IPS برای جلوگیری از ورود بدون‌مجوز به شبکه یا سرویس‌دهنده طراحی شده است و به جای اعلام اخطار مبنی بر این‌که قسمتی از سیستم دچار مشکل شده، از صدمهٔ سیستم جلوگیری به‌عمل می‌آورد.

IPS نسل جدیدی از تکنالوژی IDS است. سیستم IDS به توانایی احتیاج دارد، نه فقط شناسایی. همچنان باید توانایی مسدودکردن حملات را داشته باشد. تفاوت IPS با IDS سنتی در این است که IPS یک سد امنیتی دورادور شبکه ویا سرویس‌دهنده می‌کشد تا صدمه‌یی به آن وارد نشود. از دیگر توانایی‌های IPS بیرون‌راندن تراکم موجود در شبکه، قطع‌ووصل ارتباط شبکهٔ داخلی با شبکهٔ خارجی و کنترول رفت‌وآمدها به داخل و خارج شبکه است.

به عبارت ساده‌تر قابلیت کنترول ارتباط و توانایی بازداشتن حمله‌یی را که در حال وقوع است، دارد. درحالی‌که ممکن است، تفاوت میان IPS و IDS گیج‌کننده به نظر آید؛ از اسامی آنها به سادگی می‌توان

تفاوت میان آنها را دریافت. IDSها بیش از یک دستگاه گردآوری‌کنندهٔ معلومات و آگاه‌کنندهٔ اختلالات شبکه نیستند که تنها قادرند، هر پاکِتی را که قصد عبور دارد، ارزیابی و تحلیل کنند. IPSها تغییر شکل طبیعی IDSها هستند.

IPSها دارای همه توانایی‌های IDSها هستند؛ ولی در سطحی بالاتر. آن‌ها در حقیقت می‌توانند، بر اساس معیارهایی که به آنها می‌دهیم، تصمیم بگیرند. درنتیجه IPS ها، دارای میکانیزم پیش‌گیری هستند و نه‌فقط واکنش به یک حمله.

ذاتاً تمام IPSها IDS نیز هستند؛ اما IDSها IPS نیستند. تفاوت در میکانیزم پاسخ‌دهی است، که با تغییر وظایف IDS از حالت انفعالی به حالت تصمیم‌گیرنده صورت می‌پذیرد. هنگامی‌که مدیر شبکهٔ IPS را برای بررسی عیوب شبکه فعال می‌کند، IPS پاکِت‌های عبوری را بر اساس بانک علایم خود به‌طور دقیق بررسی می‌کند. در این میان نه‌تنها عناوین نامه‌های الکترونیکی، بلکه کل محتوای آنها را نیز قبل از ورود به شبکه بررسی می‌کند و درصورت مخرب بودن، از ورود آنها جلوگیری به عمل می‌آورد.

خودکارسازی امنیتی راهی است که منتظر استفادهٔ خراب‌کاران از یک حفره نمی‌ماند. کُدهای مخرب، ویروس‌ها و نفوذگران می‌بایست راهی برای ورود به سیستم پیدا کنند. دیوارهای آتش معمولی در جلوگیری از حملات ساده به شبکه، از طریق پورت‌های باز یا پروتوکول‌های مختلف مؤثر بودند. همچنان سیستم‌های ضد ویروس نیز در شناسایی ویروس‌هایی که می‌شناسند و از طریق نامه‌های الکترونیک و کاپی فایل وارد سیستم می‌شوند، مؤثر بودند. گرچه نویسنده‌های کُدهای مخرب به‌تازگی استفاده از پروتوکول‌های استندرد و نقاط ورودی (مانند http و پورت ۸۰) را که باید برای انجام کارهای سیستم باز نگه داشته شود، برای نفوذ به داخل سیستم شروع کرده‌اند.

بدین‌ترتیب سیستم‌های امنیتی که دارای میکانیزم‌های ثابت هستند، به مرور زمان دچار اُفت عملیاتی می‌شوند و قادر به پاسخگویی به حملات برنامه‌ریزی‌شدهٔ پیشرفته نمی‌باشند. اینجاست که نقش IPS ها پُررنگ می‌گردد تا به‌طور کاملاً مؤثری جلو نفوذگران را بگیرد.

IPS برای جلوگیری از این قبیل ورودهای غیرمجاز، از چند روش استفاده می‌کند:

IPS ها (مبتنی‌برمیزبان یا شبکه) هر پاکِتی را که قصد ورود به شبکه را دارد، بسیار بهتر از سیستم هشداردهنده، بازرسی می‌کند و سپس دو کار را به انجام می‌رساند. اول جستجوی دیتابیس برای یافتن نوع حمله، که اگر موفق به پیداکردن نوع حمله شد، از پدافند آن استفاده خواهد کرد و در غیر این‌صورت سیستم اجازهٔ دسترسی به فایل‌ها را پیدا می‌کند. این پایه و اساس کارکرد هستهٔ سیستم است که برای جستجوی فعالیت‌های غیرعادی به‌کار می‌رود.

سیستم جلوگیری از نفوذ که با عنوان IPS شناخته می‌شود، یک تکنالوژی پیش‌گیری از تهدیدهای تحت شبکه و سرور است که برای شناسایی و متوقف‌کردن فعالیت‌های مخرب و آسیب‌های احتمالی مورد استفاده

قرار می‌گیرد. سیستم‌های جلوگیری از نفوذ (IPS) همانند سیستم‌های شناسایی نفوذ (IDS) فعالیت‌های مخرب را شناسایی می‌کنند؛ با این تفاوت که در IDS صرفاً عمل شناسایی نفوذ و گزارش انجام می‌شود و قابلیت جلوگیری از تخریب وجود ندارد.

اما IPS علاوه بر شناسایی قادر به مسدودسازی حملات نیز می‌باشد. به عبارتی می‌توان گفت که IPSها نسل پیشرفتهٔ IDS می‌باشند.

IPS ها به‌طور کلی فعالیت‌های مخرب را شناسایی کرده، معلومات مربوط به این فعالیت‌ها را ثبت می‌کنند و پس از جلوگیری از انجام این فعالیت‌ها، گزارش کاملی از کارهای انجام‌شده نیز ثبت می‌کنند.

شاید این سؤال برایتان پیش آمده باشد که با این تفاسیر چه تفاوتی بین IPS و فایروال وجود دارد؟

در پاسخ به این سؤال باید توجه داشته باشید که فایروال تنها ترافیک ورودی و خروجی شبکه را کنترول می‌کند، درحالی‌که سیستم جلوگیری‌ازنفوذ، علاوه بر ترافیک ورودی و خروجی، فعالیت‌های درون سیستم‌ها را نیز بررسی می‌کند و درصورت استفاده به همراه فایروال ضریب بالایی از امنیت را به وجود می‌آورد.

به‌طور کلی IPS ها به چهار دسته تقسیم می‌شوند:

۱. سیستم‌های جلوگیری از نفوذ مبتنی‌برشبکه (NIPS): در این نمونه تمامی ترافیک شبکه به‌منظور یافتن ترافیک مشکوک مورد نظارت قرار می‌گیرد.
۲. سیستم‌های تشخیص نفوذ بی‌سیم (WIPS): در این مورد شبکهٔ بی‌سیم به‌منظور شناسایی ترافیک مشکوک توسط آنالیز پروتوکول‌های شبکه‌های بی‌سیم، مورد نظارت قرار می‌گیرد.
۳. آنالیز رفتار شبکه (NBA): در این گروه ترافیک شبکه به‌منظور شناسایی تهدیداتی مثل حملات داس ویا بدافزارها بررسی می‌شود.
۴. سیستم‌های تشخیص نفوذ مبتنی‌برمیزبان (HIPS): یک پکیج نرم‌افزاری نصب‌شده که یک «ها ستینگ» را به‌منظور شنا سایی فعالیت‌های م شکوک تو سط آنالیز اتفاقات درون‌ها ست، مورد نظارت قرار می‌دهد.

IPS ها چگونه فعالیت‌های مخرب را شناسایی می‌کنند؟

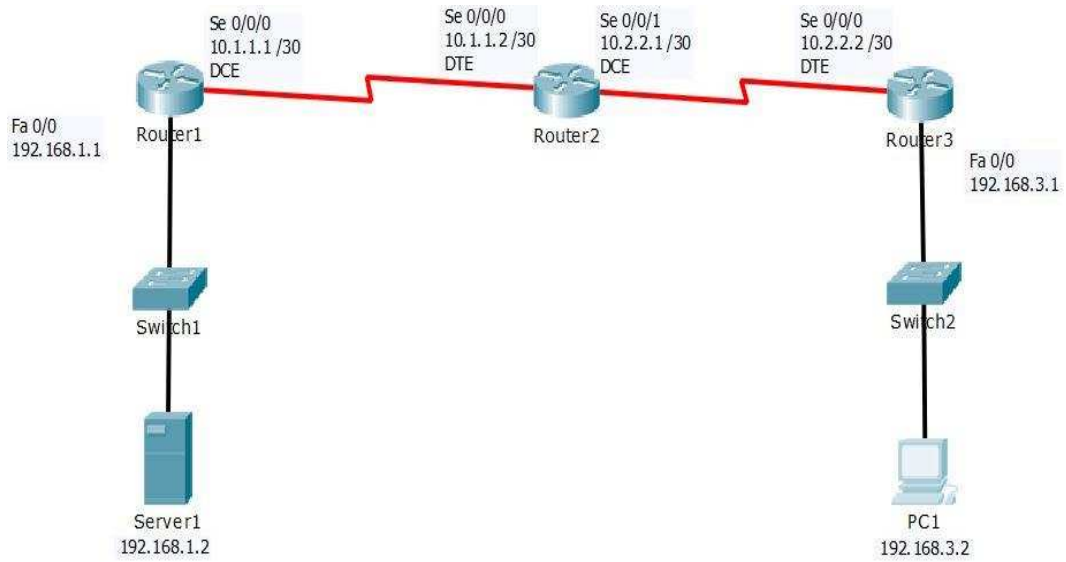
عموماً سیستم‌های تشخیص نفوذ از سه روش به‌منظور شناسایی فعالیت‌های مخرب استفاده می‌کنند:

۱. روش شناسایی با استفاده از امضا: در این روش سیستم‌های تشخیص نفوذ (IDS) ترافیک ورودی و خروجی شبکه را با الگوهای پیش از عیارسازی و پیش از حمله که به‌حیث امضا شناخته می‌شود، مقایسه می‌کنند.

۲. شناسایی مبتنی بر آنومالی آماری: سیستم تشخیص نفوذ مبتنی‌برآنومالی آماری، فعالیت شبکهٔ نارمل را مشخص می‌کند. مثلاً به‌طور کلی چه ترتیبی از پهنای باند مورد استفاده قرار گرفته است، چه پروتوکول‌هایی استفاده شده است یا کدام پورت‌ها و وسایلی به‌طور کلی به یکدیگر متصل هستند و زمانی‌که ترافیک غیر نارمل مشاهده شد، به مدیر شبکه هشدار می‌دهد.

۳. آنالیز پروتوکول‌های مبتنی‌برحالت: این روش، انحراف حالت پروتوکول‌ها را مشخص می‌کند و این عمل با مقایسهٔ رخدادهای مشاهده‌شده و پروفایل‌های از پیش تعیین‌شده‌یی که مطابق با تعریف مورد قبول هستند، انجام می‌شود.

در اینجا یک کار عملی برای کانفیگ‌کردن IPS به‌صورت مرحله‌به‌مرحله نشان می‌دهیم.



شکل ۷-۱ نمونهٔ عملی برای عیارسازی IPS

وضعیت اتصال پورت‌های Router ۱

جدول ۷-۱ وضعیت اتصال پورت‌های Router ۱

Router1	Connected	IP Address	Interface Type Serial
FastEthernet 0/0	Switch 1	192.168.1.1	-
Serial 0/0/0	Router 2	10.1.1.1	DCE

وضعیت اتصال پورت‌های Router 2

جدول ۷-۲ وضعیت اتصال پورت‌های Router ۲

Router2	Connected	IP Address	Interface Type Serial
Serial 0/0/0	Router 1	10.1.1.2	DTE
Serial 0/0/1	Router 3	10.2.2.1	DCE

وضعیت اتصال پورت‌های Router 3

جدول ۷-۳ وضعیت اتصال پورت‌های Router۳

Router3	Connected	IP Address	Interface Type Serial
FastEthernet 0/0	Switch 2	192.168.3.1	-
Serial 0/0/0	Router 2	10.2.2.2	DTE

وضعیت اتصال پورت‌های Switch۱

جدول ۷-۴ وضعیت اتصال پورت‌های Switch۱

Switch1	Connected	Cable
FastEthernet 0/1	Router 1	UTP Cat 6
FastEthernet 0/2	Server 1	UTP Cat 6

وضعیت اتصال پورت‌های Switch۲

جدول ۷-۵ وضعیت اتصال پورت‌های Switch۲

Switch2	Connected	Cable
FastEthernet 0/1	Router3	UTP Cat 6
FastEthernet 0/2	PC1	UTP Cat 6

تنظیمات کمپیوتر Server ۱

جدول ۷-۶ تنظیمات کمپیوتر Server۱

Computer Name	IP Address	Subnet Mask	Default Gateway
Server1	192.168.1.2	255.255.255.0	192.168.1.1

تنظیمات کمپیوتر PC 1

جدول ۷-۷ تنظیمات کمپیوتر PC۱

Computer Name	IP Address	Subnet Mask	Default Gateway
PC 1	192.168.3.2	255.255.255.0	192.168.3.1

Attackerها یا مهاجمان شبکه برای دسترسی به معلومات و ازکارانداختن سرویس‌های مهم، به شبکهٔ شما حمله می‌کنند. سیستم‌های IDS که برگرفته از عبارت Intrusion Detection System و سیستم‌های IPS که برگرفته از عبارت Intrusion Prevention System قادر خواهند بود، ترافیک مشکوک شبکه را تشخیص و واکنش مناسب را برای مقابله با ترافیک مشکوک و حملات داشته باشند. درحقیقت IPS و IDS با بررسی‌ترافیک و معلوماتی که قصد عبور به شبکه را خواهند داشت، ترافیک مشکوک و Attackها را شناسایی خواهند کرد.

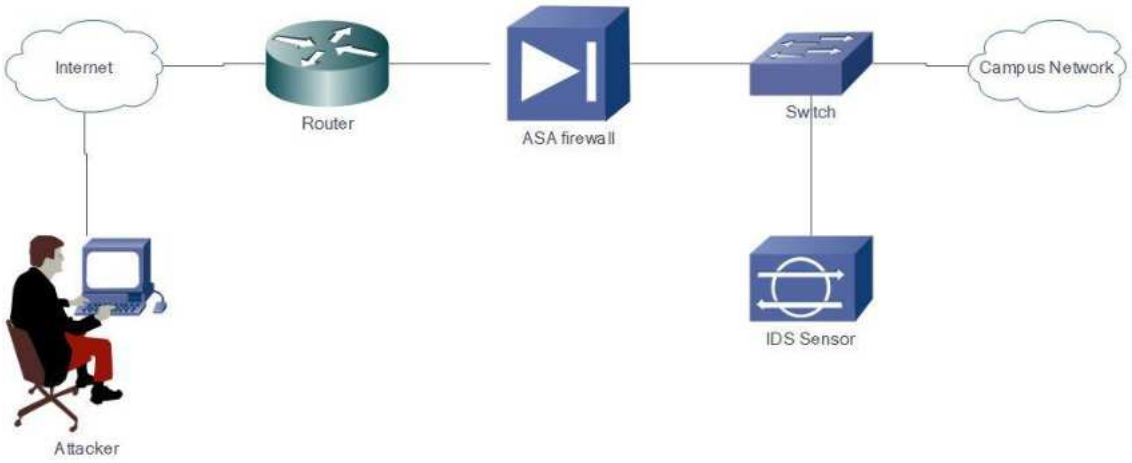
IDS و IPSها می‌توانند، به‌صورت دستگاه‌های سخت‌افزار یا پکیج‌های نرم‌افزاری ارائه شوند.

IDS و IPS هردو توانایی تشخیص حملات و ترافیک‌های مشکوک را خواهند داشت؛ اما عملکرد این دو سیستم با یکدیگر متفاوت می‌باشد.

IDS

یک IDS معلومات را به‌صورت مستقیم در ورودی شبکه دریافت نمی‌کند، بلکه یک کاپی از معلومات دریافتی برای IDS ارسال خواهد شد و IDS این معلومات را بررسی کند، درصورتی‌که IDS ترافیک مشکوک را شناسایی کند. باتوجه به عیارسازی‌های IDS می‌تواند، دستور Block کردن ترافیک را به Router یا Firewall بدهد و این رویداد را ثبت کند.

به تصویر زیر نحوهٔ قرارگیری یک سیستم IDS برای افزایش امنیت در شبکه توجه کنید:

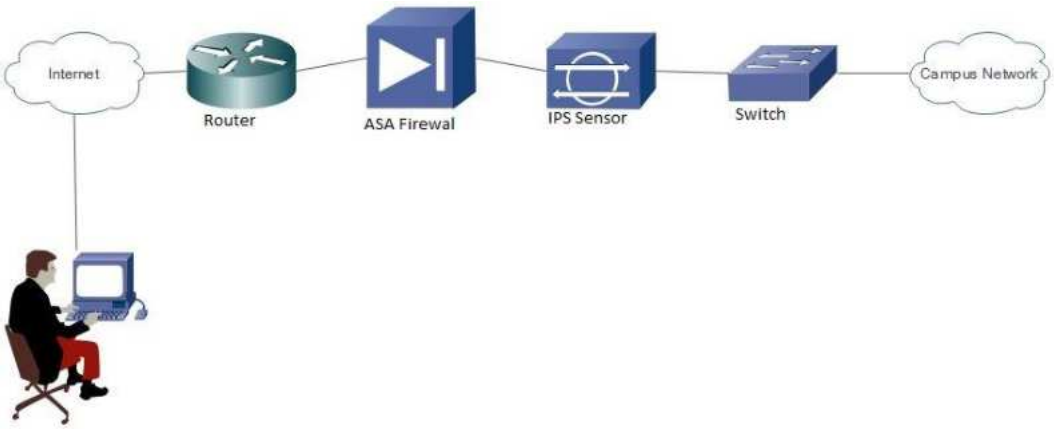


شکل ۷-۸ نحوهٔ قرارگیری IDS در شبکه

IPS

یک IPS معلومات را مستقیم دریافت می‌کند و قادر خواهد بود، معلومات دریافتی شبکه را بررسی کند، درصورتی‌که IPS ترافیک مشکوکی را شناسایی کند، اقدام به Block کردن Attack یا ترافیک مشکوک خواهد کرد. درحقیقت IPSها و IDSها توانایی مقابله با بسیاری از Attackها exploitsها، wormsها و virusesها را خواهند داشت.

به تصویر زیر و نحوهٔ قرارگیری یک سیستم IPS برای افزایش امنیت در شبکه توجه کنید:



شکل ۷-۹ نحوهٔ قرارگیری IPS در شبکه

شرکت سیسکو دستگاه‌های سری ۴۲۰۰ Cisco را تولید نموده است که به‌صورت اختصاصی توانمندی IPS و IDS را پشتیبانی می‌کنند. این دستگاه‌ها دو «مود» عملیاتی به شرح زیر خواهند داشت.

- Promiscuous Mode

- Inline Mode

Promiscuous Mode: این مود نیاز خواهد داشت، دستگاه یک Monitoring Interface داشته باشد که کلیه مُدل‌های سری Cisco 4200 این مود را پشتیبانی می‌کنند. وقتی‌که دستگاهی در این مود اجرا شود، کپی از پاکِت‌های شبکهٔ انتخابی توسط دریافت و پاکِت‌ها را مانیتور و بررسی می‌کند و درصورتی‌که ترافیک مشکوکی تشخیص داده شود، دستگاه می‌تواند، به این ترافیک واکنش‌هایی مانند ارسال هشدار یا حتا مسدودکردن ترافیک را داشته باشد. در این مود عملکرد IDS پشتیبانی می‌شود و عملکرد IPS پشتیبانی نمی‌شود.

Inline Mode: این مود به حداقل دو انترفیس نیاز خواهد داشت که از یک Monitoring Interface ترافیک وارد و از Monitoring Interface دیگر ترافیک خارج می‌شود، این مود عملکرد IPS را پشتیبانی می‌کند.

مُدل‌های دستگاه‌های سری Cisco ۴۲۰۰ به شرح زیر می‌باشد:

۱. CISCO IDS 4215
۲. Cisco IPS 4240
۳. Cisco IPS 4255
۴. Cisco IPS 4260

CISCO IDS 4215: این وسیله دارای ویژگی‌های زیر است:

۱. سرعت انترفیس: 10/100/ Mbps؛
۲. حد اکثر تعداد Monitoring Interface: 5 عدد؛
۳. در تصویر زیر شما یک CISCO IDS 4215 را مشاهده می‌کنید.

شکل ۷-۱۰ CISCO IDS 4215

Cisco IPS 4240: این وسیله دارای ویژگی‌های زیر است:

۱. سرعت انترفیس: 10/100/1000/ Mbps؛

۲. حد اکثر تعداد Monitoring Interface: 4 عدد؛

۳. در تصویر زیر شما یک Cisco IPS 4240را مشاهده می‌کنید.

شکل ۷-۱۱ Cisco IPS ۴۲۴۰

Cisco IPS 4255: این وسیله دارای ویژگی‌های زیر است:

1. سرعت انترفیس: 10/100/1000/ Mbps؛
2. حد اکثر تعداد Monitoring Interface: 4 عدد؛
3. در تصویر زیر شما یکCisco IPS 4255 را مشاهده می‌کنید.

شکل۷-۱۲ Cisco IPS 4255

Cisco IPS 4260: این وسیله دارای ویژگی‌های زیر است:

۱. سرعت انترفیس: 10/100/1000/ Mbps؛
۲. حد اکثر تعداد Monitoring Interface: 9 عدد؛
۳. در تصویر زیر شما یک Cisco IPS 4260 را مشاهده می‌کنید.

شکل۷-۱۳ Cisco IPS 4260

شرکت سیسکو علاوه بر تولید IPS سخت‌افزار یک سری از Moduleهای سخت‌افزاری دیگر را نیز با توانمندی‌های IPS و IDS تولید نموده است، برخی از آنها به شرح زیر می‌باشند:

AIP-SSM: این Module دارای توانمندی‌های پیشرفتهٔ امنیتی IPS و IDS و دارای RAM و CPU و نرم‌افزار و همچنین Storage می‌باشد که در تصویر زیر آن را مشاهده می‌کنید:

شکل ۷-۱۴ AIP-SSM

NM-CIDS: این Module در اسلات‌های NM روتر نصب خواهد شد و قابلیت مانیتورنمودن ترافیک مربوط به کل انترفیس‌های روتر را خواهد داشت و فقط توانمندی IDS را پشتیبانی می‌کند و امکان محافظت کامل Signature Protection بدون این‌که در کارایی شبکه تأثیر منفی داشته باشد، امکان‌پذیر می‌باشد.

در تصویر زیر یک NM-CIDS را مشاهده می‌کنید:

شکل۷-۱۵ NM-CIDS

NM-CIDS قابلیت نصب در روترهای زیر را خوا هد داشت.

- Cisco 2600XM Series Router
- Cisco 2691 Router
- Cisco 3660 Router
- Cisco 3725 Router
- Cisco 3745 Router
- Cisco 2811 ISR
- Cisco 2821 ISR
- Cisco 2851 ISR
- Cisco 3825 ISR
- Cisco 3845 ISR

درحقیقت IPSها و IDSها از مجموعه‌یی از علایم یا Signature برای شناسایی حملات و ترافیک مشکوک استفاده می‌کنند. درصورتی‌که ترافیک با یکی از Signatureها مطابقت داشته باشد، دستگاه IDS یا IPS می‌تواند، تولید هشدار یا حتا باعث مسدودکردن ترافیک انتقالی شوند.

Signatureها انواع مختلفی دارند و هر Signature برای بررسی ترافیک انتقالی از یک موتور به نام microegine استفاده می‌کند که کار این microegine درحقیقت بررسی ترافیک بر اساس Signatureها می‌باشد.

IDSها و IPSها برای شناسایی ترافیک مشکوک و غیر مجاز از روش‌های زیر استفاده می‌کنند:

۱. Signature-base
۲. Policy-base
۳. Anomaly-base
۴. Honey pot detection

۷.۳ انواع عملکردهای IPS در زمان یافتن ترافیک مشکوک:

۱. ایجاد یک Log Message؛
۲. Drop کردن پاکِت‌ها یا از بین‌بردن Packetهای مشکوک؛
۳. Reset کردن اتصال TCP؛
۴. Block کردن ترافیک IP مربوط به Attacker.

شما می‌توانید، توانمندی IOS IPS را برروی Routerهای Cisco عیارسازی کنید. درصورتی‌که قصد راه‌اندازی توانمندی‌های IPS را بر روی Router داشته باشید، نیاز به شرایط زیر می‌باشد:

۱. RAM حافظهٔ 128 MB؛
۲. Flash فضای خالی روی حافظهٔ 2 MB؛
۳. IOS نسخه 12.4(15) T3 و بعد از آن؛
۴. روترهای Cisco Intergrated Services سری‌ها 87x, 18x, 28xx, or 38xx.

مرحلهٔ اول: اتصال به Router ۱

در این مرحله، ابتدا توسط نرم‌افزار Hyper Terminal به Router ۱ متصل شوید و وارد مود User Mode شوید.

در خط فرمان چه چیزی را مشاهده می‌کنید؟

درصورتی‌که در خط فرمان عبارت زیر را مشاهده می‌کنید، به درستی وارد User Mode شده‌اید؛ در غیر این صورت، اتصال Router به PC توسط کیبل Console را بررسی کنید.

```
Router>
```

مرحلهٔ دوم: عیارسازی Hostname بر روی Router ۱

بعد از اتصال به Router، دستورات زیر را بر روی آن اجرا کنید:

```
Router#config t
Router(config)#hostname Router1
Router1(config)#
```

طوری‌که مشاهده می‌کنید، Hostname روتر از Router به Router ۱ تغییر پیدا خواهد کرد.

مرحلهٔ سوم: عیارسازی تنظیمات IP Address بر روی انترفیس‌های Router ۱

عیارسازی انترفیس FastEthernet 0/0و تنظیمات IP Address:

```
Router1#config t
Router1(config)#interface FastEthernet 0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
```

عیارسازی انترفیس Serial 0/0/0 و تنظیمات IP Address:

```
Router1#config t
Router1(config)#interface serial 0/0/0
Router1(config-if)#ip address 10.1.1.1 255.255.255.252
Router1(config-if)#clock rate 64000
Router1(config-if)#no shutdown
```

به علت این‌که کیبل DCE به انترفیس Serial 0/0/0 در Router متصل شده است، در عیارسازی‌های این انترفیس Clock rate باید تعیین شود.

مرحلهٔ چهارم: عیارسازی Default Route بر روی Router ۱

در این مرحله با عیارسازی یک Default Route بر روی Router ۱ کلیه ترافیکی که مقصد آنها خارج از شبکه ۱۹۲.۱۶۸.۱.۰ می‌باشد، به هر مقصدی از یک مسیر پیش‌فرض به سمت Router ۲ به آدرس ۱۰.۱.۱.۲ ارسال خواهد شد.

برای تعریف یک Default Route از دستور زیر استفاده کنید:

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

در دستور بالا هر ترافیکی به هر مقصدی، غیر از شبکهٔ ۱۹۲.۱۶۸.۱.۰ به سمت Router ۲ به آدرس ۱۰.۱.۱.۲ ارسال خواهد شد.

مرحلهٔ پنجم: اتصال به Router ۲

در این مرحله، ابتدا توسط نرم‌افزار Hyper Terminal به Router ۲ متصل شده، وارد مود User Mode شوید.

در خط فرمان چه چیزی را مشاهده می‌کنید؟

درصورتی‌که در خط فرمان عبارت زیر را مشاهده می‌کنید، به درستی وارد User Mode شده‌اید، در غیر این‌صورت، اتصال Router به PC توسط کیبل Console را بررسی کنید.

```
Router>
```

مرحلهٔ ششم: عیارسازی Hostname بر روی Router ۲

بعد از اتصال به Router ۲، دستورات زیر را بر روی آن اجرا کنید:

```
Router#config t
Router(config)#hostname Router2
Router2(config)#
```

طوری‌که مشاهده می‌کنید، Hostname روتر از Router به Router ۲ تغییر پیدا خواهد کرد.

مرحلهٔ هفتم: عیارسازی تنظیمات IP Address بر روی انترفیس‌های Router ۲

عیارسازی انترفیس Serial 0/0/0 و تنظیمات IP Address:

```
Router2#config t
Router2(config)#interface Serial 0/0/0
Router2(config-if)#ip address 10.1.1.2 255.255.255.252
Router2(config-if)#no shutdown
```

عیارسازی انترفیس Serial 0/0/1 و تنظیمات IP Address:

```
Router2#config t
Router2(config)#interface Serial 0/0/0
Router2(config-if)#ip address 10.2.2.1 255.255.255.252
Router2(config-if)#clock rate 64000
Router2(config-if)#no shutdown
```

به علت این‌که کیبل DCE به انترفیس Serial 0/0/1 در Router ۲ متصل شده است، در عیارسازی‌های این انترفیس، Clock rate باید تعیین شود.

مرحلهٔ هشتم: عیارسازی Static Route بر روی Router ۲

در این مرحله، با عیارسازی دو عدد Static Route بر روی Route ۲ کلیه ترافیکی که مقصد آنها شبکهٔ ۱۹۲.۱۶۸.۱.۰ می‌باشد، به Router ۱ یعنی آدرس ۱۰.۱.۱.۱ و کلیه ترافیکی که مقصد آنها شبکهٔ ۱۹۲.۱۶۸.۳.۰ می‌باشد، به Router ۳ یعنی آدرس ۱۰.۲.۲.۲ ارسال خواهند شد.

برای تعریف Static Route از دستور زیر استفاده خواهد شد:

```
Router2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
Router2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.2
```

مرحلهٔ نهم: اتصال به Router ۳

در این مرحله، ابتدا توسط نرم‌افزار Hyper Terminal به Router ۳ متصل شده، وارد User Mode شوید.

در خط فرمان چه چیزی را مشاهده می‌کنید؟

درصورتی‌که در خط فرمان عبارت زیر را مشاهده می‌کنید، به درستی وارد User Mode شده‌اید، در غیر این‌صورت اتصال Router به PC توسط کیبل Console را بررسی کنید.

```
Router>
```

مرحلهٔ دهم: عیارسازی Hostname برروی Router ۳

بعد از اتصال به Router ۳ دستورات زیر را برروی آن اجرا نمایید.

```
Router#config t
Router(config)#hostname Router3
Router3(config)#
```

همان طور که مشاء هده می‌کنید Hostname روتر از Router به Router۳ تغییر پیدا خوا هد کرد.

مرحلهٔ یازدهم: عیارسازی تنظیمات IP Address روی انترفیس‌های Router ۳

عیارسازی انترفیس FastEthernet ۰/۰و تنظیمات IP Address:

```
Router3#config t
Router3(config)#interface FastEthernet 0/0
Router3(config-if)#ip address 192.168.3.1 255.255.255.0
Router3(config-if)#no shutdown
```

عیارسازی انترفیس Serial ۰/۰/۰ و تنظیمات IP Address:

```
Router3#config t
Router3(config)#interface Serial 0/0/0
Router3(config-if)#ip address 10.2.2.2 255.255.255.252
Router3(config-if)#no shutdown
```

مرحلهٔ دوازدهم: عیارسازی Default Route بر روی Router ۳

در این مرحله، با عیارسازی یک Default Route بر روی Router ۳ کلیه ترافیکی که مقصد آنها خارج از شبکهٔ ۱۹۲.۱۶۸.۳.۰ می‌باشد، به هر مقصدی از یک مسیر پیش‌فرض به سمت Router ۲ به آدرس ۱۰.۲.۲.۱ ارسال خواهد شد.

برای تعریف یک Default Route از دستور زیر استفاده خواهد شد:

```
Router3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

در دستور بالا هر ترافیکی به هر مقصد، غیر از شبکهٔ ۱۹۲.۱۶۸.۳.۰ به سمت Router ۲ به آدرس ۱۰.۲.۲.۱ ارسال خواهد شد.

مرحلهٔ سیزدهم: بررسی اتصال بین Router ۱ و Server ۱

در این مرحله، قصد داریم، اتصال بین Server ۱ و Router ۱ را با دستور Ping تست کنیم.

برای این منظور در Server ۱ از دستور زیر استفاده می‌کنیم:

```
Server1>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=20ms TTL=254
Reply from 192.168.1.1: bytes=32 time=20ms TTL=254
Reply from 192.168.1.1: bytes=32 time=20ms TTL=254
Reply from 192.168.1.1: bytes=32 time=20ms TTL=254
```

همان طور که مشاهده می‌کنید بین Server ۱ و Router ۱ به صورت صحیح، ارتباط وجود دارد.

مرحلهٔ چهاردهم: بررسی اتصال بین Router ۳ و PC ۱

در این مرحله، قصد داریم، اتصال بین PC ۱ و Router ۳ را با دستور Ping تست کنیم.

برای این منظور، در PC ۱ از دستور زیر استفاده می‌کنیم:

```
PC1>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
```

چنان‌که مشاهده می‌کنیم، بین PC ۱ و Router به‌صورت صحیح، ارتباط وجود دارد.

مرحلهٔ پانزدهم: بررسی اتصال بین Server ۱ و PC ۱

در این مرحله، قصد داریم، اتصال بین PC ۱ و Server ۱ را با دستور Ping تست کنیم.

برای این منظور، در Server ۱ از دستور زیر استفاده می‌کنیم:

```
Server1>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.2: bytes=32 time=20ms TTL=254
Reply from 192.168.3.2: bytes=32 time=20ms TTL=254
```

چنان‌که مشاهده می‌کنید بین PC ۱ و Server ۱ به صورت صحیح، ارتباط وجود دارد.

مرحلهٔ شانزدهم: دانلود آخرین نسخه Signature Package از سایت سیسکو

در این مرحله، شما باید آخرین نسخهٔ Signature Package File و Public Crypto Key File را دانلود و آنها را بر روی Server ۱ قرار دهید. برای دانلود شما نیاز به یک Username و Password از سایت شرکت سیسکو خواهید داشت.

Signature Package File را از سایت www.Cisco.com دانلود کنید. نام این فایل IOS-Sxxx-CLI.pkg می‌باشد.

Public Crypto key file را از لینک زیر دانلود کنید. نام این فایل realm-cisco.pub.key.txt می‌باشد.

http://download-sj.cisco.com/cisco/ciscosecure/ids/sigup/5.0/ios/realm-cisco.pub.key.txt

در صفحهٔ بازشده، باید نام کاربری و Password معتبر دسترسی به سایت سیسکو را وارد کنید که توانایی دانلود Signature package file و Public Crypto key file را داشته باشید.

معلومات مربوط به Username و Password معتبر در داخل سایت شرکت سیسکو را وارد کرده، بر روی گزینهٔ Log in کلیک کنید.

مرحلهٔ هفدهم: ایجاد یک Directory بر روی حافظهٔ Flash روتر ۱ Router

در این مرحله، بعد از دانلودکردن فایل‌های Signature از سایت شرکت سیسکو بر روی حافظهٔ Flash یک Directory به نام IPS ایجاد خواهیم کرد.

برای ایجاد یک Directory روی حافظهٔ Flash روتر از دستور زیر استفاده کنید.

```
Router1#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

دستور بالا یک Directory بر روی حافظهٔ Flash روتر ۱ Router ایجاد می‌کند، با واردکردن این دستور، یک سؤال از شما پرسیده می‌شود. نام Directory را تصدیق کنید و پس از تصدیق نام Directory در خط بعد پیام ساخته‌شدن Directory را نمایش خواهد داد.

برای تصدیق ایجادشدن Directory با نام IPS بر روی حافظهٔ Flash از دستور زیر استفاده کنید:

```
Router1#dir flash:ips
Directory of flash:/ips/
No files in directory
```

در خروجی دستور بالا مشاهده می‌کنید که در داخل Directory ساخته‌شده با نام IPS، هیچ فایلی وجود ندارد. در مراحل بعدی معلومات فایل‌های Signature و عیارسازی‌های IPS در داخل Directory قرار خواهد گرفت.

مرحلهٔ هژدهم: عیارسازی IPS Crypto key بر روی ۱ Router

در این مرحله، کلیدهای IPS crypto که در فایل realm-cisco.pub.key.txt قرار دارند که در مرحلهٔ شانزدهم همین لابراتوار آن را دانلود نمودیم، بر روی Router تعریف خواهیم کرد.

در ابتدا این فایل را توسط یک نرم‌افزار ویرایشگر متن، مانند Notepad یا سایر نرم افزارهای ویرایشگر فایل متنی، باز کنید و محتویات کل فایل را انتخاب کنید. برای این منظور می‌توانید، از مینوی Edit نرم‌افزار Notepad گزینهٔ Select all را انتخاب کنید تا کل محتویات متن انتخاب شود و سپس کلید Ctrl+C را فشار دهید تا کل محتویات متن کاپی شود.

بعد از کاپی‌کردن کل محتویات فایل realm-cisco.pub.key.txt باید آن را به ۱ Router کاپی کنید. برای این منظور به ۱ Router متصل شوید، همان‌طورکه در خط زیر مشاهده می‌کنید:

```
Router1#config t
Router1(config)#
```

در مود عیارسازی global config کلید Ctrl + V را فشار دهید تا کلیه محتویات فایل realm-cisco.pub.key.txt بر روی Router ۱ کاپی شود.

مرحلهٔ نزدهم: فعال‌نمودن و عیارسازی IPS

برای فعال‌سازی IPS شما باید یک IPS rule با یک نام ایجاد کنید، به‌شکل کلی این دستور توجه کنید:

```
ip ips name <rule name> <optional ACL>
```

rule name: در این قسمت یک نام برای IPS rule تعریف خواهد شد.

ACL: این قسمت از دستور اختیاری می‌باشد که می‌توانید، از ACL های Extended یا Standard برای فلترکردن ترافیک یک rule استفاده کنید.

به مثال زیر توجه کنید:

```
Router1#config t
Router1(config)#ip ips name ips list 110
```

در مثال بالا یک IPS rule به نام ips بر روی Router ۱ ایجاد کردیم.

در تعریف یک IPS rule می‌توانید، از ACL یا Access List استفاده کنید؛ به مثال زیر توجه کنید:

```
Router1#config t
Router1(config)#ip ips name ips list 110
```

در مثال بالا یک IPS rule به نام ips ایجاد و از ACL یا Access List شماره ۱۱۰ استفاده خواهد شد. در این حالت Router ترافیکی که با Access List شمارهٔ ۱۱۰ مطابقت داشته باشد، بررسی خواهد کرد. دستورات مربوط به فعال‌کردن IPS را در جدول ۷-۸ مشاهده می‌کنید:

جدول۷-۸ دستورات مربوط به فعال‌کردن IPS

Command	تشریح Command
Router(config)#ip ips name ips	این دستور یک IPS rule به نام ips ایجاد می‌کند.
Router(config)#ip ips name ips list 110	این دستور یک IPS rule به نام iosips ایجاد خواهد کرد و فقط ترافیکی که با Access List شماره 110 مطابقت داشته باشد، توسط این IPS rule بررسی خواهد کرد.
Router(config)#ip ips fail closed	این دستور یک دستور Optional می‌باشد و باعث خواهد شد درصورتی‌که Router یک Signature engine را پیدا نکند، ترافیک را مسدود کند و مانع از انتقال ترافیک گردد.
Router(config)#no ip ips fail closed	این دستور یک دستور Optional می‌باشد و باعث خواهد شد درصورتی‌که Router یک Signature engine را پیدا نکند، کلیه ترافیک را عبور دهد.

مرحلهٔ بیستم: تعیین محل قرارگیری فایل‌های IPS Signature در حافظهٔ Flash روتر

در مرحلهٔ هفدهم همین لابراتوار یک Directory به نام IPS بر روی حافظهٔ Flash روتر ایجاد کردیم، حال می‌خواهیم، در این مرحله، مکان قرارگیری فایل‌های IPS Signature را تعیین کنیم. برای این منظور از دستور زیر استفاده کنید:

```
Router1#config t
Router1(config)ip ips config location flash:ips
```

در دستور بالا محل Directory به نام IPS که در مرحلهٔ هفدهم همین لابراتوار بر روی حافظهٔ Flash روتر ایجاد شد، به‌حیث محل ذخیرهٔ فایل‌های Signature تعیین خواهد شد.

مرحلهٔ بیست‌ویکم: عیارسازی IPS SDEE برای اعلام وقایع (Eventnotification)

IPS می‌تواند، وقایع و رویدادها را به SDEE ارسال کند، در این مرحله، می‌خواهیم، پروتوکول Security Device Event Exchange (SDEE) را برای اعلام وقایع (event notification) بر روی Router عیارسازی کنیم. برای استفاده از این پروتوکول نیاز به فعال‌کردن HTTP Server دارید که باید بر روی Router با استفاده از دستور ip http server آن را فعال کنید.

برای فعال‌ساختن SDEE از دستور زیر استفاده کنید:

```
Router1#config t
Router1(config)#ip ips notify sdee
```

مرحلهٔ بیست‌ودوم: عیارسازی IPS syslog برای اعلام وقایع (event notification)

همچنان IPS می‌تواند، وقایع و رویدادها را به سمت یک Syslog server ارسال کند و این وقایع در Syslog Server ثبت شود. در لابراتوار هفت در این کتاب نحوهٔ راه‌اندازی یک Syslog server تشریح شده است.

برای ثبت وقایع IPS در Syslog server از دستور زیر استفاده کنید:

```
Router1#config t
Router1(config)#ip ips notify log
```

مرحلهٔ بیست و سوم: اعمال IPS rule به انترفیس Router

بعد از ایجاد یک IPS rule باید IPS rule ایجادشده را به ترافیک ورودی به انترفیس In یا ترافیک خروجی از انترفیس Out یا در هر دو جهت اعمال شود. برای این منظور از دستور زیر استفاده کنید:

```
Router  #config t
Router1(config)#interface Fastethernet 0/0
Router1(config-if)#ip ips in
```

در مثال بالا IPS rule به نام IPS به کلیه ترافیک ورودی به انترفیس FastEthernet ۰/۰ اعمال خواهد شد.

```
Router1#config t
Router1(config)#interface Fastethernet 0/0
Router1(config-if)#ip ips ips out
```

در مثال بالا IPS rule به نام IPS به کلیه ترافیک خروجی از انترفیس FastEthernet ۰/۰ اعمال خواهد شد.

می‌توانید، با استفاده از دستور زیر User Account به‌صورت Local بر روی Router عیارسازی کنید که در این حالت Password مربوط به User Account به‌صورت رمزگذاری (Encrypted) در عیارسازی Router تعریف می‌شود.

مرحلهٔ بیست‌وچهارم: نصب و عیارسازی TFTP Server برای قراردادن Signature package file بر TFTP Server

ابتدا در این مرحله، TFTP Server را نصب و عیارسازی می‌کنیم.

TFTP برگرفته از عبارت Trivial File Transfer Protocol می‌باشد. این پروتوکول بر روی لایهٔ ۷ Layer مُدل OSI کار می‌کند و بسیار شبیه FTP می‌باشد و از پروتوکول UDP جهت انتقالات استفاده می‌کند و یکی از کاربردهای پروتوکول TFTP انتقال Firmware و سیستم‌عامل دستگاه‌هایی مانند Routerها، Switchها و سایر دستگاه‌های سخت‌افزار می‌باشد. پروتوکول TFTP سرعت بیشتری نسبت به پروتوکول FTP دارد و نیاز به احراز هویت با authenticate ندارد.

برای انجام این مرحله باید نرم‌افزار TFTP مربوط به شرکت Cisco را بر روی Server ۱ نصب کنیم. این نرم‌افزار در CD همراه این کتاب موجود می‌باشد که از بخش Tools می‌توانید، آن را بر روی Server ۱ نصب کنید که به‌حیث یک TFTP Server می‌تواند، در شبکه مورد استفاده قرار گیرد.

در این مرحله، شما نرم‌افزار TFTP مربوط به شرکت Cisco را که در CD همراه این کتاب در بخش Tools موجود می‌باشد، برروی Server ۱ نصب و آن را اجرا کنید و تنظیمات زیر را بر روی آن انجام دهید:

بر روی مینوی View کلیک کنید و گزینهٔ Option را انتخاب کنید تا کادر Option ظاهر شود. طوری‌که در تصویر زیر مشاهده می‌کنید.

در کادر ظاهرشدهٔ Option در قسمت TFTP Server Root Directory باید یک مسیر برای نگهداری از معلومات تعیین کنید که این مسیر به مسیر ریشه یا Root معروف می‌باشد و محل نگهداری معلومات موجود و معلومات منتقل‌شده به TFTP Server می‌باشد.

در مرحلهٔ بعدی می‌خواهیم، Signature Package File را که در مرحلهٔ شانزدهم این لابراتوار Download نمودیم، بر روی Root نرم‌افزار TFTP Server قرار دهیم و از طریق Rooter این فایل‌ها را به محل دایرکتوری IPS که در حافظهٔ Flash وجود دارد، کاپی کنیم.

مرحلهٔ بیست‌وپنجم: کاپی Signature Package File به حافظهٔ Flash

در این مرحله، می‌خواهیم، Signature Package File را که در مرحلهٔ قبل بر روی TFTP Server قرار داده شد، به محل دایرکتوری IPS که در حافظهٔ Flash وجود دارد، کاپی کنیم. برای این منظور از دستور زیر استفاده کنید:

```
Router1#copy tftp://192.168.1.2/IOS-S364-CLI.pkg idconf
```

در مثال بالا ۱۹۲.۱۶۸.۱.۲ آدرس TFTP Server می‌باشد و نام IOS-S۳۶۴-CLI.pkg- Signature Package File می‌باشد که در TFTP قرار دارد.

بعد از کاپی Signature Package File می‌توانید، کاپی‌شدن صحیح آن را با دستور زیر تصدیق کنید. برا این منظور از دستور زیر استفاده کنید:

```
Router1#dir ips
Directory of flash:/ips/
Router-sigdef-default.xml 7 –rw- 203419 Feb 14 2010 16:45:24 -08:00
Router-sigdef-dalta.xml 8 –rw- 271 Feb 14 2010 16:43:36 -08:00
Router-sigdef-typdef.xml 9 –rw- 6159 Feb 14 2010 16:44:24 -08:00
Router-sigdef-category.xml 10 –rw- 22873 Feb 14 2010 16:44:26 -08:00 l
Router-seap-delta.xml 11 –rw- 257 Feb 14 2010 16:43:36 -08:00
Router-seap-typedef.xml 12 –rw- 491 Feb 14 2010 16:43:35 -08:00
64016384 bytes total (12693504 bytes free)
```

مشاهده می‌کنید که فایل‌های Signature Package File در محل دایرکتوری IPS که بر روی Flash ایجاد شد، کاپی شده‌اند.

مرحلهٔ بیست و ششم: مشاهدهٔ وضعیت و تعداد Signatureها

برای مشاهدهٔ وضعیت تعداد Signatureهای اجراشده و ایجاد بر روی Router از دستور زیر استفاده نمایید:

```
Router1#show ip ips signature count
Cisco SDF release version S247.0
Trend SDF release version V1.2

Signature Micro-Engine: multi-string
Total Signatures: 7
Enabled: 7
Retired: 2
Complied: 5

Signature Micro-Engine: service-http
Total Signatures: 541
Enabled: 284
Retired: 336
Complied: 205
```

Signature Micro-Engine: string-tcp

Total Signatures: 487

Enabled: 332

Retired: 352

Complied: 135

Signature Micro-Engine: string-udp

Total Signatures: 50

Enabled: 3

Retired: 23

Complied: 27

Signature Micro-Engine: staete

Total Signatures: 26

Enabled: 15

Retired: 23

Complied: 3

Signature Micro-Engine: atomic-ip

Total Signatures: 140

Enabled: 87

Required: 93

Complied: 46

Inactive – invalid param: 1

Signature Micro-Engine: string-icmp

Total Signatures: 2

Enabled: 0

Retired: 1

Complied: 1

Signature Micro-Engine: service-ftp

Total Signatures: 3

Enabled: 3

Complied: 3

Signature Micro-Engine: service-rpc (INACTIVE)

Signature Micro-Engine: service-dns

Total Signatures: 1

Enabled: 1

Retired: 1

Signature Micro-Engine: normalizer

Total Signatures: 9

Enabled: 9

Complied: 9

Total Signatures: 1266

Total Enabled Signature: 741

Total Retired Signature: 831

Total Complied Signature: 434

Total Signatures with invalid parameters: 1

به خروجی دستور Show ip ips signature count که در بالا مشاهده می‌کنید، توجه نمایید.

دستورات زیر را برروی Router ۱ اجرا کنید و به خروجی دستورات توجه فرمایید.

Router1#show ip ips all

Router1#show ip ips configuration

در کادر زیر عیارسازی مربوط به Router ۱ را مشاهده می‌کنید:

عیارسازی Router 1

```
Hostname Router 1
!
!
Ip ips config location flash:ips/ retires 1
Ip ips name ips
Ip ips name ips list 110
!
!
Interface FastEthernet0/0
 Ip address 192.168.1.1 255.255.255.0
Ip ips ips in
Ip ips ips out
Duplex auto
Speed auto
!
!
!
Interface serial0/0/0
 Ip address 10.1.1.1 255.255.255.252
 Clock rate 64000
!
!
Ip ips notify log
!
!
Ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
Line con 0
 Login
!
!
!
End
```

در کادر زیر عیارسازی‌های مربوط به Router ۲ را مشاهده می‌کنید:

عیارسازی Router 2

```
Hostname Router 2
!
!
Interface serial0/0/0
 Ip address 10.1.1.2 255.255.255.252
!
!
Interface serial0/0/1
 Ip address 10.2.2.1 255.255.255.252
 Clock rate 64000
!
!
!
Ip route 192.168.1.0 255.255.255.0 10.1.1.1
Ip route 192.168.3.0 255.255.255.0 10.2.2.2
!
!
!
Line con 0
 Login
!
!
!
End
```

در کادر زیر عیارسازی‌های مربوط به Router 3 را مشاهده می‌کنید:

عیارسازی Router 3

```
Hostname Router3
!
!
!
!
Interface FastEthernet0/0
 Ip address 192.168.3.1 255.255.255.0
 Duplex auto
 Speed auto
!
!
!
Interface serial0/0/0
 Ip address 10.2.2.2 255.255.255.252
!
!
!
Ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
!
!
!
Line con 0
 Login authentication default
!
!
Line vty 0 4
Exec timeout 4 0
Login authentication default
!
!
!
End
```

خلاصهٔ فصل هفتم

در این فصل سیستم‌های جلوگیری از نفوذ یا IPS مورد مطالعه قرار گرفت. باتوجه به این‌که در فصل قبلی گفته شد، برای شناسایی حملات کمپیوتری از IDS استفاده می‌شود، اما این سیستم‌ها قادر به جلوگیری از حملهٔ انجام شده نبودند. لذا نیاز به سیستم دیگری برای انجام کارهایی برای جلوگیری از حمله ویا کاهش حملات احتمالی خواهد بود. در این فصل تفاوت‌های عمده بین IDS و IPS معرفی شد و نحوهٔ عملکرد IPS در زمان حملات یا فعالیت‌های مشکوک نیز به بحث گرفته شد. در آخر با عیارسازی یک IPS به‌صورت عملی و نحوهٔ قراردادن آن در یک شبکه آشنا شدیم.

سوالات و فعالیت فصل هفتم

۱. اولین IPS تجاری چگونه ایجاد شد؟

۲. تفاوت میان IPS و IDS را تشریح کنید.

۳. انواع عملکردهای IPS را در اتفاقات مشکوک تشریح کنید.

۴. روش‌های جلوگیری از حمله را تشریح کنید.

فعالیت

با استفاده از نرم افزارهای شبیه‌سازی مانند GNS3 یک IPS را در یک شبکه عیارسازی کنید.

(References) منابع

1. Albanese, J., & Sonnenreich, W. (2004). *Network Security Illustrated*: McGraw-Hill.
2. Bishop, M. (2003). *Computer security: art and science*: Addison-Wesley Professional.
3. Maiwald, E. (2001). *Network security: a beginner's guide*: McGraw-Hill Professional.
4. Perlman, R., Kaufman, C., & Speciner, M. (2016). *Network security: private communication in a public world*: Pearson Education India.
5. Stallings, W. (2008). Cryptography and network security: principles and practice. *Practice (6th Edition), 9*, 09685.
6. Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: principles and practice*: Pearson Education.
7. Tanenbaum, A. S., & Wetherall, D. (2014). *Computer networks*: Harlow, Essex: Pearson.
8. CISCO (2016), CCNA Security
9. https://www.cisco.com/c/en/us/index.html