خلاصه

مقصود اصلی طرح امنیتی Cisco برای شبکه های سازمانی (SAFE) ، فراهم آوردن بهترین اطلاعات تمرینی برای علاقمندان به طراحی و پیاده سازی شبکه های کامپیوتری امن می باشد . SAFE به عنوان راهنما ، با توجه به نیازهای امنیتی ، به طراحان شبکه خدمت می کند . SAFE دفاع در عمق (defence-in-depth) را در طراحی شبکه امن فراهم می نماید این نوع طراحی بر روی حملات پیش بینی شده و راه های کاهش آنها متمرکز می باشد . (مثل اینکه بگوییم در اینجا یک Firewall قرار بده ، در آنجا یک سیستم تشخیص ورود غیر مجاز قرار بده و . . .) . نتیجه ا ی این استراتژی ، در یک سیستم امنیتی لایه لایه ، اینست که با نقص و از کارافتادن یک سیستم امنیتی ، احتمال مورد مصالحه قرار گرفتن (Hack شدن) منابع شبکه وجود ندارد . SAFE مبتنی بر محصولات شرکت Cisco و شرکایش می باشد .

ضمیمه B ، شامل مبانی امنیت شبکه می باشد ، به خوانندگانی که با مفاهیم امنیت شبکه آشنا نیستند ، پیشنهاد می شود که قبل از مطالعهٔ بقیه مستند ، این بخش را مطالعه فرمایند .

ضمیمه C ، شامل واژه نامه تعاریف و اصطلاحات فنی ، و همچنین تصاویر بکار رفته در این مستند می باشد .

این نوشته با یک نگاه وسیع به معماری ، سپس ماژولهای منحصر به فردی را که طراحی شبکه واقعی را می سازد را شرح میدهد . سه قسمت اولیه هر ماژول جریان ترافیکی ، ابزارهای کلیدی و تهدیدات قابل پیش بینی و نمودارهای اساسی کاهش آنها را شرح می دهد . تجزیه تحلیل فنی طراحی تشریح می شود در امتداد تشریح تکنیکهای تضعیف و رفع تهدیدات و استراتژیهای تهدید .

این مستند به شدت بر روی تهدیداتی که در محیط های سازمانی با آن مواجه هستیم ، متمرکز می شود . در صورت آشنایی طراحان شبکه با این تهدیدات ، می توانند در مورد چگونگی و محل استفاده از تکنیک های تخفیف ، تصمیم بهتری را اتخاذ نمایند . بدون درک کاملی از تهدیدات پیچیده در امنیت شبکه ،آرایش تجهیزات ، ممکن است به سمت پیکربندی نادرست متمایل شود ، بیش از حد برروی تجهیزات امنیتی متمرکز شود ، و یا منجر به نداشتن انتخاب های مختلف در پاسخ به تهدید ها گردد . با مطالعه این مستند و فهمیدن شیوه های کاهش تهدید ، یک طراح شبکه باید اطلاعات لازم جهت پیاده سازی یک شبکهٔ امن را بدست آورده باشد .

مخاطبین

با توجه به طبیعت فنی این مستند ، بسته به خواننده ، می تواند درسطوح مختلفی از نظر جزئیات ، مورد مطالعه قرار گیرد . به عنوان مثال ، یک مدیر شبکه می تواند جهت بدست آوردن یک دید مناسب بر استراتژی های طراحی شبکه های امن ، بخش های مقدماتی درهر مبحث را مورد بررسی و مطالعه قراردهد .

یک مهندس و یایک طراح شبکه می تواند با خواندن این مستند ، اطلاعات مناسبی در زمینهٔ طراحی بدست آورد . همچنین جزئیات تجزیه و تحلیل تهدید ها و نحوهٔ پیکر بندی سریع تجهیزات مورد بحث در مستند جهت اطلاع این دسته از افراد ارائه شده است .

*** پیش بینی های احتیاطی

این مستند فرض می کند که هم اکنون ، شما از یک سیاست امنیتی درمحلتان بر خوردارید . مستقر نمودن تکنولوژی های امنیتی ، بدون سیاست های وابسته به آنها ، پیشنهاد نمی گردد . این مستند مستقیما" نیازهای شرکت های بزرگ را نشان می دهد . حال آنکه اکثر اصولی که دراینجا مورد بحث قرار می گیرد ، می تواند مستقیما توسط شرکت های متوسط و کوچک و حتی دفاتر خانگی (Home Office) در مقیاس های متفاوت ، مورد استفاده قرارگیرد . تجزیه و تحلیل مشروح انواع حرفه ها و نیازهای خاص آنها از محدودهٔ این مستند خارج است .

دنبال نمودن راهنمایی این مستند ، داشتن یک محیط امن ، و یا جلوگیری از کلیهٔ دسترسی های غیرمجاز را تضمین نمی کند . امنیت واقعی مطلق فقط می تواند طریق جداکردن یک سیستم از شبکه ، قراردادن آن در یک محفظهٔ بتونی ، و گذاشتن آن در ته یکپناهگاه مستحکم ، بدست آید .

(داده هایتان فقط از طریق غیر قابل دسترس شدن ، خیلی امن خواهند شد .) به هر حال شما می توانید توسط: بر پایی یک سیاست امیتی مناسب ، دنبال نمودن راهنمایی های این مستند ، به روز بودن با توجه به آخرین دست آوردهای مطرح شده در مجامع امنیتی و همچنین مجامع Hacker ها ، و نگهداری و نظارت (مانیتورینگ) تمامی سیستم ها توسط تمرینات Administration با سیستم صوتی ، امینت معقولی را در شبکه تان بدست آورید . این هچنین شامل پی آمدهای امنیت برنامه های کاربردی مورد استفاده در شبکه نیز می باشد که به طور کامل توسط این مستند ، نشان داده نشده است .

با وجود اینکه این معماری ، شبکه های خصوصی مجازی (VPN) را نیز شامل می شود ، اما آنها به تفصیل مورد بحث قرار نگرفته اند . همچنین این مستند اطلاعاتی مانند جزئیات تغییر مقیاس ، استراتژی های ارتجاعی ، و دیگر موضوعات وابسته به VPN را شامل نشده است .

مانند VPN ها ، استراتژی های شناسایی (شامل تصدیق مجوزها (CA) ، در هیچ سطحی از این مقاله مورد بحث قرار نگرفته است . به طور مشابه ، CA ها ، به یکسطح تمرکز نیاز دارند که این مستند قادر به فراهم آوردن آن نیست و هنوز همهٔ نواحی مربوط به امنیت شبکه را به قدرکافی نشان نمی دهد . همچنین بدلیل اینکه هنوز اغلب شبکه های سازمانی ، محیط های کاملا CA ی کاربردی (Functional) را مستقر می نمایند ، چگونگی صفت آرایی شبکه ها بدون آنها ، دارای اهمیت می باشد . در پایان تکنولوژی ها و کاربردهای پیشرفته خاص در زمینهٔ شبکه (مانند شبکه سازی محتوا (Content Networking) ، کش کردن اطلاعات (Caching) و متعادل نمودن بار سرور (Server Load Balancing) ، را شامل نمی شود .

گرچه نتیجه استفاده از تجهیزات در معماری SAFE مطابق با انتظار می باشد ، اما این مستند نیازهای خاص امنیتی درشبکه های خاص را پوشش نمی دهد .

SAFE ، محصولات Cisco و شرکایش را بکار می برد . به هرحال این مستند ، به محصولات با نام آنها اشاره نمی کند . در عوض بجای اسم و یا شمارهٔ مدل اجزاء از منظورکار بردی آنها استفاده شده است . جهت امتحان اعتبارSAFE محصولات واقعی ، دریک شبکهٔ دقیق ، پیاده سازی و پیکربندی شده اند که اطلاعات مربوط به این پیکربندی ها درضمیمهٔ A «آزمایشگاه درستی SAFE» ، ارائه شده است .

درتمامی این مستند اصطلاح Hacker به فردی که با قصد مغرضانه ، جهت دسترسی به منابع شبکه تلاش می کند اطلاق می گرد . در اینجا برای راحتی و خوانایی بیشتر از اصطلاح Hacker برای اینگونه افراد استفاده شده است ، زیرا درجامعه از عمومیت بیشتری برخوردار است .

روشهای حمله به سایتها

I:Packet shiffers :

یک Packet shiffers یک نرم افزار کاربردی است که از یک کارت شبکه در حالت بی قاعده استفاده کرده تا (حالت بی قاعده حالتی است که در آن کارته شبکه همه بسترهایی را که روی کابل شبکه دریافت میشود را جهت پردازش بهٔک برنامه کاربردی می فرستند) همه بسترهای شبکهخ را که بهٔک را ضد تصادفی خاصی ارسال میشوند را بدست آورد .

Sniffer ها در شبکه ای امروزی در جهت خطایابی و تجزیه و تحلیل ترافیک شبکه مفید هستند . به هر حال چون چندین برنامه کاربردی شبکه اطلاعات را به صورت test خالی ارسال میکنند (از قبیل POP3, SMTP, FTP, Tdnet) یک Packet shiffers میتواند اطلاعات حساس و پرمعنی را از قبیلusernameها و posswordها را فراهم کند .

یکی از مسائل جدی کشف username و password این است که کاربران اغلب از این نام وردی logiw و password شان د رچندین برنامه ها و سیستم استافده میکنند و در حقیقت خیلی از کاربران از یک رمز عبور password برای عبور از همه برنامه ها و accountهایشان بهره میبرند . اگر یک برنامه در client server اجرا شود و اطلاعات تصدیقی در شبکه با متن ساده ارسال شوند آنگاه به طور مشابه این اطلاعات تصدیقی میتواند استفاده شود در مقابل سایر منابع خارجی و همکار

بخاطر اینکه hackerها به خصوصیات اشخاص استفاده کننده آشنا هستند و از قبیل استفاده از یک رمز عبور یکتا در چندین account آنها اغلب در بدست آوردن این اطلاعات حساس موفق هستند .

در بدترین حالت ممکن ، یک Hacker میتواند به سیستم سطوح Account کاربران دسترسی پیدا کند و کد Hacker از آن استفاده کرده تا یم اجازه دسترسی جدید ایجاد کند تا هر لحظه بتواند آن را بکار گیرد و به منابع مختلف شبکه وارد شود .

شما میتوانید از چندین راه تهدید Packet shiffersها را کاهش دهید .

۱ – تصدیق :

استفاده از تصدیف قوی انتخاب برای دفاع در برابر Packet shiffersها است . تصدیق قوی میتواند به عنوان یک روش از تصدیق کاربرها که به سادگی نمیتواند فاش شود بکار برد . یک مثال مشترک از تصدیق قوی one- time – pass ها هستند (OTPS) . یک OTPS یکی از دو جزء تصدیق است دو جزء تصدیق شامل استفاده از چیزهایی است که شما با آنچه که میدانید ترکیب کرده اید . ماشینهای گوینده اتوماتیکی (ATM) از دو جزء تصدیف استفاده میکنند . یک مشتری هم کارت ATM و هم شماره شناسایی شخصی(PIN) را برای ساختن یک تراکنش احتیاج دارد . با OTP شمابه PIN و کارت Token برای تصدیق بۀک دستگاۀا برنامه کاربردی احتیاج دارد . یک کارت توکن(Token) یک وسیله سخت افزاری با نرم افزاری است که بطور تصادفی رمزهای عبور را در فواصل زمانی مشخص تولید می کند (معمولا هر ۶۰ ثانیه) و کااربر این رمزهای عبور تصادفی را با یک شماره شناسایی شخصی (PIN) ترکیب کرده تا یک رمز عبئر یکتا تولید شود . که فقط برای یک مدتی رسمیت داشته باشد . اگر یک Hacker رمز عبور را بوسیلۀک Packet Sniffer یاد بگیرد و اطلاعات بی مصرف و بیفایده می شود بخاطر اینکه رمز عبور قبلا منقضی شده است . توجه داشته باشید این تکنولوژی کاهش مؤثر است بر ضد یک Sniffer که طراحی وپیاده سازی شده برای ربودن رمزهای عبور Sniffer ها به صف هستند تا اطلاعات حساسی را بیاموزند (همانند محتوی نامه) همچنان بی اثر خواهد بود .

۲- Switched infrostrutur :

روش دیگر برای شمارش استفاده ازکلید Packet Sniffer در محیط شما گسترش زیربنای کلید شده است برای مثال اگر یک سازمان بی نقص اینترنیتی سوئیچ شده را گسترش دهد hackerها فقط میتوانند ترافیکی را که روی پورت خاصی به آنها وصل میشود را بدست آورند . یک زیربنای سوئیچینگ نمیتواند کاملا تعدی Packet shiffersها را برطرف کند اما میتواند تاثیرشان را کاهش دهد .

۳ - Anti shiffers :

سومین روش در برابر shiffers بکارگیری طراحی سخت افزاری ونرم افزاری برای محافظت و شناسایی فعالیت shifferها بر روی شبکه است . این قبیل نرم افزارها و سخت افزارها به طور کامل از تهدید برطرف نمیکنند اما مانند خیلی ابزارهای امنیتی شبکه قسمتی از سربار سیستم هستند . این روش که Anti shiffers نامیده میشود تغییرات در زمان پاسخ از میزبانها

را محافظت میکند و اگر میزبانهای در حال پردازش ترافیکهای بیشتری از ترافیک خودشان باشند تعیین میکنند . یکی از ابزارهای نرم افزاری امنیت شبکه که از صنایع Lopht در دسترسی است که Anti shiffer نامیده میشوند .

به آدرس زیر مراجعه کنید :

URL : http//www .lopht .com/antisniff/

٤ – cryptography (رمزنگاری – پنهان شناسی) :

موثرترین روش برای شماره peacker shifferها جلوگیری و یا محافظت از آنها نیست اما آنها را میتوان به طور نامشخصی منتقل کرد . اگر یک کانال ارتباطی امن به طور رمزنگاری باشد یک peacker shiffer فقط داده ای را که میتواند تشخیص دهد یک متن رمزنگاری شده است (ظاهرا یک رشته تصادفی از بیتها)اما پیام اصلی نیست . سطوح شبکه CISCO بر پایه امنیت IP است . IPSEC روشهای استانداردس است برای ابزارهای شبکه تا با بکارگیری IP بطور اختصاصی بهم مرتبط شوند . بقیه پروتکلهای رمزگزاری برای مدیریت شبکه شامل لایه امن (SSH) و لایه های سوکت امن (SSL) هستند .

II – IP Spoofing :

یک حمله Ip Spoofing وقتی اتفاق می افتد کهٔک Hacker داخل یا خارج شبکه وانمود کند کهٔک کامپیوتر معتبر است یک Hacker میتواند این کار را بهٔکی از دو روش ممکن اجرا کند . یک hacker یا از یک آدرس IP که در داخل آدرسهای IP معتبر است استفاده میکند و یا از یک آدرس IP خارجی که معتبر شده است و از طریق آن دسترسی به منابع خاص که روی یک شبکه فراهم شده است استفاده میکند . حلمه های Ip Spoofing اغلب نقطه شروع حمله برای سایر حمله ا هستند . مثال کلاسیک یک حمله از طریق POS برای استفاده که درسهای منبع Spoof شده برای مخفی کردن هویت Hacker ها است .

به طور طبیعی Ip spoofing (کلاهبرداری IP) محدود شده است به تزریق دادهٔا دستورات مخرب به داخل یک رشته موجود از داده است که این یک برنامه کاربردی Client / server و یا یک ارتباط شبکه ای Pear-to- pear است برای فعال کردن ارتباط دوطرفه Hacker rها باید همه جدولهای مسیریابی به نقطه آدرس Ip Spoofing شده را تغییر دهد .

روش دیگر بعضی وقتها Hacker ها نگران دریافت پاسخی از برنامه کاربردی نیستند . اگر یک Hacker سعی کند که فایل های حساسی را از سیستم بدست آورد ، پاسخهای برنامه کاربردی مهم نیست . اگر تصمیم به تغییر جداول مسیریابی

بگیرد تا به آدرس IPتقلبی اشاره کند ، این Hacker میتواند تمام بسته های شبکه را که به این آدرس تقلبی ارسال می شوند دریافت کند و پاسخ آنها را مانند کاربران واقعی دیگر بدهد .

تهدیدهای Ip Spoofing میتواند تعدیل شود نه اینکه حذف گردد برطبق توضیح زیر:

۱ – Access control (کنترل دسترسی):

عمومی ترین روش برای جلوگیری از Ip spooling ساختار کنترل دسترسی است . برای کاهش تاثیر Ip spooling کنترل دسترسی ایجاد میشود که هر عبور و مروری از شبکه های خارجی کهٔک آدرس منبع دارد و باید در کنار شبکه داخلی باشد را رد کند . توجه باید کرد این روش کمک می کند به جلوگیری از حمله های Ip spoolingها اگر و فقط آدرسهای داخلی معتبر شده باشند اگر بعضی از آدرسهای خارجی معتبر باشد این روش تاثیری ندارد .

۲ – فیلتر RFC 2827 :

شما همچنین میتوانید جلوگیری کنید از کاربران شبکه درSp کردن سایر شبکه ها از طریق جلوگیری هر عبور و مرور خارج از باند (محدوده) شبکه تان که آدرس منبع آن در دامنه IPهای شناخته شده شما نباشد .

ISP شما نیز میتوانید این نوع فیلترها را پیاده سازی کند که به طور مفصل در RFC2827 به آنها اشاره شده است .

موثرترین روش برای کاهش خطوط Ip spooling مشابه کاهش خطر pocker shifferها هستند . Ip spooling فقط وقتی به درستی میتواند فعالیت کند که ابزارها از آدرس IP ای که بر پایه تصدیق است استفاده کنند . به هر حال اگر شما از روشهای تصدیق جمعی استفاده می کنید . حمله های Ip spool نامعین است . تصدیق رمزنگاری بهترین شکل تصدیق جمعی است اما اگر در دسترس نباشد تصدیق دوجزئی قوی تر که از OTP استفاده میکند نیز میتواند موثر باشد .

III- Denial of sevice (عدم پذیرش سرویس) :

مطمئنا عمومی ترین شکل حمله حمله های عدم پذیرش سرویس است که از جمله سخترین حمله های برای حذف بطور کامل است . حتی در مجموعه hackerها حملات Dos حملاتی جزئی تلقی شده و مشکل ساز می باشند چرا که با تلاش اندکی اهداف خود راعملی می سازند . این حملات بخاطر سهولت عملکرد و آسیبهای جدیشان مستلزم توجهی خاص از سوی مجریان امنیتی هستند . چنانچه علاقه مندید تا در مورد این حملات بیشتر بدانید تحقیق در مورد روشهای اتخاذ شدهتوسط بعضی از مشهورترین حملات مفید میباشد این حملات عبارتند از:

۱ – TCP SYN Flood

۲ – ping of Death

۳ – tribe flood Network (TFN) and (TFN 2x)

Trinco – ۴

stachelrrants – ۵

Trinity – ۶

حمله های dos با بیشتر حمله های دیگر متفاوت است زیرا به طور کلی هدف آن گرفتن دسترسی به شبکه شما یا اطلاعات روی شبکه شما نیست . این حمله ها متمرکز شده اند بر روی غیر قابل دسترسی نمودن یک سرویس برای استفاده معمولی از آن که به عنوان نمونه از محدودیت بعضی از منابع را از روی یک شبکهٔا در درون یک سیستم عامل یا برنامه کاربردی خارج می کنند هنگامی کهٔک برنامه کاربردی سرور یک شبکه خاص مانند یک سرویس دهنده وب یا یک سرویس دهنده FTP موجود است این حمله هامیتوانند متمرکز شوند برای بدست آوردن و باز نگاه داشتن همه ارتباطات موجود که توسط آن سرور پشتیانی میشوند به طور موثر کاربران معتبر را سرور یا سرویس را خارج می کند .

حملات DOS همچنین می توانند پیاده سازی شوند برای پرونکلهای معمولی اینترتن همانند TCP و پروتکل کنترل پیام اینترنت (ICMP) بیشتر حملات DOS نقاط ضعف معماری سیستمی که مورد حمله قرار گربته استفادعه می کند به نسبت خطاهای سخت افزاری یا حفره های امنیتی .

اگر چه تفضی حملات داندمان شبکه شما را به مخاطره می اندازند با مشعول کردن شبکه بوسیله بسته های شبکه نامطلوب و اغلب بی مصرف و بوسیله ایجاد کردن اطلاعات نادرست درباره ضعیت منابع شبکه .

اگر ترافیک به معنای این باشد که پهنای باند موجود شما قبلا مصرف شده است . وقتی این نوع حمله از بسیاری از سیستمهای مختلف داخل میشوند در یک احظه اغلب رجوع می کنند نمایانگر یک حمله سرویس گسترش یافته است .

تا ثیر حملات DOS با پیروی از این سه روش کاهش می یابد .

: Anti spolf Features – ۱

پیاده سازی یک خصوصیات Anti spool بر روی routerها و firewall های شما میتوانید این دیسک را کاهش دهد . که این شامل فیلتر کردن RFC 2827 مینیمم است .اگر Hacker ها نتوانند هویت خود را بپوشانند ممکن نیست حمله کنند .

: Anti – Dos Features – ۲

تهیه و پیاده سازی ترکیبات Anti – Dos بر روی Routerها و fire wall ها میتواند به محدود کردن تاثیرات یک حمله کمک کند . این ترکیبات اغلب محدودیتهایی را روی محتوای نصف ارتباطات در بر می گیرد ، کهٔک سیستم اجازه دارد در هر لحظه باز باشد .

:Traffic rate limiting – ۳

یک سازمان میتواند محدودیت سرعت ترافیک را پیاده سازی کند بوسیله ISPتان این نوع فیلتر کردن حجم غیرضروری ترافیک را محدود میکند که از بخشهای شبکه با سرعت مشخصی عبور میکند . مثال معمولی محدود کردن محتوای ترافیک ICMP که اجازه دارد وارد شبکه شود بخاطر اینکه این تنها راه برای شناخت هدف و منظور می باشد . ICMP بر پایه حملات DDOS متداولتر هستند .

: Password Attacks – IV

Hacker ها می توانند با چندین روش مختلف حمله به رمزهای عبور را پیاده سازی کنند ، این حملات ناشیانه شامل ، برنامه های Trojan Hourse ، IP Spoofing ، و Packet Sniffer ها هستند .اگر چه Packet Sniffer ها و IP Spoofing
می توانند شماره کاربر و رمز های عبور را واگزار کنند ، حمله به رمز عبور اشاره می کند به تلاشهای مستمر برای شناسائی شماره کاربر و یا رمز عبور . این تلاشهای مستمر حملات ناشیانه نامیده می شود .

تغلب یک حمله ناشیانه ، مهیا کردن یم برنامه است که در کنار شبکه اجرا می شود و تلاش می کند تا به منابع مشترک داخل شود . مثلا یک سرور هنگامی که Hacker ها بطور موفقیت آمیزی به منابع دسترسی پیدا کردند و آنها قوانین مشابهی را برای کاربران اعمال کنند ، که شماره دسترسی آنها برای دسترسی به منابع سیستم فاش شود . اگر شماره دسترسی مصونیت کافی داشته باشد ، Hacker ها می توانند یک وسیله نهانی را برای دسترسی بعدی ایجاد می کنند بدون اینکه نگران وضعیتها و رمز های عبور برای شماره دسترسی کاربران سازشگر داشته باشند .

مشکل دیگری وجود دارد ، بوسیله کاربرانی که رمز عبور یکسانی دارند برای تمام سیستمهایی که به آنها وصل می شوند . اغلب ، اینها شامل سیستمهای شخصی ، سیستمهای شرکتها و سیستمهای روی اینترنت می باشد . بخاطر اینکه این رمز عبور به همان اندازه امن است که بیشتر میزبانان ضعیف مدیریتی آنها که شامل آ ن میباشند امن هستند ، و اگر آن میزبانان بوسیله Hacker هایی که تمام دامنه میزبانها یی را که رمز عبور مشابه دارند به مخاطره بیفتند . شما می توانید براحتی جلوی حملات به رمز عبور را بگیرید به وسیله اعتماد نکردن به رمز های عبور متنی معمولی دراملین مرحله ، بکارگیری OTP و یا رمزهای موثق و صحیح می توان بطور مجازی از تهدیدات . حملات به رمزعبور جلوگیری کنید . بدبختانه ، نه همه برنامه های کاربردی نه میزبانها و نه ابزارها این روشها را پشتیبانی نمی کنند وقتی که رمزهای عبور استاندارد بکارگرفته شود ، این مهم است که رمز عبوری انتخاب شود که مشکل حدس زده شود ، رنز عبور باید حداقل دارای ۸ کاراکتر طول باشد وکه شامل حروف بزرگ وکوچک و اعداد و کاراکترهای مخصوص باشد(ّ ٪ #) .بهترین رمزهای عبور بطور تصادفی تولید می شوند ، که برای بخاطر سپاری خیلی سخت هستند و اغلب کاربران را راهنمائی کنید که رمز عبورشان را بنویسند .

پیشرفتهای گوناگون مشروط به حفظ و نگهداری رمز عبور وجود دارد هم برای کاربر و هم مدیر . نرم افزارهای کاربردی اکنون وجود دارند که می توانند یک لیست از رمزهای عبور را که بر روی یک کامپیوتر دستی وجود دارد را رمز گشائی می کند . این به کاربران امکان می دهد که فقط یک رمز عبور را خاطر بسپارند و بقیه کلمات عبور بطور مطمئن در یک برنامه کاربردی ذخیره شود . از لحاظ مدیریتی ، راهای گوناگونی برای حمله ناشیانه به کلمات عبور خودتان وجود دارد . یکی از این روشها شامل بکارگیری ابزاری است که جامعه Hacker ها آنرا Lophtcrack می نامند . Lophtcrack حملات ناشیانه به کلمه عبور Win NT است و می تواند نشان دهد که کاربر چه وقت یک کلمه عبور را انتخاب می کند که بسیار ساده حدس زده می شود .

برای اطلاعات بیشتر به آدرس URL زیر مراجعه کنید :

URL : http://www .lopht .com/lophtcrack

(MITM) :man – in - the - middle Atteck – V

یک حمله (MITM) نیازمند این است که hacker به بسته های داده شبکه که در جریان هستند دسترسی داشته باشد . مثالی در رابطه با این ساختار شخصی میتواند باشد که برای یک ISP کار میکند کسی است که به تمامی داده های شبکه که بین کارکنان شبکه و هر شبکه دیگری رد و بدل میشود دسترسی دارد . این چنین حمله هایی اغلب با بکارگیری Packer shiffer ها و مسیریابی و انتقال پروتکلها پیاده سازی میشود . ممکن است راه بکارگیری این چنین حمله هایی دزدی اطلاعات و تجزیه و تحلیل ترافیک شبکه برای راندن اطلاعات مربوط به شبکه وکاربران آن ومسدود کردن سرویس انتقال نادرست داده ومعرفی اطلاعات جدید به بخشهای شبکه .

حمله (MITM) به طور موثری میتواند کاهش یابد فقط در راستای بکارگیری رمزی و پنهانی اگر یک نفر داده ها را بدین یک جلسه پنهانی خصوصی به سرقت ببرده همه چیزی کهٔک hocker خواهد دید . یک متن رمزنگاری شده است و نهٔک پیام واقعی – توجه کنید اگر یک Hocker بتواند اطلاعاتی را درباره جلسه پنهانی (رمزی) بیاموزد حمله (MITM) هنوز هم ممکن خواهد بود .

:Application layer Attoeks – VI

حمله به لایه نرم افزاری میتواند بوسله متدهای مختلفی پیاده سازی شود . یکی از متداولترین متدهای موجود استخراج کامل نقاط ضعف در نرم افزار است که معمولا بر روی سرویس دهنده ها موجود هستند مانند ارسال کننده پیامها HTTP و FTP با استخراج این ضعفها با اجازه رمز عبور به کامپیوترها دسترسی پیدا کرده و برنامه ها را اجرا کنند که مصونیت ویژه ای به سطوح دسترسی سیستم میدهد .

این حمله به لایه های نرم افزاری به صورت گسترده آشکار خواهد شد در تلاشی که به مدیر اجازه اصلاح کردن مشکلات را میدهد. بدبختانه بیشتر Hacker ها مشترک این لیستهای پستی ارسالی می شوند . که نتایج چیزهایی که تا کنون آموخته امد حمله در زمان یکسان است (اگر آنها را نتوانیم قبلا شناسائی کنیم) .

اولین مشکل به لایه برنامه کاربردی این است که آنها اقلب از پورتهایی که از فایروال می گذرد استفاده می کند . به عنوان مثال حمله کنندگان به برنامه آسیب رسانی را بر علیه سرویس دهنده های وب اجرا کنند که اغلب از پورت TCP 80 برای حمله استفاده میکنند . حمله به لایه های نرم افزاری هیچگاه بطور کامل برطرف نمیشود بهترین راه کاهش این دیسک خوب بودن سیستم است . برای کاهش این ریسک باید از یکسری مقیاسها استفاده کنیم .

۱ – خواندن OS و فایلهای Log شبکه (ثبت وقایع) و تجزیه و تحلیل آنها بوسیله برنامه های تحلیلی ثبت وقایع

۲ – نگهداری OS و نرم افزارهای موجود بوسیله latex patchesها

۳ – بعلاوه برای تهیۀک مدیر سیستم بکارگیری (intrusion detection system) میتواند در رسیدن به این هدف ما را یاری کند و دو نوع تکنولوژی IDS وجود دارد .

۴ – NIDS: IDS متکی به شبکه کار می کند بوسیله مشاهده تمام بسته هایی که در دامنه عمومی دچار تصادم میشود وقتی که NIDS یک بستۀا سری از بسته هایی را که مظنون به حمله هستند را مشاهده میکند میتواند آشکار کند یا ادامه فعالیت را قطع کند .

۵ – HIDS: IDS بر پایه ضربان بوسیله درج یک واسط به میزان إنرا محافظت میکند .

۶ – سیستم IDS کار میکند با بکارگیری امضا حمله کننده امضاء حمله کننده Profile است که برای یک حمله خاص یا نوعی حمله بکار میرود . آنها شرایط معین بخصوصی دارند که باید قبل از اینکه متوجه وجود یک حمله در ترافیک شبکه باشیم انتقال انجام شود . در جهان فیزیکی IDS را میتوان با یک سیستم هشدار دهندۀا دوربینهای حفاظتی مقایسه کرد .

بزرگترین محدودیت سیستمهای IDS اعلانهای درست و غلطی است که این سیستم بخصوص تولید می کند . وفق دادن IDS برای جلوگیری از چنین اعلانهای غلط خطرناک است برای واکنشهای بموقع IDS در شبکه .

: Network Reconnaissance – VII

شناسایی شبکه رجوع میکند به وقایعی که اطلاعاتی را در رابطه با شبکه های مورد نظر از طریق بکارگیری اطلاعات آماده و برنامه های عمومی به ما می دهد . وقتی که hackerها تلاش میکنند به شبکه نفوذ کنند آنها اغلب احتیاج دارند که اطلاعات بیشتری را درباره شبکه بدانند قبل از اینکه حمله اتفاق بیفتد که این میتواند به فرم سوالهای DNS Ding sweep, و پیمودن پورت باشد . سئوالهای DNS میتواند اطلاعاتی از قبیل صاحب دامنه اختصاصی و آدرسی که به این دامنه اختصاص دارد را معلوم کند . Ping sweeps این آدرسها بوسیله سئوالهای DNS مشخص میشوند و میتواند یک

تصویر زنده از میزان را در یک محیط اختصاصی آشکار کند . بعد از اینکه این چنین فهرستی تولید شده ابزارهای همایش درگاه (پورت) میتوانند تمام درگاهها را به صورت دوره ای شناسایی کرده تا پست کامل سرویسهای اجرایی در میزبان شناخته شود . سرانجام hackerها میتوانند ماهیت برنامه های در حال اجرا بر روی میزبان را بررسی کنند . این اطلاعات بخصوص سودمند هستند برای وقتی که hackerها تلاش میکنند که سرویس ها را به مخاطره بیندازند .

نمی توان بطور کامل از شناسائی شبکه جلوگیری کرد . اگرICMP ارسال شود و پاسخ آن در مسیریابهای حاشیه ای گرفته شود ، بطور مثال ،Ping Swap (بررسی نسیر ابتدا و انتهای نودها) می تواند متوقف شود انا در قبال آن شبکه شناسائی شده است . اگر چه پیمایش پورت می تواند به آسانی بدون Ping Swap کامل که زمان گیر است انجام شود ، بخاطر اینکه آنها احتیاج دارند که آدرس رابیابند که ممکن است مؤثر نباشد .IDS در شبکه ودر سطوح میزبان غالبا می تواند مدیر شبکه را کند وقتی که احتمال وقوع یک حمله شناسائی قوت گیرد .این به مدیر اجازه میدهد که بهتر آماده شود برای وقوع حمله احتمالی و یا به ISP خبر میدهد جائی که میزبان سیستم است که جستجوی حملات شناسائی به آنجا وارد می شود .

:Trust Exploitation –VIII

. یک شبکه سراسری (محیطی) یک مثال کلاسیک است . بخشهای این شبکه اغلب DNS و HTTP, SMTP خواهد بود بخاطر اینکه همه آنها در یک بخش همسان مقیم هستند به مخاطره انداختن یک سیستم ممکن است باعث به مخاطره افتادن سیستمهای دیگر شود . بخاطر اینکه آنها ممکن است اعتماد سیستمهای دگیر را جذب کند تا به شبکه مشابه ای متصل شود . سیسستمهای بیرون از فایروال نباید بطور کامل به سیستمهای داخل فایروال اعتماد کنند ، انچنین اعتمادی باید محدود شود بوسیله پروتکلهای ویژه و باید تصدیق شود بوسیله چیزی به غیر ازیک آدرس IP اگر ممکن باشد . مثال دیگر سیستمی است که خارج از یک دیواره آتش است یک ارتباط معتبر با سیستمی که داخل دیواره آتش است برقرار میکند .

وقتی که سیستم خارجی به مخاطره بیفتد میتواند باعث نفوذ و حمله به شبکه داخلی شود به واسطه این ارتباط معتبر شما میتوانید حمله های بر پایه جلب اعتماد را به وسیلهٔک محدودیت مداوم بر روی سطوح معتبر در داخل یک شبکه را کاهش دهید .

سیستمهای خارج دیواره آتش هرگز نباید کاملا مورد اعتماد سیستمهای داخل دیواره آتش باشد این اعتماد با محدود به پروتکلهای خاصی باشد و باید در صورت امکان با چیزی غیر از آدرس IP رسمیت پیداکند .

: Port Redirection – Ix

راهنمای مجدد پورت (درگاه)یک نوع از حمله های Trist Exploitation است که از یک میزبان سازشگر برای عبور دادن ترافیک از میان یک دیواره آتش بهره می برد که در غیر اینصورت ارتباط قطع خواهد شد . یک دیواره آتش به همراه

سه رابط و یک میزبان روی هر رابطه در نظر بگیرید . یک میزبان خارجی میتواند به میزبان بخش سرویسهای عمومی برسد اما به میزان داخلی دسترسی ندارد . میزبان موجود در بخش سرویسها ی عمومی میتواند به هر دو میزبان داخلی وخارجی متصل شود . اگر Hackerها قادر باشند که میزبان بخش سرویسهای عمومی را به مخاطره بیندازند آنها میتوانند نرم افزاری را نصب کنند که ترافیک را از میزبان خارجی به طرف میزبان داخلی هدایت کند . اگر چه هیچ ارتباط قوانین پیاده سازی در دیواره آتش را نقض نمی کند میزبان خارجی اکنون به واسطه راهنمایی مجدد پورت روی میزبان سرویس دهنده های عمومی به میزبان داخلی متصل شده است . Net cat نمونه برنامه ای است که این چنین دسترسی را فراهم میکند .

تعیین جهت مجدد پورت اصولا میتواند بواسطه بکارگیری مدلهای مناسب و مطمئن متصل شود یک سیستمی که مورد حمله قرار گرفته میتواند از IDSهای متکی بر میزبان برای شناسایی وجلوگیری از نصب چنین امکاناتی بر روی میزبان توسط Hackerها جلوگیری کند .

: Unthorized Access – X

این نوع بخصوصی از حمله ها نیست حمله های دسترسی غیر مجاز برمی گردد به اکثر حملاتی که علیه شبکه ها امروزه انجام میشود . بدین ترتیب برای بعضی از افرادی که از رمز ورود به telnet بطور ناشیانه استفاده میکنند آنها ابتدا باید اعلان TelNet روی سیستم بعد از اتصال به پورت TelNet بگیرند کهٔک پیغام باید نشان داده شود .

برای استفاده از منابع به مجوز نیاز است . اگر Hacker به تلاش خود برای دسترسی ادامه دهد اعمال او غیر مجاز میشود این اعمال و حمله ها میتواند به هر دو صورت از درون و بیرون شبکه شروع شود .

تکنیکهای کاهش حمله دسترسی غیرمجاز بسیار ساده هستند که شامل کاهش یا حذف توانایی Hackerها برای دسترسی و استفاده از سیستم با پروتکلهای غیر مجاز هستند یک مثال این خواهد بود که از دسترسی hackerها به پورت TelNet یک سرور که مجهز به ارائه سرویسهای وب به بیرون است جلوگیری کنند .

اگر hacker نتواند به این پورت برسد حمله او بسیار سخت میشود . تابع اصلی یک دیواره آتش در یک شبکه جلوگیری کردن از حمله های ساده غیرمجاز میباشد .

:Virus and trogan Hours Application – XI

آسیب های اصلی برای ایستگاههای کاری کاربران نهایی ویروسها و حمله های Trojan horse هستند یک مثال از یک ویروس برنامه است که وصل شده به Command . Com که فایلهای معینی را حذف میکند و هر نسخه دیگری از Command . Com را آلوده میکند .

یک مثال نزدیک TroJan Hourse یک نرم افزار کاربردی است کهٔک بازی ساده را بر روی ایستگاه کاری کاربر به اجرا درمی آورد . هنگامی که کاربر بوسیله این بازی مشغول شده است . این Trojan horse کپی از آن را برای هر کاربر

دیگری که در آدرسش در کتابخانه آدرسهای کاربر وجود دارد می فرستند . سپس بقیه کاربران این بازی را دریافت کرده و با آن بازی میکنند . بدین وسیله Trojan hourse انتشار می یابند .

نرم افزارهای ضد ویروس میتوانند بیشتر ویروسهای و برنامه های کاربردی Trojan hourse را تشخیص دهند و از گسترش آن در شبکه جلوگیری کنند از آنجایی که ویروسهای جدید و برنامه های کاربردی Trojan hourse به وجود می آیند داشتن برنامه های ضد ویروسی بروز و نسخه های کاربردی آن ضروری است .

یک روش امنیتی چیست

متد های امنیتی می تواند به سادگی یک روش قابل قبول برای منابع شبکه باشد یا می تواند چند صد صفحه باشد وجزییات هرقطعه امن اتصال و روشهای امن ارتباط را شروع دهد . اگر چه تا اندازه ای وسعت کمی دارد ، RFC 2196 به شایستگی یک روش امنیتی را در زیر شرح می دهد . یک روش امنیتی شرح دقیق قوانین است بوسیله اشخاصی که به آنها اجازه دسترسی به قسمت فنی سازمان و اطلاعات موجود داده شده است . این مقاله تلاش نمی کند داخل جزئیات گسترش روشهای امنیتی وارد شود . RFC 2196 حاوی اطلاعات خوبی در رابطه با این موضوع می باشد و مکانهای زیادی در وب حاوی مثالهایی از روشهای و رهنمودها هستند .

صفحات وب زیرین ممکن است خوانندگان علاقه مند را کمک کند .

- RFC 2196 کتاب جیبی امنیت شبکه

URL :http://www .ietf .org/rfc/rfc2196 .txt

- یک روش امنیتی ساده برای دانشگاه النویز

URL : http://aits .ullinois .edu/security/securestandard .html

- طراحی و پیاده سازی روشهای امنیتی یک شرکت

URL : http://www .knowcisco .com ./content/1578700434/cho06 .shtml

ضرورت داشتن یک روش امنیتی

این مهم است که بفهمیم که امنیت شبکهٔک فعالیت روبه رشد است . هیچ کس نمی تواتند یک سازمان امن بسازد .یک شبکه امن درست از ترکیب محصولات مختلف و سرویسهای ترکیبی شکل می گیرد بوسیلهٔک روش امنیتی جامع و یک ارجاع به طرفداران این روش از راس سازمان به پایین است .

در واقع یک پیاده سازی صحیح و متد امنیتی بدون اهدا ، سخت افزار امن برای کاهش تهدیدات منابع مهم مؤثرتر است از پیاده سازی جامع با محصولات امن ولی خط مشی متحد باشد .

دیدگاه معماری (overview)

مبانی طراحی

SAFE بطور بسیار سر بسته نیازهای کاربردی شبکه های سازمانی امروزی را سر مشق و الگوی خود قرار داده است . اتخاذ تصمیات پیاده سازی بسته به نیازمندی های کاربردی شبکه قابل تغییراست . به هرحال در ادامه اهداف طراحی با توجه به اولویت جهت راهنمایی دراتخاذ تصمیم بطور فهرست وار ارائه شده است:

- امنیت و تخفیف حملات مبتنی بر سیاست
- پیاده سازی امنیت از طریق زیر ساخت (نه فقط از طریق تجهیزات امنیتی خاص)
- مدیریت و گزارشگیری امن
- تصدیق و مجوز دهی کاربران Administrator ها در مورد منابع بحرانی شبکه
- تشخیص ورود غیر مجاز برای منابع و زیر شبکه های بحرانی
- پشتیبانی برای نرم افزارهای شبکه ای جدید

در درجه اول SAFE یک معماری امنیتی است . آن باید از اکثرحملات به منابع تاثیر پذیر و با ارزش شبکه جلوگیری کند .

حملاتی که موفق به نفوذ در اولین خط دفاعی می شوند و یا اینکه از داخل شبکه آغاز می گردند باید با دقت شناسایی شوند و جهت به حداقل رساندن اثرشان بر روی بقیهٔ شبکه ، از آنها جلوگیری بعمل آید . به هر حال که هیچ خطری شبکه را تهدید نمی کند و محیط کاملا" امن است باید فراهم نمودن خدمات بحرانی و اورژانسی که حمله مورد انتظار و نیاز کاربران است ادامهٔابد .

امنیت شبکهٔ مناسب و همچنین کارآیی خوب شبکه می تواند همزمان تامین شود . معماری SAFE راهی ریشه ای برای طراحی شبکه نیست بلکه صرفا" نقشه ای برای امن نمودن شبکه هاست .

همچنین SAFE ، ارتجاعی و مقیاس پذیر (قابل توسعه) می باشد . خاصیت ارتجاعی در شبکه افزونگی (Redundancy) را نیز ، جهت جلوگیری از خرابی یک دستگاه شامل می شود خواه بدلیل نقص پیکربندی اشکالات فنی ، و یا حملات شبکه ، بوجود آمده باشد .

با وجود اینکه طراحی ساده تر نیز امکان پذیر است خصوصا" کارآیی بسیار زیاد در شبکه مورد نیاز نباشد این مستند به عنوان مثال ، از یک طراحی مختلط استفاده می نماید . زیرا پیاده سازی امنیت در یک محیط مختلط بسیار پیچیده تر از محیط های ساده می باشد . انتخاب هایی جهت محدود ساختن پیچیدگی طراحی درتمام این مستند ، مورد بحث قرار گرفته است .

در روند طراحی شبکه شما در بسیاری از جاها نیاز دارید که بین استفاده از کارآیی مجتمع دریک ابزار شبکه و یا وسیلهٔ کاربردی خاص یکی را انتخاب نمایید . کارآیی مجتمع اغلب از جذابیت بیشتری برخوردار است ، زیرا می

توانید آن را بر روی تجهیزات موجود پیاده سازی نمایید و یا اینکه این خصوصیات می توانند برای تامین یک راه حل کاربردی بهتر با بقیه تجیزات کارکنند . اغلب تجهیزاتی که هنگام نیاز به وظیفه مندی (Fanctionality) بالا ، مورد استفاده قرار می گیرند خیلی پیشرفته هستند ویا زمانی که کارآیی (Performance) مورد نیاز می باشد سخت افزارهای تخصصی مورد استفاده قرار می گیرند . تصمیم گیری هایتان را بر اساس ظرفیت وظیفه مندی تجهیزات در مقابل مزیت مجتمع سازی یک وسیله انجام دهید . به عنوان مثال شما می توانید بعضی از اوقات از یک Cisco IOS Router مجتمع شدهٔ ظرفیت بالا ، با نرم افزار IOS Firewall بجای یک IOS Router کوچکتر ، با یک Firerwall مجزا استفاده نمایید . در این معماری هردو نوع سیستم ها بکارگرفته شده است . اغلب وظایف امنیتی بحرانی در شبکه های سازمانی بزرگ به دلیل نیاز به کارآیی ، به تجیزات اختصاصی واگذار می شوند .

مفهوم ماژول

رشد نیازمندی های سازمانها به IT ، موجب تکامل شبکه های سازمانی شده است . معماری SAFE برای شبکه های سازمانی ، از یک ساختار ماژولار به صورت Green- Field استفاده می کند .

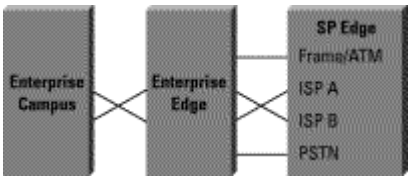
روش ماژولار دو مزیت اصلی دارد :

اول اینکه به معماری اجازه می دهد که رابطهٔ امنیتی بین بلوک های کارکردی مختلف در شبکه را نشان دهد .

دوم اینکه به طراحان اجازه می دهد که بجای تلاش بر روی معماری کامل در یک فاز امنیت را در یک ماژول بر اساس ساختار ماژولار ارزیابی و پیاده سازی کنند .

شکل ۱ ، اولین لایهٔ تقسیم بندی ماژولها (ماژولاریتی) را در معماری SAFE نشان می دهد .

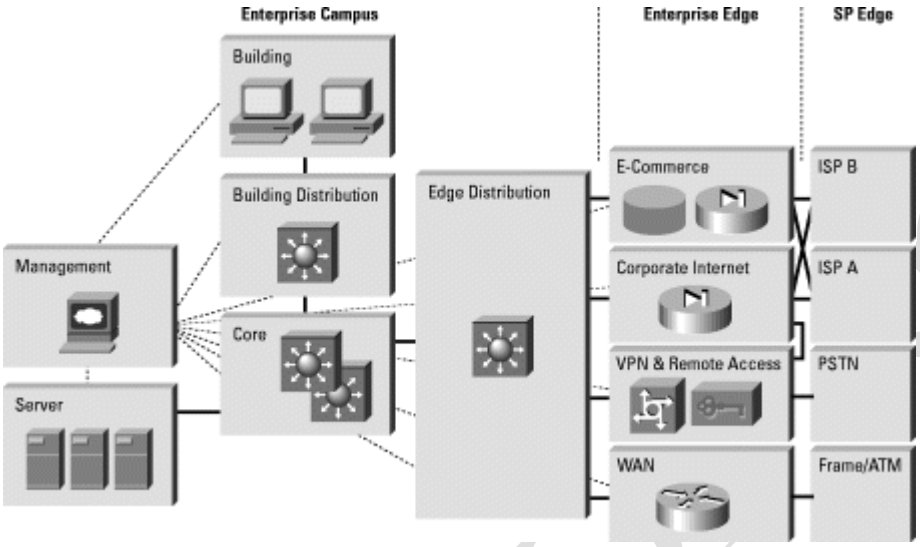
هر بلوک یک محدودهٔ وظیفه مند را نشان می دهد . دریک سرویس دهندهٔ اینترنت (ISP) ماژول توسط سازمان پیاده سازی نشده است . اما خصوصیات امنیتی خاصی را که جهت کاهش دادن حملات حتمی مورد نیاز است را شامل می شود .



شکل۱- ماژول سازمانی مرکب (مختلط)

لایهٔ دوم تقسیم بندی ماژول ها (ماژولاریتی) که در شکل ۲ نشان داده شده است دیدی از ماژول ها در هر محدودهٔ کاری ، ارائه می کند . این ماژول ها درشبکه ، نقش های خاص خود را ایفا می کنند و نیازهای امنیتی خاص خودشان

را دارند اما اندازه شان نمی تواند ابعادشان را در یک شبکهٔ واقعی نشان دهد . به عنوان مثال ، ماژول ساختمان که تجیزات کاربران نهایی را نشان می دهد می تواند شامل ۸۰ درصد از کل تجهیزات شبکه باشد .
طراحی امنیت هر واحد بطور مجزا شرح داده شده است . اما اعتبار آن به عنوان بخشی از طراحی کامل سازمان مورد بررسی قرارگرفته است .



شکل۲- بلوک دیاگرام سازمانی SAFE

حال آنکه اغلب شبکه های موجود را نمی توان به سادگی بصورت شفاف به بخش های مختلف تقسیم بندی و تشریح نمود . این روش راهنماییهایی را جهت پیاده سازی کارکردهای امنیتی متفاوت در شبکه فراهم می آورد . نوسیندگان این مستند از طراحان شبکه انتظار ندارند که شبکه هایشان را مطابق با معماری SAFE طراحی کنند اما آنها می توانند ترکیبی از ماژول های مورد بحث را بصورت مجتمع در شبکهٔ موجود بکاربرند .

قواعد کلی SAFE

روترها (Routers) هدف هستند

روترها دسترسی از هر شبکه ای را به هر شبکه ای کنترل می کنند . آنها به شبکه ها و فیلترها اعلان می کنند که چه کسانی می توانند از آنها استفاده کنند و آنها به طور پتانسیل یکی از بهترین دوستان Hacker ها هستند . روتر ، در هر آرایش امنیتی ، یک عنصر بحرانی می باشد . روترها دسترسی را فراهم می کنند ، از اینرو ، برای کاهش احتمال اینکه آنها مستقیما Hack شوند ، شما باید آنها را امن کنید . شما می توانید به مدارک دیگری که در زمینه امنیت روترها موجود است ، رجوع کنید . این مستندات ، جزئیات بیشتری را راجع به موضوعات زیر فراهم می کنند:

- قفل کردن دسترسی Telnet به یک روتر
- قفل نمودن دسترسی پروتکل مدیریت شبکه ساده (SNMP) به یک روتر
- کنترل کردن دسترسی به یک روتر از طریق استفاده از

Terminal Access Controller Access Control System Plus (TACACS+)

- خاموش کردن سرویس هایی که مورد نیاز نیستند
- واقعه نگاری (Logging) در سطوح مقتضی
- تصدیق (مجوز دهی) در به روز رسانی اطلاعات مسیر یابی

یکی از رایج ترین مطالب راجع امنیت روتر در آدرس زیر موجود است :

URL : http:// www .Cisco .Com/Warp/public/707/2 .html

سوئیچ ها (Switches) هدف هستند

سوئیچ ها (هر دو نوع لایهٔ سه و لایهٔ ۲) نیز مانند روترها به توجه در مورد مجموعه نیازهای امنیتشان نیاز دارند . بر خلاف روترها اطلاعات عمومی زیادی در مورد مخاطرات امنیتی و راه های تخفیف آن خطرات در سوئیچ ها موجود نیست . بسیاری از تکنیک های امنیتی که در بخش قبلی « *روترها هدف هستند* » به تفصیل بیان شد را می توان در سوئیچ ها استفاده نمود . بعلاوه شما باید احتیاط های زیر را انجام دهید:

- پورت ها بدون هیچ نیازی به Trunk باید تمامی تنظیمات Trunk به حالت خاموش تنظیم شود همانطور که از حالت Auto جلوگیری می شود . این کار باعث می شود که یک Host نتواند با دسترسی به یک پورت Trunk شده به ترافیکی که در حالت عادی باید بروی یک پورت Trunk شده قرارگیرد دسترسی داشته باشد .

- مطمئن شوید که پورت های Trunk شده از یک شمارهٔ شبکهٔ مجازی (VLAN) استفاده می کنند که در هیچ جای دیگری به جز سوئیچ استفاده نشده باشد . این از رسیدن Packet هایی که برچسب VLAN مشابهی را خورده اند به VLAN های دیگر بدون گذشتن از تجهیزات لایهٔ ۳ (روتر و سوئیچ های لایهٔ ۳) جلوگیری می کند . برای اطلاعات بیشتر به URL زیر مراجعه فرمایید:

URL : http: // www .sans .org/newlook/resources/ IDFAQ/ vlan . Htm

- کلیهٔ پورت های استفاده نشده از یک سوئیچ را بعنوان یک VLAN که هیچ اتصال لایهٔ ۳ ای ندارد تنظیم کنید . در عین حال ، هنوز بهتر است که پورت هایی که مورد نیاز نیستند را غیر فعال کنید . این از Hacker هایی که با اتصال به پورت های بدون استفاده با بقیهٔ شبکه ارتباط برقرار می کنند ، جلوگیری می کند .

- از بکاربردن VLAN ها به عنوان تنها روش دسترسی امن به زیر شبکه ها اجتناب کنید . استعداد برای خطای انسانی با این مسئله که VLAN ها و پروتکل های برچسب زدن در VLAN (Tagging) ، با امنیت در داخل خود طراحی نشده اند ، استفاده از آنها را در محیط های حساس دور از مصلحت می سازد . هنگامی که VLAN ها در یک آرایش امن مورد نیاز هستند ، مطمئن شویدکه پیکربندی و رهنمون های ذکر شده در بالا مورد توجه قرار گرفته باشد .

در داخل یک VLAN موجود ، VLAN های خصوصی ، کمی به امنیت شبکه در کاربردهای خاص می افزاید . VLAN های خصوصی با محدود کردن اینکه کدام پورت از یک VLAN با پورت های دیگردر یک VLAN مشابه ارتباط برقرارکند کار می کنند . پورت های ایزوله شده در یک VLAN فقط می توانند با پورت های بی قید ارتباط برقرار نمایند . پورت هایی که بصورت VLAN درآمده اند ، فقط می توانند با سایر اعضا از همان VLAN و نیز پورت های بی قید ارتباط برقرارکنند .

این یک راه موثر برای تخفیف اثرات یک میزبان Hack شدهٔ تنها است . بخشی را که دارای سرویس های استاندارد عمومی مانندWeb ،FTP و DNS مورد دسترسی غیر مجاز قرار بگیرد یک Hacker می تواند دو Host دیگر را نیز بدون به عقب برگشتن از Firewall ، مورد تعقیب قرار دهد . اگر VLAN ها را به مصا ف بیاوریم ، وقتی که یک سیستم مورد دسترسی غیر مجاز قرارگرفت ، آن نمی تواند با دیگر سیستم ها ارتباط قرار کند . اهداف یک Hacker فقط می توانند از طرف دیگر Firewall تعقیب شوند .

میزبانها (Hosts) هدف هستند

یک Host دوست داشتنی ترین هدف درطول یک حمله می باشد و سخت ترین مبارزات را از لحاظ امنیتی می طلبد . تعداد بی شماری تجهیزات سخت افزاری ، سیستم های عامل ، و برنامه های کاربردی مختلفی وجود دارند که هریک از آنها Patch ها ، Update ها ، وFix هایی دارند که درزمان های مختلفی در دسترس قرار می گیرند . زیرا Host هایی که سرویس های کاربردی را برای سایر Host ها که متقاضی آن سرویس ها هستند فراهم می کنند ، به شدت در داخل شبکه ، قابل رویت هستند . به عنوان مثال بسیاری از مردم سایت

http://www.Whitehouse.gor

،که یک Host است را دیده اند اما تعداد کمی برای دسترسی به S2-O تلاش کرده اند .

Whitehouseisp.net که این هم یک روتر است . بدلیل این پدیداری در کوشش برای ورود غیر مجاز به شبکه Host ها بیشترین تجهیزاتی هستند که مکررا" مورد حمله قرار گرفته اند .

در بخش بالا که مبارزات امنیتی مورد بحث قرار گرفت Host ها بیشترین تجهیزاتی هستندکه دسترسی غیر مجاز به آنها کاملا" موفقیت آمیز است .

به عنوان مثال یک سرور web در اینترنت باید قدرت اجرای یک Platform سخت افزاری از یک فروشنده را داشته باشد ،همینطور یک کارت شبکه از دیگری یک سیستم عامل از یک فروشنده دیگر ، و یک web سرور که یا Open Source است و یا از یک فروشنده دیگر . بعلاوه سرورهای web مشابه ، ممکن است برنامه هایی را که به صورت مجانی از طریق اینترنت توزیع شده اند را اجرا کنند و ممکن است با یک سرور بانک اطلاعاتی ارتباط برقرار کنند که همواره همهٔ اطلاعاتش تغییر می کند . این درست نیست که بگوییم آسیب پذیری امنیتی بطور خاص توسط طبیعت چند منبعی همهٔ اینها ایجاد می شود بلکه هرچه که تجهیزات ترکیبی سیستم (Complexity) آن افزایش می یابد ، احتمال وقوع اشکال هم افزایش می یابد .

برای امن کردن Host ها ، به هریک از اجزاء درون سیستم به دقت رسیدگی نمایید .کلیهٔ سیستم ها را با آخرین اصلاحات ، ثابتها ، و چنین چیزهایی به روز نگه دارید . به خصوص به این مسئله توجه کنید که این اصلاحات چه تاثیری بر روی سایر اجزا سیستم می گذارند . کلیه Update ها را قبل از پیاده سازی در یک محیط عملیاتی ، بر روی یک سیستم آزمایشی ، ارزیابی کنید .کوتاهی در انجام این کار ممکن است منجر به یک حمله از نوع در دسترس نبودن سرویس (DoS) توسط خود اصلاحات شود .

شبکه ها (Networks) هدف هستند

بدترین حمله ، حمله ایست که نتوان جلوی آن را گرفت . وقتی که DoS توزیع شده به طور مناسب و بجا انجام شود ، فقط یک حمله است . که در ضمیمه B « مبانی امنیت شبکه » ، به طور اجمالی به آن پرداخته شده است . DDoS بوسیلهٔ واداشتن دهها و یا صدها ماشین که به طور همزمان داده های جعلی را به یکIP آدرس ، ارسال می کنند کار می کند . هدف چنین حملاتی معمولا" از سرویس خارج کردن یک Host مشخص نیست ، بلکه بیشتر ناتوان کردن کل شبکه است . [کل شبکه توانایی پاسخگویی به در خواست های رسیده را نداشته باشد]. به عنوان مثال سازمانی را فرض کنید که با یک اتصال DS3 (45Mbps) به اینترنت می باشد ، و سرویس های تجارت الکترونیکی را برای کاربران وب سایتش فراهم می کند . چنین سایت هایی از نظر امنیتی بسیار آگاه و هوشیار هستند و از تجهیزات و روش هایی مانند شناسایی ورود غیر مجاز Firewall ثبت وقایع و مانیتورینگ فعال ، استفاده می کنند . متاسفانه هنگامی که یکHacker یک حملهٔ موفق DDoS را شروع می کند ، تمام این تجهیزات امنیتی نمی توانند به ما هیچ کمکی بکنند .

تعداد ۱۰۰ ابزار را که هریک دارای یک ارتباط (1.5 Mbps) به اینترنت هستند را در سراسر دنیا در نظر بگیرید . اگر از راه دور به این سیستم ها گفته شود که سیلی از اطلاعات را به واسط سریال روتر اینترنت سازمانی که سرویس تجارت الکترونیکی ارائه می دهد ، سرازیر کنند آنها می توانند بسادگی سیلی از داده های نادرست را به حجم DS3 تولید کنند . هر Host می تواند فقط 1 Mbps از ترافیک را تولید کند ، (تحقیقات آزمایشگاهی نشان می دهد که ایستگاه های کاری unix بسادگی می توانند بوسیلهٔ یک ابزار DDoS معمولی 50Mbps اطلاعات تولید کنند .)

این مقدار خود بیش از دوبرابر ترافیکی است که آن سایت تجارت الکترونیکی می تواند با آن سروکار داشته باشد .

بعنوان نتیجه درخواست های web مشروع ، گم می شوند و از دید بسیاری از کاربران بنظر می آید که سایت از کار افتاده است . یک Firewall محلی تمامی داده های نادرست را حذف می کند و بدین وسیله خسارت بوجود می آید . ترافیک از طریق ارتباط WAN عبور کرده و خط ارتباطی را اشباع می کند .

شرکت های تجارت الکترونیکی فقط از طریق همکاری با ISP هایشان می توانند امیدوار باشند که چنین حملاتی را خنثی سازند . یک ISP می تواند محدودیت نرخ ارسال را بر روی واسط خروجی به سمت سایت آن کمپانی تنظیم کند . این محدود سازی نرخ ارسال ، می تواند ترافیک های ناخواسته را زمانی که به مقدار از پیش تعیین شده ای از پهنای باند موجود می رسند حذف کند . شناسایی درست ترافیک نا خواسته ، راه حل این مسئله می باشد .

شکل های عمومی حملات DDoS ، سیل های ICMP ، TCPsyn یا UDP هستند . در یک محیط تجارت الکترونیکی ، معمولا" این نوع ترافیک را می توان بسادگی دسته بندی کرد . فقط هنگامی که یک جمله TCPsyn فقط به پورت 80 (http) محدود می شود ، سوپروایزر ریسک عدم دادن اجازهٔ ورود به کاربران مجاز را در طول حمله ، می پذیرد . حتی پس از آن بهتر است که بطور موقتی جلوی ورود کاربران مجاز را نیز بگیرد و مسیریابی و اتصالات مدیریت را نگه دارد تا اینکه یک تهاجم سراسری صورت گیرد و کل اتصال را از دست بدهد .

بیشتر حملات سطح بالا از پورت 80 استفاده می کنند . آنها با ست کردن بیت ACK بگونه ای وانمود می کنند که آن ترافیک ، یک تراکنش مشروع می باشد . احتمال اینکه سوپروایزر بتواند چنین حملاتی را دسته بندی کند ، بسیار کم است ، زیرا پاسخ ارتباطات TCP ، صحیح هستند و شبکه شما می خواهد که آنها را عبور دهد .

دنبال کردن راهنمایی های کلی مطرح شده در RFC 1918 و RFC 2827 Filtering ، می تواند شما را در محدود ساختن این حملات یاری کند . RFC 1918 ، شبکه هایی را که برای کاربردهای خصوصی رزرو شده اند و نباید از طریق اینترنت عمومی ، دیده شوند را مشخص می کند . RFC 2827 Filtering ، در بخش IP Spoofing از ضمیمهٔ B « مبانی امینت شبکه » ، مورد بحث قرار گرفته است . برای ترافیک ورودی بر روی یک روتر متصل به اینترنت ، جهت جلوگیری از رسیدن ترافیک بدون مجوز به شبکهٔ Corporate شما باید از RFC 1918 و RFC 2827 Filtering استفاده نمایید . پس از پیاده سازی این Filtering در ISP ، از Packet های حملات DDoS که از طریق پیمودن لینک WAN که این آدرسها را بعنوان مبدا بکار می برند جلوگیری می کند . پهنای باند بطور بالقوه در طول حمله حذف می شود .

در مجموع اگر همهٔ ISP های دنیا راهنمایی های RFC 2827 را بکار ببندند ، جعل آدرس مبداء بطور قابل ملاحظه ای کاهش خواهد یافت . حال آنکه این استراتژی بطور مستقیم از حملات DDoS جلوگیری نمی کند . این از حملاتی که آدرس مبدا آنها پوشانده شده است جلوگیری می کند . این کار باعث می شود که ردیابی حملات شبکه ، بسیار آسانتر گردد .

اهداف برنامه ریزی کاربردی هستند

برنامه های کاربردی (اغلب) توسط انسان ها (که موجوداتی زنده هستند) نوشته شده و می شوند ، و به همین دلیل در معرض خطاهای بیشماری قرار دارند . این خطاها ممکن است خوش خیم باشند ، بعنوان مثال یک خطا باعث می شود که مطالب شما در چاپگر به صورت غلط چاپ شود ، و یا خطرناک ، به عنوان مثال یک خطا که شماره های کارت اعتباری را بر روی سرور بانک اطلاعاتی از طریق یک FTP با نام مستعار ، در اختیار افراد قرار می دهد . این مشکلات نیز مانند دیگر آسیب پذیری های عومی امنیتی ، خطرناک هستند . که سیستم های تشخیص نفوذ غیرمجاز (ISP) ها وظیفهٔ شناسایی آنها را بر عهده دارند . کار تشخیص نفوذ غیر مجاز مثل یک سیستم هشدار دهنده ، در جهان فیزیکی عمل می کند . هنگامی که یکIDS ، چیزی را که یکحمله به نظر می رسد ، شناسایی می کند ، می تواند به دو صورت عمل نماید:

یا خود جهت جلوگیری از ورود عمل می کند و یا برای انجام عمل توسط سوپروایزر ، به یک سیستم مدیریت اطلاع می دهد . اکثر سیستم ها کم و بیش جهت پاسخگویی و جلوگیری از چنین حملاتی تجهیز شده اند . تشخیص ورود غیر مجاز می تواند بوسیلهٔ جلوگیری از درخواست های سیستم عامل و برنامه های کاربردی بر روی یک Host منحصر به فرد (خاص) انجام گیرد . همچنین می تواند توسط تجزیه و تحلیل حقیقت جویانهٔ فایل های ثبت وقایع محلی ،صورت گیرد . تا زمانی که دسترسی های قبلی وظیفهٔ یک پاسخ حملهٔ غیر فعال را بازی می کنند ، دسترسی های قبلی مارا قادر می سازند تا دفاع بهتری را در مقابل حملات انجام دهیم . به دلیل ویژگی این نقش ، سیستم های IDS مبتنی بر Host (HIDS) ، برای جلوگیری از حملات خاص ، اغلب نسبت به IDS های شبکه (NIDS) ، که معمولا" فقط در پی تشخیص حمله ، آلارم می دهند ، بهتر هستند . به هر حال این ویژگی از دید کلی باعث ایجاد خسارت در شبکه می شود . در اینجا NIDS برتری دارد . Cisco ، یک سیستم ترکیبی از هر دو سیستم را برای یک سیستم تشخیص ورود غیر مجاز توصیه می کند:

استفاده از HIDS بر روی Host های حیاتی (بحرانی) و NIDS برای نظارت بر کل شبکه . شما هنگامی که برای اولین بار یک IDS را پیاده سازی می کنید ، باید برای افزایش کارآیی آن ، و نیز کاهش پاسخ های مثبت غلط (False-Positive) ، آنرا تنظیم نمایید . پاسخ های مثبت غلط ، به عنوان هشدار هایی که توسط ترافیک مشروع و یا فعالیت زیاد ایجاد می گردند ، شناخته می شوند . پاسخ های منفی غلط (False-Negtive) حملاتی هستند که سیستم IDS از شناسایی آنها ناتوان است . زمانی که IDS تنظیم شد ، شما می توانید آنرا برای تخفیف تهدیدات خاص تر ، پیکر بندی نمایید . همانگونه که در بالا ذکر شد ، شما باید HIDS را برای توقف بیشترین تهدیدات معتبر در سطح Host پیکر بندی کنید ، زیرا این بهترین تدارک جهت تصمیم گیری است که آیا یک فعالیت خاص براستی که حمله است یا نه . هنگامی که وظایف اصلی NIDS را تشخیص دادید ، دو انتخاب اصلی وجود دارد:

اولین انتخاب اجتناب از ترافیک از طریق قراردادن فیلتر های کنترل دسترسی بر روی روتر می باشد .که در صورت آرایش نامناسب می تواند به طور ذاتی زیان آورترباشد . هنگامی که NIDS حمله ای را از یک Host خاص ، بر روی یک پروتکل خاص ، شناسایی کرد ، می تواند آن Host را بلوکه کند و از ورود مجدد او به شبکه برای مدت زمان پیش تعیین شده ای ، جلوگیری بعمل آورد . در ظاهر این توانایی ، کمک بزرگی به سوپروایزر امنیتی به نظر

می رسد ، در حقیقت در همه جا باید خیلی با دقت پیاده سازی شود . اولین مشکل از طریق آدرس های جعل شده بوجود می آید . اگر ترافیک با یک حمله مطابقت داشته باشد ، توسط NIDS شناسایی شده و آلارم مخصوص به آن ، یک پاسخ اجتناب ناپذیر را فعال خواهد کرد .NIDS ، لیست دسترسی را توسط آن آرایش خواهد داد . به هرحال اگر حمله ای که موجب آلارم شده است ، از یک آدرس جعل شده استفاده نماید ، NIDS آدرسی را که هرگز حمله را آغاز نکرده است ، قفل می نماید . اگر آدرسی راکه یکHacker بکار برده است تصادفا با IP آدرس خروجی یک http پروکسی سرور در یک ISP بزرگ یکسان باشد ممکن است که تعداد بسیار زیادی از کاربران قفل شوند . این می تواند بخودی خود ، در دست یک Hacker خلاق ، یک تهدید DoS جالب باشد .

برای کاهش خطرات Shunning شما باید آنرا فقط برروی ترافیک TCP بکار برید ، زیرا انجام عمل Spoofing موفق آمیز بر روی آن بسیار مشکل تر از UDP می باشد . آنرا فقط درزمانی که تهدید وجود دارد و احتمال پاسخ مثبت غلط بسیار پایین است ، بکار برید . به هر حال ، در درون یک شبکه ، انتخاب های بسیار زیادی وجود دارند . با صف آرایی موثر بر اساس RFC 2727 Filtering ، ترافیک spoof شده بسیار محدود خواهدشد . همچنین به دلیل اینکه اکثر مشتریان در شبکه داخلی نیستند ، شما می توانید حالت پیش گیرانهٔ بیشتری در مقابل کوشش های حملهٔ نشات گرفته از داخل شبکه ، به دست آورید . دلیل دیگر این است که اغلب شبکه های داخلی ، سطوح مشابه برای Stateful Filering را که اتصلات لبه دارا هستند ، را ندارند . در نتیجه IDS نیاز دارد که به محیط درونی ، خیلی بیشتر از محیط بیرونی ، اعتماد داشته باشد .
دومین انتخاب برای کاهش تهدیدات NIDS ، بکاربردن Reset های TCP می باشد . همانگونه که از نامش بر می آید ، Reset های TCP ، فقط بر روی ترافیک TCP کارمی کند و یک حمله فعال را با ارسال پیام TCP RESRT به Host های حمله کننده و مورد حمله قرار گرفته خاتمه می بخشد . به دلیل اینکه Spoof کردن ترافیک TCP بسیار مشکل تر است ، شما باید از بکاربردن بیش از حد TCP RESET اجتناب کنید .

از دیدگاه اجرایی ،NIDS Packet هارا برروی سیم مشاهده می کند . اگر Packet ها سریعتر از آنکه NIDS بتواند آنها را پردازش کند ، ارسال شوند ، دیگر ایرادی به شبکه وارد نیست ، زیرا NIDS به صورت مستقیم در جریان داده ها نمی نشیند . به هر حال NIDS کارآیی خود را از دست خواهد داد و Packet های از دست رفته ، می توانند موجب اختارهای غلط و یاعدم اخطار در موارد صحیح شوند . مطئن باشید که با عدم زیاده خواهی از قابلیت های IDS ، شما می توانید فواید بسیاری از آنها بدست آورید .

از دیدگاه مسیر یابی IDS ، مانند بسیاری از موتورهای State-aware ، در محیط هایی که مسیر یابی به صورت نامتقارن انجام می گیرد ، بدرستی کار نخواهد کرد . Packet ها از طریق یک سری از روترها و سوئیچ ها به خارج ارسال می شوند و از طریق دیگری به داخل شبکه بر می گردند . که این امر باعث می شود که سیستم های IDS ، فقط نیمی از ترافیک را ببنند . که این موجب بوجود آمدن پاسخ های مثبت و منفی غلط می شود .

مدیریت امنیت و گزارش گیری

« اگر شما می خواهید وقایع چیزی را ثبت کنید ، حتما" آنرا بخوانید » . یک قضیه ساده اینست که تقریبا هر کسی که با امنیت شبکه سر وکار دارد ، می گوید که این کمترین کاری است که می توان انجام داد . هنوز ثبت وقایع و خواندن اطلاعات از بیش از ۱۰۰ دستگاه مختلف را می توان به عنوان یک مشکل مطرح کرد . کدام مهمتر هستند ؟ چگونه پیام های مهم را از آنهایی که فقط حاوی اطلاعات عمومی سیستم می باشند ، جدا کنیم؟ چگونه مطمئن شویم که گزارشات هنگام عبور دستکاری نشده اند؟ چگونه مطمئن شویم هنگامی که چندین دستگاه ، یک هشدار مشابه را ارسال می کنند ، Time-Stamp ها با هم مطابقت دارند؟ اگر اطلاعات ثبت شده جهت یک تحقیق کیفری مورد استفاده قرارگیرد ، چه اطلاعاتی مورد نیاز است؟ ما با چه حجمی از اطلاعات ، که می تواند توسط یک شبکه بزرگ تولید شود ، سرو کارداریم؟ شما هنگامی که Log File های مدیریتی را به طور موثر مورد رسیدگی قرار می دهید ، باید بتوانید به کلیهٔ سوالات فوق پاسخ گویید .

از یک دیدگاه مدیریتی ، سوالات مختلفی باید پرسیده شود :

چگونه می توان یک وسیله را به صورت امن مدیریت نمود؟ چگونه می توان محتوای چیزی را به یک سرور عمومی ارسال کرد و مطمئن بود که در هنگام ارسال دستکاری نشده است؟ چگونه می توان هنگام حمله و یا بروز اشکال درشبکه ، تغییرات اعمال شده بر روی تجهیزات را برای رفع اشکال دنبال کرد؟

از یک دیدگاه وابسته به معماری ، اولین قدم در هر استراتژی مدیریت و گزارشگیری ، ایجاد مدیریت Out-of-Band بر روی سیتم های شبکه می باشد . Out-of-Band (OOB) ، همانگونه که از نامش برمی آید ، به شبکه ای اشاره دارد که تولید ترافیک در آن مستقر نیست . در چنین شبکه هایی ، تجهیزات باید که اتصال محلی مستقیم داشته باشند . درجاهایی که امکان دارد و یا امکان ندارد ، (با توجه به جغرافیا و یا بسته به نیازهای سیستم) ، برای برقرار ارتباط جهت مدیریت و گزارش گیری فقط از طریق یک پورت خاص ازقبل پیکربندی شده است .

همچنین تونل باید بگونه ای قفل شود که فقط Host های مجاز بتوانند آنرا آغاز کنند و خاتمه بخشند . مطمئن باشید که شبکهٔ Out-of-Band ، خودش نمی تواند پی آمدهای امنیتی ایجاد کند . برای جزئیات بیشتر به بخش « ماژول مدیریت (Management Module) » ، از این مقاله مراجعه فرمایید .

پس از پیاده سازی یک شبکه مدیریت OOB ، گزارشگیری و ثبت وقایع آسانتر خواهد شد . بسیاری از تجهیزات شبکه می توانند اطلاعات Syslog را ارسال کنند ، که این اطلاعات می توانند هنگام تهدیدات و یا رفع اشکال شبکه بسیار با ارزش باشند . این اطلاعات به یکیا چندین Host موجود بر روی شبکهٔ مدیریتی که وظیفهٔ تجزیه و تحلیل Log ها را بر عهده دارند ، ارسال می شود . بسته به پیچیدگی تجهیزات ، شما می توانید جهت اطمینان از صحت ارسال داده ها به دستگاه های ثبت وقایع ، سطوح ثبت وقایع مختلفی را انتخاب نمایید . همچنین شما نیاز

دارید که از طریق نرم افزار تجزیه و تحلیل ، برای اجازه دادن به دید درجه بندی شده و گزارش گیری ، علامت دهید . به عنوان مثال ، در طول یک حمله ، اطلاعات Log ارسال شده توسط یک سوئیچ لایهٔ ۲ ، ممکن است به اندازهٔ اطلاعاتی که توسط یک سیستم تشخیص ورود غیر مجاز تولید می شود ، جالب نباشد . کاربردهای خاص مثل IDS ها ، اغلب از پروتکل های ثبت وقایع خودشان برای انتقال اطلاعات مربوط به آلارم ها استفاده می کنند . معمولا" این اطلاعات باید برروی Host های جداگانه که برای مدیریت شبکه به طور مناسبی تجهیز شده اند ، ثبت شود . اطلاعات آلارم ارسال شده از منابع مختلف ، می توانند اطلاعاتی راجع به وضعیت (سلامت) کل شبکه را برای ما فراهم کنند . برای اطمینان از اینکه پیام های Log از نظر زمانی ، با دیگری ، همزمان (سنکرون) شده اند ، ساعت Host ها و تجهیزات شبکه باید همزمان باشد . پروتکل زمان شبکه Network Time Protocol (NIP) ، راهی را برای تجهیزاتی که از آن پشتیبانی می کنند ، فراهم می کند ، تا مطمئن شویم که زمان دقیق بر روی تمام تجهیزات نگهداشته شده است . هنگامی که با حملات سرو کار داریم ، ثانیه ها اهمیت دارند ، زیرا باید از اتفاقات مختلفی که در طول یک حملهٔ خاص ، در جاهای مختلف ، اتفاق می افتد آگاه شویم .

ازیک دیدگاه مدیریت ، در این مقاله ، برای تامین اهداف مورد نظر ، غیراز ثبت وقایع و گزارش گیری که بر روی یک وسیله توسط Administrator انجام می شود ، به هر تابعی که در آن نتایج و راه حل های دیگری نیز وجود داشته باشد ، مراجعه می کند . چنانکه شبکهٔ OOB ، با ثبت وقایع و گزارش گیری به انتقال اطلاعات اجازه می دهد که دریک محیط کنترل شده بمانند که در آن محیط کنترل شده ، اطلاعات در معرض دستکاری نیستند . این هنگامی برتری دارد که پیکربندی امن امکانپذیر باشد . بعنوان مثال زمانی که از لایهٔ سوکت امن Secure(SSL) Socket Layer یا پوسته امن Secure Shell (SSH) استفاده می کنیم ، پروتکل SNMP باید با مراقبت بیشتری رفتار کند ، زیرا پروتکل زیری مجموعه آسیب پذیری های امنیتی خود را داراست . فرض کنید یک دسترسی فقط خواندنی از طریق SNMP ایجاد می شود ، با توجه به رفتار عمومی رشتهٔ SNMP ، شما ممکن است دسترسی یکسانی به رمز عبور Root (admin) یک Unix Host بحرانی و نیز تجهیزات دیگر در شبکه داشته باشید [با همه تجهیزات با درجه های اهمیت مختلف به طور یکسان بر خورد می شود] .

مدیریت تغییرات پیکر بندی ، یکی دیگر از بحث های وابسته به مدیریت امنیت می باشد . هنگامی که یک شبکه مورد حمله قرار گرفته است ، داشتن وضعیت تجهیزات بحرانی شبکه اهمیت دارد و اینکه چه زمانی آخرین تغییراتی که از آن آگاه هستیم برروی این تجهیزات اتفاق افتاده است . ایجاد یک طرح برای مدیریت تغییرات باید بخشی از سیاست جامع امنیتی شما باشد . اما تغییرات رادر کمترین مقدار با استفاده از تائید اعتبار برروی تجهیزات و بایگانی پیکر بندی از طریق FTP و یا TFTP ذخیره نمایید .

ماژول Enterprise

Enterprise دو محدوده اصلی را بر می گیرد: Campus (فضای اصلی) و لبه . این محدوده خود به بخش های Enterprise options نیز مانند اکثر شبکه های دیگر به اینترنت متصل است . د رداخل این شبکه کاربرانی وجود دارند که به داخل شبکه دسترسی داشته باشند . آنجا تهدید های عمومی مختلفی وجود دارد که می تواند سازش اولیه ای راکه یکHacker برای نفوذهای آینده اش به شبکه با بهربرداری های ثانویه به آن نیاز دارد را تولید کند .

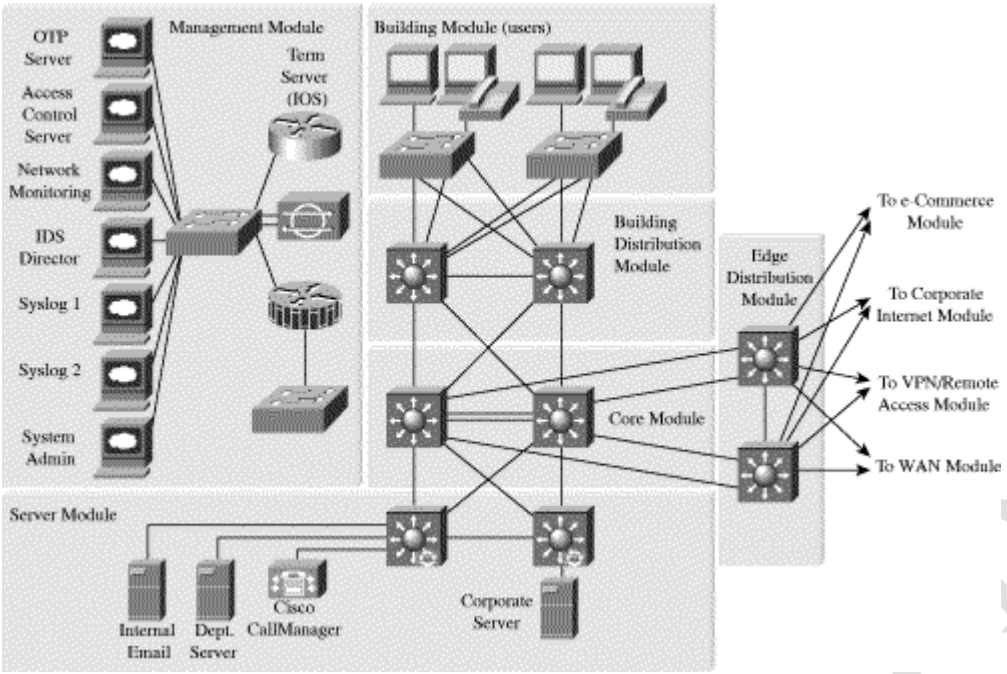
این تهدید از طرف کاربران داخلی است طبق آمادگی برحسب درصد این حقیقت به اثبات می رسد که اکثریت حملات از داخل شبکه صورت می گیرد کارمند های ناراضی جاسوس های اقتصادی میهمانان ملاقات کننده وبی توجهی و سهل انگاری بعضی از کاربران همگی منابع بالقوهٔ چنین حملاتی هستند هنگام طراحی امنیت آگاهی از پتانسیل تهدیدهای داخلی دارای اهمیت است .

دومین تهدیدHost های قابل آدرس دهی متصل به اینترنت می باشند این سیم ها به احتمال زیاد بااستفاده از آسیب پذیری های لایهٔکاربرد و حملات DOS مورد حمله قرار خواهند گرفت .

آخرین تهدید امنیت که یکWar-dialer سعی کندکه شماره تلفن مودم های شبکهٔ شمارا پیدا کرده و از طریق به شبکهٔ شما دسترسی پیدا کند War-dialer ها نرم افزار های و یا سخت افزار هایی هستند برای شماره گیری تعداد زیادی شماره تلفن و تعیین سیستمی که در طرف دیگر اتصال مشغول به کار است .طراحی شده اند آسیب پذیری سیستم سیستم های مشخص ای می باشد که کاربر نرم افزارهای کنترل از راه دور (دسترسی ازراه دور) بر روی آنها نصب کرده باشد این سیستم ها امنیت چندانی ندارند این تجهیزات پشتFirewall قرار گرفته اند هنگامی که Hacker ها از طریق شماره گیری به آن Host دسترسی پیدا کنند می توانند نقش کاربران مجاز شبکه را ایفا کنند برای توضیحات بیشتر درمورد جزئیات این تهدید به ضمیمهٔ B مبانی شبکه مراجعه فرمایید .

Enterprise Campus

در ادامه مشروحی ازماژواهایی که درداخل Enterprise Campus قرار دارند به عمل آمده است .

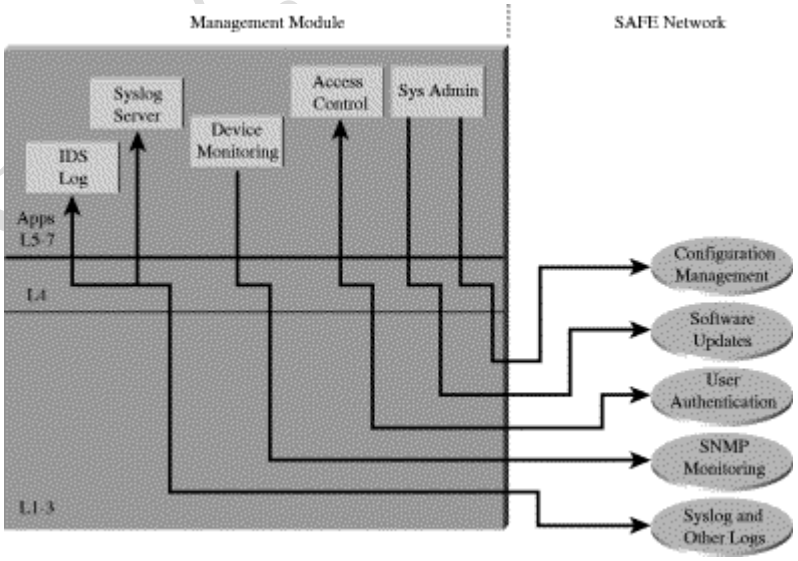


شکل ۳- جزئیات Enterprise Campus

ماژول مدیریت (Management Module)

هدف اصلی ماژول مدیریت تسهیل اعمال مدیریت امن بر روی تجهیزات . Host ها در معماری Enterprise SAFE می باشد

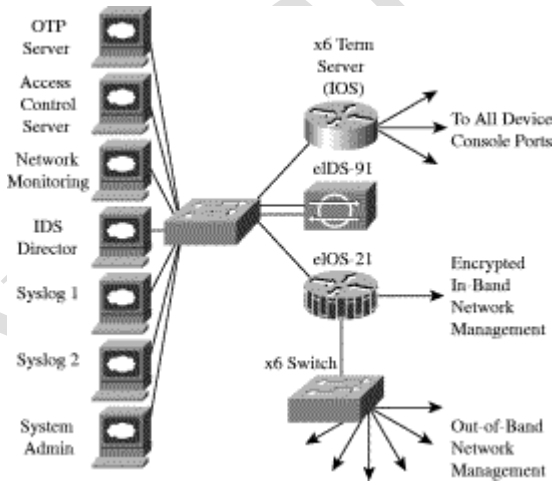
اطلاعات ثبت وقایع و گزارشگیری از تجهیزات به Host های مدیریت ارسال می شود حال آنکه محتوی پیکربندی و نرم افزاری جدید از Host های مدیریت به تجهیزات ارسال می گردد .



شکل ٤- مدیریت جریان ترافیک

ابزارهای کلیدی

- SNMP Management Hosts – مدیریت SNMP را برای تجهیزات تامین میکند .
- NIDsHost – جمع آوری هشدارها (آلارم ها) را از تجهیزات NIDS بر عهده دارد .
- Syslog Host – اطلاعات log ها را برای fire wall و Host های NIDS جمع آوری می کند .
- Access control server – خدمات تائید اعتبار به صورت two factor و one time را به تجهیزات می رساند .
- On-timepassword sevser(OTP) – اطلاعات On-timepassword پخش شده توسط Server . (سرور کنترل دسترسی) را تایید اعتبار می نمایید .
- system Admin Host – پیکر بندی نرم افزارو تغییر محتوی را بر روی تجهیزات فراهم می کند .
- NIDS appliance – مانیتورینگ لایهٔ۴ تا ۷ را بر روی تجهیزات کلیدی موجود در ماژول تامین می کند .
- Cisco IOS firewall – کنترل دسته بندی شده را برروی ترافیک های جاری بین Host های مدیریت و تجهیزات مدیریت شده (تحت مدیریت) امکانپذیر می سازد .
- Layer2 switch (با قابلیت پشتیبانی از VLAN)- اطمینان می دهد که داده ها از تجهیزات مدیریت شده فقط بتوانند مستقیما" به IOS firewall بروند .

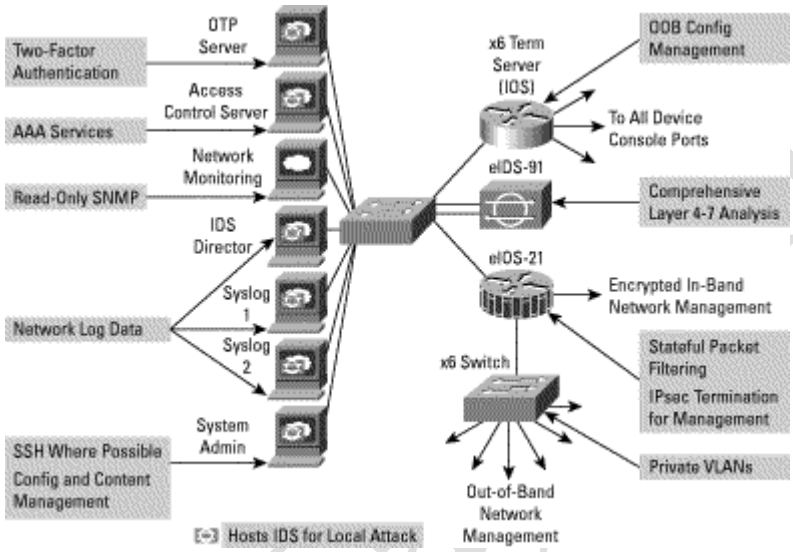


شکل۵- جزئیات ماژول مدیریت

کاهش تهدیدات

- دسترسی های غیر مجاز– IOS firewall وfiltering از بسیاری از ترافیک های غیر مجاز در هر دو جهت جلوگیری می کنند .
- حملات Man-in-Midde (**شخص درمیانه**)- عبور اطلاعات مدیریت از یک شبکهٔ خصوصی حملات Man-in-middle را مشکل می سازد .

- شناسایی شبکه **(Network Reconnaissance)** – به دلیل عبور کل ترافیک مدیریت ازاین شبکه و عدم عبور آن از شبکهٔ محصول می توان از شناسایی شبکه جلوگیری به عمل آورد .
- حملات رمز عبور (Password Attacks)- سرور کنترل دسترسی به کلیهٔ تجهیزات اجازه می دهد که از یک تایید اعتبار two factor قوی استفاده نمایند .
- آدرس تقلبی (IP Spoofing) – توسط firewall ترافیک spoof شده را کاهش می دهد .
- بهره برداری ازاعتماد (Trust exploitation- VLAN های خصوصی از تغییر قیافهٔ یک وسیلهٔ Hack شده به عنوان یک Host مدیریت جلوگیری می کنند .



شکل ٦- قوانین کاهش حملات برای ماژول مدیریت

نکات راهنمای طراحی

همانگونه که در شکل بالا دیده می شود شبکهٔ مدیریت سازمانی SAFE enterprise دارای در بخش می باشد که توسط یک IOS روتر از یکدیگر جدا شده اند که این روتر به عنوان Firewall و یک پایان دهندهٔVPN عمل می کند . بخش بیرون Firewall به کلیهٔ تجهیزاتی که نیازمند مدیریت هستند متصل می شود بخش داخل Host Firewall های مدیریت و IOS روتر را که به عنوان ترمینال سرور عمل می کند شامل می شود . واسطه های باقی مانده به شبکهٔ محصول متصل می شود اما Ipsec – ترافیک مدیریت cisco که از نظر فیزیکی به طور طبیعی واسط های لازم را برا پیشتیبانی از اتصالات مدیریت دارا نیستند به کار می رود IOS Firewall جهت ورود اطلاعات لازم syslog به داخل بخش مدیریت پیکربندی شده است . این اطلاعات شامل Telnet .. SSH SNMP و ..... می باشد . (ورود آنها به شبکه در صورتی که قبلا" در داخل شبکه راه اندازی شده باشند) هر دو زیر شبکهٔ مدیریت بر روی یک فضای آدرسدهی کار می کنند که این فضا کاملا" از بقیهٔ شبکه جدا می باشد .

این اطمینان می دهد دیگران نمی توانند از هیچ پروتکل مسیر یابی ای جهت شناسایی شبکه استفاده نمایند همچنین تجهیزات شبکهٔ تولیدی را قادر می سازد که هر ترافیکی را که از زیر شبکه های مدیریت بر روی لیلک های شبکه تولیدی ظاهر می شود بلوکه کند .

ماژول مدیریت مدیریت پیکر بندی را تقریبا برای تمامی تجهیزات موجود در شبکه از طریق دو تکنولوژی پایه فراهم می کند روترهای Cisco IOS به عنوان ترمینال سرور و بخش شبکهٔ مدیریت اختصاصی عمل می کند روترها وظیفهٔ Telnet معکوس بر روی پورت کنسول موجود بر روی تجهیزات Cisco را از طریق Enterprise تامین می کنند اکثر خصوصیات مدیریت گسترده (تغییرات نرم افزار به روز رسانی جمع آوری و آلارم و مدیریت SNMP از طریق بخش شبکهٔ مدیریت اختصاصی تامین میگردد تعداد کمی از تجهیزات Host های غیر قابل مدیریت از طریق تونل های Ipsec تولید شده توسط روتر مدیریت مدیریت می شوند به دلیل اینکه مدیریت به تقریبا هر ناحیه ای از شبکه دسترسی اجرایی (Administrator) دارد هدفی جذاب برای Hacker ها بشمار می رود ماژول مدیریت با تکنولوژی های مختلفی که برای کاهش تهدید ها طراحی شده اند ساخته شده است اولین تهدید جدی Hacker است که برای دسترسی به شبکهٔ مدیریت خودش تلاش می کنداین تهدید را فقط می توان از طریق آرایش موثر ویژگی های امنیتی درماژولهای باقیمانده د رEnterprise کاهش داد برای کاهش تهدید یک وسیلهٔ مورد مصالحه قرار گرفته (Hack) شده برای جلوگیری از بهره برداری از کانال مدیریت کنترل دسترسی در Firewall و هر دستگاه ممکن دیگر پیاده سازی می شود .یک وسیله مصالحه (Hack) شده نمی تواند هیچ اطلاعاتی را بر روی یک زیر شبکهٔ مشترک با دیگر Host ها ردو بدل نماید زیرا VLANهای خصوصی موجود بر روی سوئیچ های بخش مدیریت تمامی ترافیک را مجبور می کند که از تجهیزات تحت مدیریت مستقیما به Firewall بروند که در آنجا نیز عملFiltering صورت می گیرد .به دلیل استفاده از رمز عبور یکبار مصرف (one-time) در محیط Sniffing رمز عبور فقط اطلاعات غیر قابل استفاده را آشکار می سازد همچنین IDSهای مبتنی بر Host و شبکه بر روی زیر شبکهٔ مدیریت حالتی بسبار محدود کننده پیکربندی شده اند زیرا تنوع ترافیک در این شبکه بسیار محدود بوده و هر در خواست صحیح باید با پاسخ فوری مواجه شود .

مدیریت SNMP مجموعه نیاز های مشخص خود را داراست نگهداشتن ترافیک SNMP برروی بخش مدیریت اجازه می دهد که هنگام دریافت اطلاعات را از دستگاه ها می خواند تا اینکه به آنها اجازه دهد که تغییراتی را اعمال نمایند برای اطمینان از این امر هر وسیله فقط به صورت " فقط خواندنی " پیکر بندی شده است .

جمع آوری و تجزیه و تحلیل مناسب اطلاعات Syslog برای مدیریت شبکه جنبهٔ حیاتی دارد از دیدگاه امنیتی Syslog اطلاعات مهمی را در ارتباط با تجاوزات امنیتی و تغیرات پیکربندی فراهم می آورد بسته به نوع تجهیزات بکار رفته در مسئله ممکن است که سطوح مختلفی از اطلاعات Syslog مورد نیاز باشد داشتن یک ثبت وقایع کامل با تمامی پیام های ارسالی می تواند اطلاعات بسیار زیادی را جهت مرتب سازی توسط یک فرد و یا یک الگو و سیستم تجزیه و تحلیل Syslog فراهم نماید ثبت کردن وقایع صرفا" جهت ثبت آنها نمی تواند جهت بالابردن امینت سودمند باشد اگر اطلاعات ثبت شده مورد تجزیه و تخلیل قرار نگیرد و نتایج حاصل از آنها در سیستم اعمال نشود این ثبت وقایع کاملا بی ارزش خواهد بود .

****

برای تائید اعتبار SAFE کلیهٔ پیکربندی ها با استفاده ا زبرنامه های مدیریت مستقل و Command line (CLI) Interface در آزمایشگاه پیاده سازی شده اند به هر حال هیچ چیز در SAFE مانع بکارگیری سیستم های مدیریت سیاست جهت پیکربندی تجهیزات نمی شود بر پا کردن این ماژول مدیریت آرایش چنین تکنولوژی را کاملا" بادوام و ماندنی می سازد . CLI و برنامه های مدیریت مستقل بدین دلیل مورد استفاده قرارگرفته اند که اکثریت تجهیزات در آرایش های شبکهٔ جاری برای پیکربندی از این روشها استفاده می نمایند .

انتخابها(Alter natires)

مدیریت outof-band همواره به طور کامل امکان پذیر نیست زیرا ممکن است که بعضی از تجهیزات آنرا پشتیبانی ننمایند و یا اینکه ملاحظات جغرافیایی مدیریت in-band را بجا دیکته نماید هنگامی که مدیریت in-band مورد نیاز است تاکید بیشتری جهت اعمال امنیت بر روی انتقال پروتکل های مدیریت مورد نیاز می باشد . این امر می تواند از طریق استفاده ازssl, ssh, ip-ses و یا هر انتقال مجوزدهی و رمز نگاری شدهٔ دیگری که قابلیت انتقال مدیریت را فراهم آورد انجام شود هنگامی که مدیریت بر روی واسطه های مشابه وسیله ای که جهت داده های کاربر بکارمی رود اعمال می گردد بسیار با اهمیت است که ارتباط بر روی رمز عبور رشته های عمومی کلید های رمز نگاری و لیست های دسترسی که ارتباط به سرویس های مدیریت را کنترل می تماید قرار گیرد .

اهداف معماری در آینده نزدیک

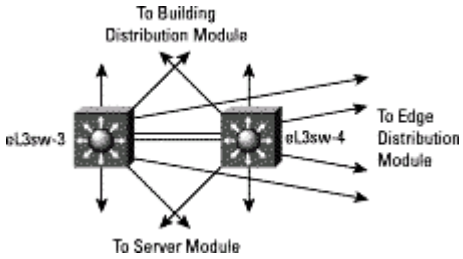
اجرای گزارش گیری و اخطار دهی جاری بین چندین Host تقسیم شده است در بعضی از جاها از Host های هوشمند جهت تجزیه و تحلیل اطلاعات firewall ها و IDS ها استفاده شده است درحالی که بقیهٔ Host های عادی جهت تجزیه و تحلیل اطلاعات روترها سوئیچ ها مناسب تر هستند در آینده کلیهٔ اطلاعات بر روی یک مجموعه مشابه از Host های اضافی (Redundant) مجتمع خواهندشد تا همبستگی رویدادها را بین تمامی تجهیزات به توان بدست آورد .

ماژول هسته (core Module)

ماژول هستند درمعماری SAFE تقریبا همان معماری ماژول هستند درسایر شبکه ها می باشد این بخش صرفا" وظیفهٔ سوئیچینگ و مسر یابی ترافیک را به آخرین سرعت ممکن از یک شبکه به شبکه های دیگر بر عهده دارد .

تجهیزات کلیدی

- سوئیچ های لایهٔ ۳- اطلاعات شبکهٔ تولیدی را از یک ماژول دیگر مسیر یابی و سوئیچ می کند . شکل



شکل ۷ – جزئیات ماژول هسته ای

کاهش تهدیدات

- Packet sniffer ها یک زیر ساخت سوئیچ شده تاثیر sniffer ها را کاهش می دهد

نکات راهنمای طراحی

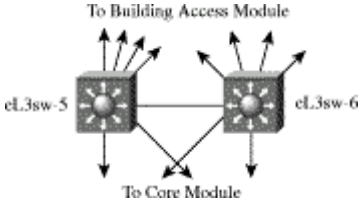
رهنمودهای پیاده سازی استاندارد بر اساس آرایش معمول لایه های هستند توزیع و دسترسی دنبال شده است که در شبکه های مبتنی بر تجهیزات cisco که از طراحی خوبی برخور دارند مشاهده می شوند به هر حال در معماری SAFE برای هسته شبکه های سازمانی (Enterprise) نیازهای خاص در نظر گرفته نشده است برای اطمینان از اینکه سوئیچ های core در برابرحملات مستقیم بخوبی محافظت شده اند آنها را اصول امنیت سوئیچ ها در بخش " سوئیچ ها اهداف هستند " پیروی می کنند .

ساختمان ماژول توزیع (Building distribution Module)

هدف ماژول فراهم نمودن سرویس های لایهٔ توزیع برای سوئیچ های ساختمان می باشد این سرویس ها شامل مسیر یابی کیفیت خدمات (QOS) و کنترل دسترسی می باشد در خواست جهت بر قراری جریان داده به این سوئیچ ها و از آنها به هسته و برقراری جریان پاسخ در عکس همان مسیر ا زوظایف این بخش است

ابزارهای کلیدی

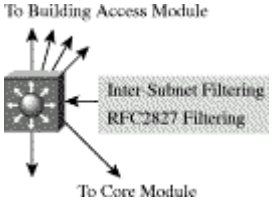
سوئیچ های لایهٔ ۳- وظیفهٔ متمرکز کردن سوئیچ های لایهٔ ۲ در ماژول ساختمان و ارائه خدمات پیشرفته را بر عهده دارند .شکل



شکل ۸ – جزئیات ساختمان ماژول توزیع

کاهش تهدیدات

- دسترسی های غیر مجاز حمله به منابع ماژول سرور با انجام layer3 filtering درزیر شبکه های خاص کاهش می یابد
- RFC2827 filtering – tp spoofing اکثر تلاش های spoofing را متوقف می سازد .
- Packer sniffers – یک زیر ساخت سوئیچ شده تاثیر sniffer ها را کاهش می دهد .



شکل ۹ - قوانین کاهش حملات برای ساختمان ماژول توزیع

نکات راهنمای طراحی

علاوه برمبنای استاندارد طراحی شبکه بهینه سازی هایی که در بخش " سوئیچ ها اهداف هستند مورد بحث قرارگرفت جهت افزایش امنیت کاربران شبکه پیاده سازی شده است تشخیص ورود غیر مجاز در ساختمان ماژول توزیع پیاده سازی نشده است زیرا این سیستم فقط بعضی از در ماژولها پیاده سازی شده است این ماژولها دارای منابعی هستند که بدلیل محتوایشان اهداف جذابی برای حمله می باشند (مثل سرورها دسترسی از راه دور اینترنت وعیره)

ساختمان ماژول توزیع اولین خط دفاعی پیشگیری در برابر جملاتی که از داخل آغاز شده اندرا تامین می کند این می تواند با بکاربردن کنترل دسترسی سانس دسترسی یک قسمت را به اطلاعات محرمانه موجود برروی سرورهای بخش های دیگر کاهش دهد به عنوان مثال یک شبکه که شامل بخش های بازاریابی و تحقیق و توسعه می باشد می تواند سروز بخش R8D را توسط یک VLAN ویژه از سایر بخش ها جدا نماید و با انجام عمل filtering برروی آن اطمینان دهد که فقط کارمندان بخش R8D به این سرور دسترسی دارند .

به جهت کارآیی این مسئله اهمیت می باشد که این کنترل دسترسی را در یک paltform سخت افزاری پیاده سازی نماییم تا بتواند ترافیک فیلتر شده را با نرخ نزدیک به سیم به مقصد برساند ترافیک را با سرعت زیاد نزدیک به سرعت دریافت آنها از روی پردازش و فیلتر کند و به مقصد ارسال دارد این عموما" استفاده از سوئیچ های لایهٔ ۳ را به عنوان رایج ترین تجهیزات اختصاصی مسیریابی بما دیکته می نماید این می تواند مانند کنترل دسترسی با استفاده از RFC 2827 filering از sowrce- addres spoofing جلوگیری به عمل آورد در نهایت جدا سازی زیر

شبکه مسیریابی ترافیک voice- over- IP (70IP) به مدیریت تلفن دروازه ها (Gateway) های مربوط بکارمی رود این از عبور ترافیک 70IP از سایر بخش های مشابه که اطلاعات دیگر در آنجا جریان دارد جلوگیری می کند و با این کار احتمال sniffing ارتباطات صوتی را کاهش می دهد و با استفاده از یک صاف کننده (smooter) کیفیت سرویس (QOS) را پیاده سازی می نماید .

انتخابها

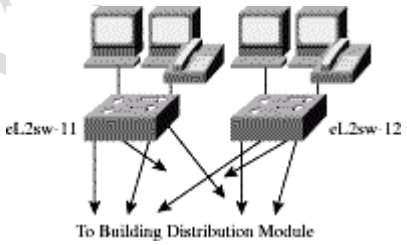
بسته به اندازه کارآیی مورد نیاز شبکه برای کاهش تعداد تجهیزات مورد نیاز در محیط لایهٔ توزیع می تواند با لایهٔ هستند ترکیب شود .

ماژول ساختمان

SAFE ماژول ساختمان را به عنوان گسترده ترین بخش شبکه که ایستگاه های کاری end-user تلفن ها و نقاط دسترسی لایهٔ ۲ مربوط به آنها را شامل می شود تعریف می نماید هدف اصلی آن رایانه خدمات مصرف کنندگان (end-user) می باشد

ابزارهای کلیدی

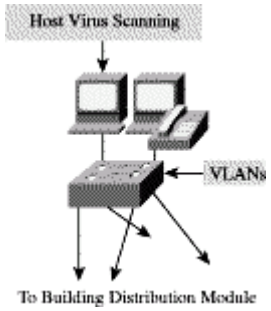
- سویچ لایهٔ ۲ خدمات سوئیچینگ لایهٔ ۲ برای تلفن ها و ایستگاههای کاری کاربران فراهم می آورد .
- ایستگاه های کاری کاربران – خدمات اطلاعاتی را برای کاربران مجازشبکه فراهم می آورد .
- IP phone – سرویس های IP Telephony را برای کاربران بر روی شبکه فراهم می آورد .



شکل ۱۰ – جزئیات ساختار مازول دسترسی

کاهش تهدیدات

- Packet sniffer ها- یک زیر ساخت سوئیچ شده و سرویس های VLAN پیش فرض تاثیر sniffer ها را کاهش می دهد .
- برنامه های ویروس و اسب تروا (trujan horse) استفاده از نرم افزارهای ویروس یاب بر روی Host ها می تواند از اکثر ویروسها و بسیاری از اسب های تروا جلوگیری نماید .



شکل ۱۱ -- قوانین کاهش حملات برای ساختمان ماژول دسترسی

نکات راهنمای طراحی

بدلیل اینکه تجهیزات کاربران عموما" بزرگترین بخش عناص رمنفرد شبکه را تشکلیل می دهند پیاده سازی امنیت به روش ساده و موثر کارساده ای نیست .

ازیک پرسپکتو امنیت ماژول توزیع ساختمانی مانند هر چیزی در ماژول ساختمان اکثر کنترل های دسترسی ای را که مجبور هستیم در سطح مصرف کنندهٔ نهایی داشته باشیم را فراهم می نماید . دراینجا بدین دلیل از سوئیچ های لایهٔ ۲ استفاده شده است زیرا ایستگاه های کاری و تلفن های متصل به آن از هیچ قابلیت کنترل دسترسی لایهٔ ۳ بر خوردار نیستند علاوه بر رهنمودهای امنیت شبکه که در بخش امنیت سوئیچ ها ارائه شده است از نرم افزارهای ضد ویروس نیز در Host های و در سطح ایستگاه های کاری استفاده شده است .

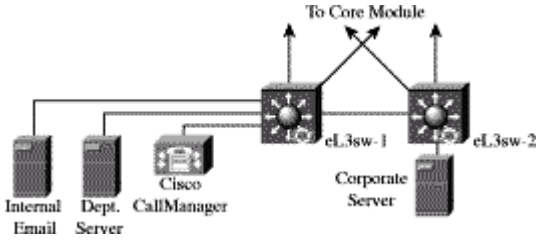
ماژول سرور

هدف اصلی ماژول سرور ارائه خدمات برنامه های کاربردی به تجهیزات و کاربران نهایی می باشد جریان ترافیک موجود در ماژول سرور توسط یک آشکار ساز ورود غیر مجاز on-board در سوئیچ های لایهٔ ۳ بازرسی می شود .

ابزارهای کلیدی

- سوئیچ لایهٔ ۳- خدمات لایه ۳ راجهت سرور ها تامین نموده و اطلاعاتی را که از ماژول سرور عبور می کند سرور عبور می کند توسط NIDS بازرسی می نماید .
- مدیریت تلفن (Call Mamager) وظایف مسیر یابی تماس های تلفنی را برای تجهیزات IP tele phony در سازمان Centerprise بر عهده دارد .
- سرورهای بخش ها و شرکت – سرویس های DNS- print- file را به ایستگاه های کاری موجود در ماژول ساختمان ارائه می دهند .

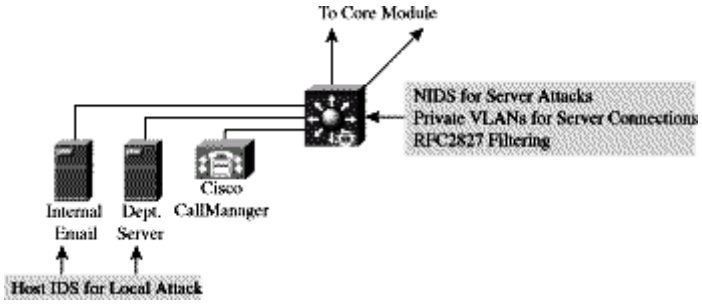
- سرویس دهندهٔ پست الکترونیکی – خدمات SMTP -pop3 را برای کاربران داخلی تامین می نماید .شکل



شکل۱۲ – جزئیات ماژول سرور

کاهش تهدید ات

- دسترسی های غیر مجاز – از طریق بکاربردن آشکار سازهای ورود غیر مجاز بر روی Host ها همچنین کنترل دسترسی تهدید دسترسی های غیر مجاز کاهش یافته است .
- حملات لایهٔ کاربرد به روز رسانی سیستم عامل ها تجهیزات و برنامه های کاربردی توسط جدین ترین fix ها و Patch های امنیتی و محاظت توسط IDS مبتنی بر Host .
- IP spoofing- RFC 2827 filtering از جعل آدرس مبدا جلوگیری می نماید .
- بهره برداری از اعتماد – چیدمان اعتمادی بسیلر صریح می باشد VLAN های خصوصی از ارتباط بین Host های بر روی یک شبکه جلوگیری بعمل می آورد مگر در مواقع لزوم .
- تغییر جهت پورت (port- Redirection) – IDS های مبتنی بر Host از نصب شدن عوامل (نرم افزار های) تغییر دهندهٔ مسیر پورت جلوگیری بعمل می آورند .شکل



شکل ۱۳ – قوانین :کاهش حملات برای ماژول سرور

نکات راهنمای طراحی

ماژول سرور اغلب از دیدگاه امنیتی مورد بررسی قرار می گیرید زمانی که سطوح دسترسی توسط کاربرانی که به سرورهایشان متصل هستند امتحان می شود سرورها می توانند هدف اصلی حملاتی قرار گیرد که از داخل شروع شده است . اعتماد ساده به رمزهای عبور موثر یک استراتژی جامع تخفیف حملات را تامین نمی نماید بکارگیری IDS های مبتنی بر Host و شبکه VLAN های خصوصی کنترل دسترسی و تمرین های خوب system administration (مانند به روز نگهداشتن سیستم ها با آن آخرین patch ها) پاسخ بسیار جامعتری را فراهم می نماید .

به دلیل اینکه NIDS فقط می تواند حجم محدودی از ترافیک را تجزیه و تحلیل کند این نکته حائز اهمیت است که فقط ترافیک های حساس به جمله را برای آن ارسال نماییم ای از شبکه به شبکهٔ دیگر تغییر می کند اما احتمالا" باشد شامل www . FIP . telnet . Smtp باشد . دلیل انتخاب NDIS های مبتنی ب سوئیچ این است که آنها می توانند کلیهٔ ترافیک هایی را که از همهٔ VLAN های می گذارد برسی کنند . نوع ای ترافیک ها از نظر اهمیت توسط سیاست امنیتی تعریف می شود .

هنگامی که IDS به طور صحیح تنظیم شد می توان آنها را به طور محدود نصب نمود . زیرا آنها نیاز دارند که ترافیک جاری را بخوبی شناسایی نمایند .

انتخابها

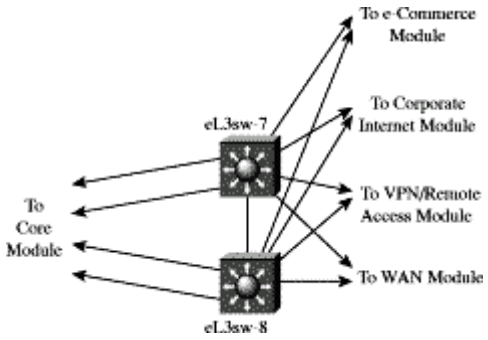
ماژول سرور مانند ماژول توزیع ساختمانی در صورتی که محدودیت ها و نیازهای کار آرایی ما را مجبور به جدا سازی نکند در محیط های حساس که از سرور هایی با کارآیی بالا استفاده می کنند می توان قابلیت NIDS موجود در سوئیچ های لایهٔ ۳ را توسط نصب بیش از یک تیغهٔ NIDS و هدایت هر نوع ترافیک به تیغه ای خاص مطابق سیاست امنیتی گسترش داد .

ماژول گسترده حاشیه ای

مقصود این ماژول بهم پیوستن و اتصالات اجزاءمختلف حاشیه ای است .

ابزار کلیدی

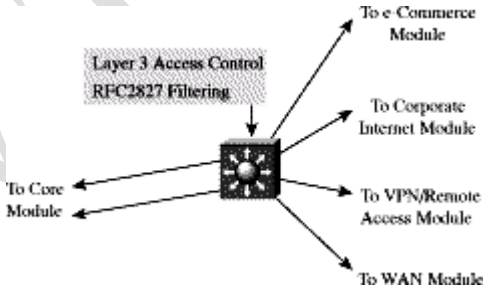
سوئیچهای لایه -۳ اتصال حاشیه ای را متراکم می کنند و سرویسهای پیشرفته ای را مهیا می سازند .



شکل ١٤- جزئیات ماژولهای گسترده حاشیه ای

کاهش تهدیدات

- تصفیه دسترسی غیر مجاز – کنترل تک تک را بر روی زیر شبکه های حاشیه ای و توانایی آنها برای رسیدن به محدوده درونی خود را نیاز دارند .
- IPSPoofing (آدرس تقلبی) – RFC – 2827 که شروع حملات تقلبی را بطور محلی محدود می کند .
- NetworkReconnaissance – ترافیک غیر واقعی را تسویه می شود و توانایی Hackerها را در شناسایی شبکه محدود می کند .
- Pocket Sniffer – یک گزینش زیرساختاری تاثیر shiffing را محدود می کند .



شکل ١٥- قوانین کاهش حملات به ماژولهای گسترده حاشیه ای

نکات راهنمای طراحی

ماژولهای گسترده حاشیه ای از بعضی جهات شبیه مدل گسترده ساختمانی است به اصطلاح کاربرد ویژه (overal Functio) هر دو مدل (ماژول) کنترل دستری به فیلتر (صافی) ترافیک رابکار می برند و هرچند که ماژول گسترده حاشیه ای تا اندازه ای اطمینان دارد به تمامی نواحی و ابتدا حاشیه ای تا توابع امنیتی بیشتری را مهیا کند .

هر دو مول سوئیچهای لایه ۳ را بکار میبرند تا به بازده بالاتری دست یابند اما ماژولهای گسترده حاشیه ای می توانند امکانات امنیتی بیشتری را مهیا کند بخاطر اینکه ملزومات بازده و راندمان خیلی زیاد نیست .

ماژول کننده حاشیه ای آخرین خط دفاعی پیش بینی شده است برای همه ترافیکها تخصیص داده می شود بخاطر ماژولهای دانشگاهی از این شامل تخفیف ارسال بسته های قبلی (spoofcalpaeled) و بروز درآوردن مسیرهای غلظ و تدارک کنترل دسترسی به لایه شبکه میباشد .

انتخابها

همانند سرودها و ماژولهای گسترده ساختمانی ماژولهای گسترده حاشیه ای میتوانند ترکیب بشوند با مدل هسته ای اگر نیازمندیهای راندمان کاری آنها همانند دقت مراجع پیاده سازی safe باشد .

NIDS(Netwolk Intrusion Detection Systems)

سیستمهای کشف نفوذ متکی بر شبکه در این ماژول حضور ندارند اما می توانند در اینجا قرار گیرند بواسطه کارتهای سیستمهای کشف نفوذ خطی که در سوئیچهای لایه ۳ بکار میروند .

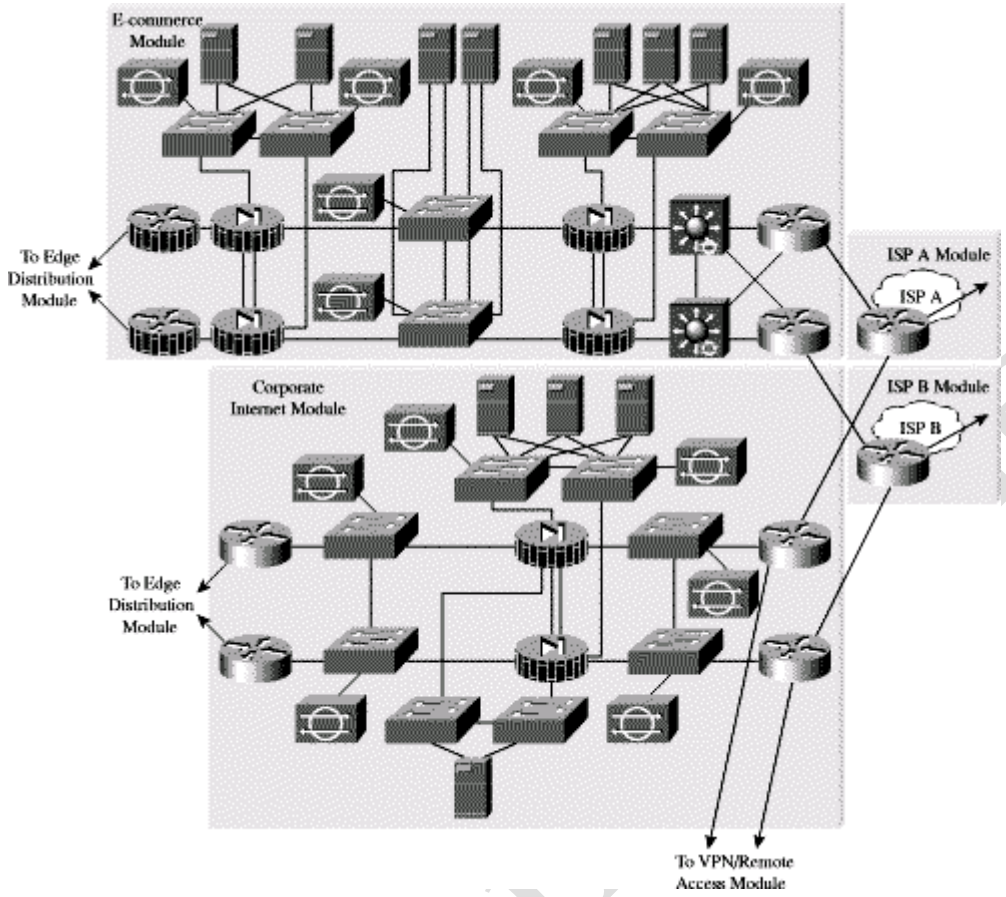
که باعث کاهش نیاز به بکارگیری NIDS در قسمت بحرانی ماژولهای حاشیه ای که به محیط دانشگاه متصل هستند میشود .

هر چند که دلایل بکارگیری ممکن است دیکته شده باشد و همچنانکه آنها در مراجع طراحی safe انجام داده اند یعنی دیکته کردن قرار دادن کشف و شناسایی نفوذ در ماژولهای مختلف حاشیه ای برخلاف ماژول گسترده

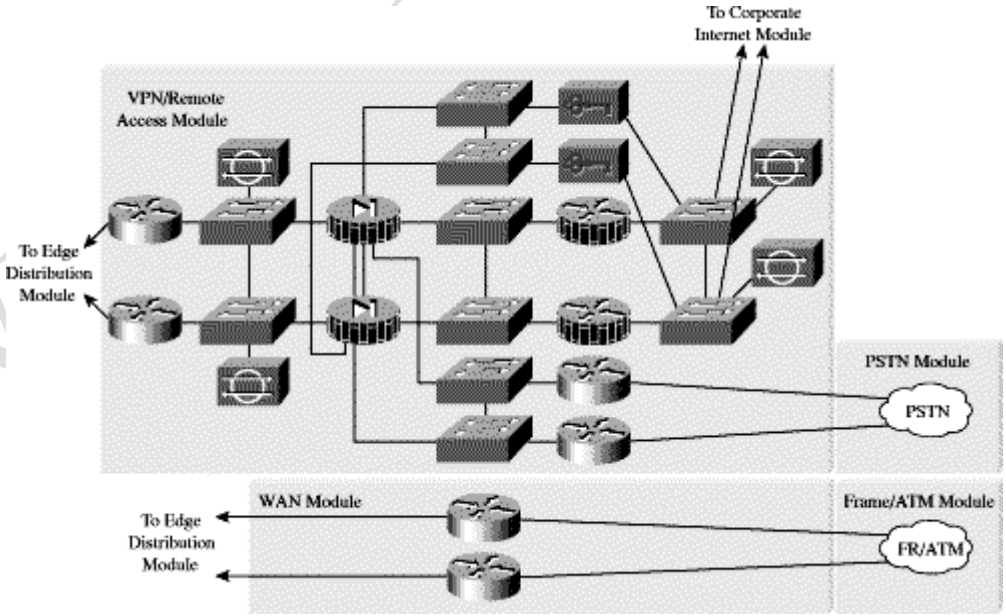
حاشیه ای است .

Enterprise edge

شرح ذیل تفصیل جزئیات تجزیه و تحلیل همه ماژولها را که در داخل حاشیه خارق العاده هستند شامل میشود .



شکل ١٦- جزئیات حاشیه خارق العاده- قسمت ١



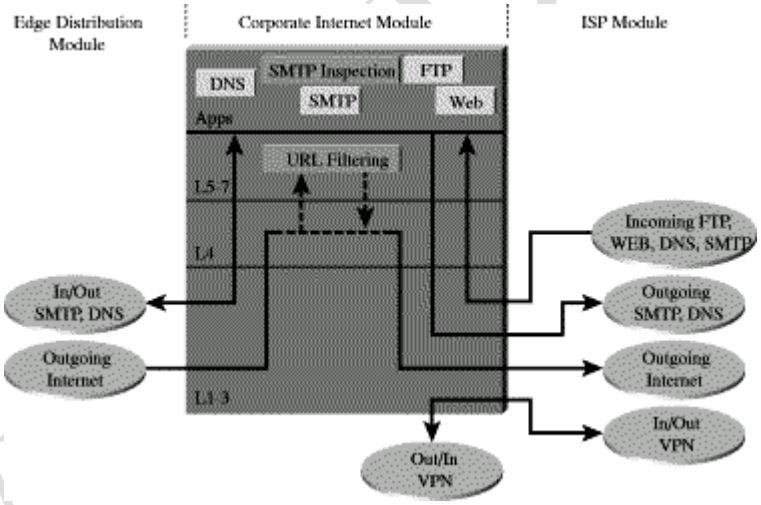
شکل ۱۷- جزئیات حاشیه خارق العاده- قسمت ۲

ماژولهای متحد اینترنتی

ماژولهای مقصد اینترنتی ارتباط کاربران داخلی را به سرویسهای اینترنیتی فراهم می کند تا کاربران اینترنت به اطلاعات سرویس دهنده های عمومی دسترسی پیدا کنند .

همچنین ترافیک از این ماژول به طرف (wirtud private Network) شبکه های خصوصی مجازی و ماژولهای دسترسی از راه دور جریان پیدا میکند . جایی که پایانه های شبکه های خصوصی مجازی دارند .

این ماژول برای سرویسهایی مانند تجارت الکترونیک و برنامه های کاربردی طراحی نشده اند . بعدا با بخش ماژولهای تجارت الکترونیک که درا ین مقاله مراجعه کنید تا جزئیات بیشتری در رابطه با فراهم کردن تجارت اینترنیتی بدست آورید .

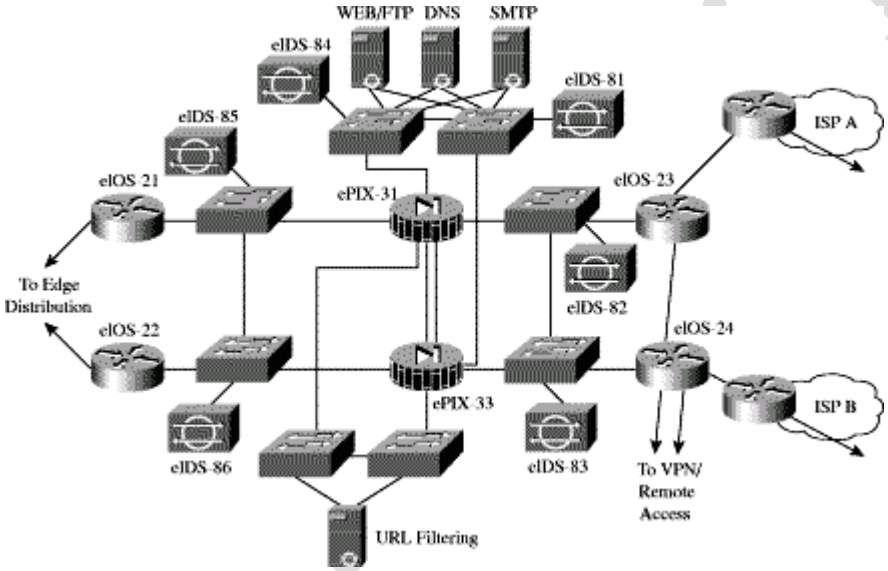


شکل ۱۸- جریان ترافیکی اینترنت های متحد

ابزارهای کلیدی

- سرویس دهنده (SMTP server) SMTP – مانند یک (تقویت کننده) بین سرویس دهنده های اینترنیتی و نامه های اینترنیتی عمل می کند . محتوا را بازدید کنید .

- سرویس دهنده (Domain Name server) – سرویس می دهد مانند اجازه نامه بۀک سرویس دهنده DNS خارجی (اجازه می دهد) برای مبادرت کردن به تقویت درخواستهای داخلی به اینترنت .
- سرویس دهنده (FTP, HTP) – اطلاعات عمومی را درباره سازمانها فراهم می کند .
- دیواره آتش (firewall) – سطوح محافظتی منابع شبکه و حالتهای سودمند تصفیه کردن ترافیک (تردد شبکه) را فراهم می کند .
- ابزارهای NIDS – این ماژول در لایه ها کنترل بخشهای کلیدی لایه شبکه را فراهم می کند .
- سرویس دهنده صافی URL با شجاعت درخواستهای غیرمجاز URL را تصفیه می کند .

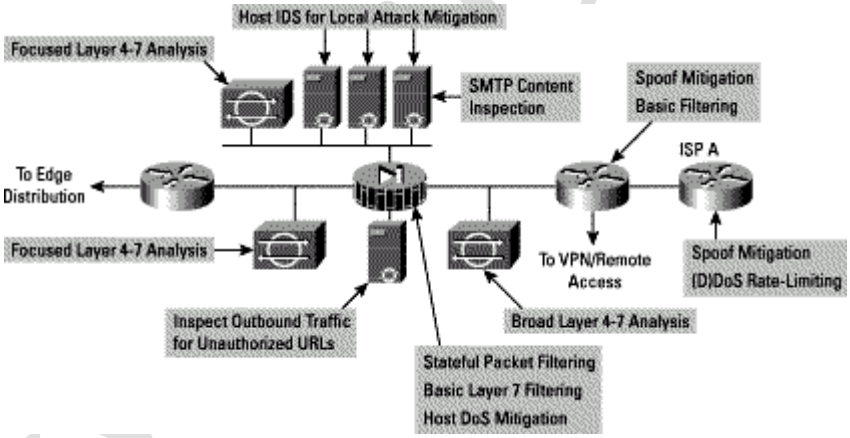


شکل ۱۹- جزئیات ماژولهای اینترنتی متحد

کاهش تهدیدات

- unauthorizedAccess (استرمی غیرمجاز) کاهش دادن بوسیله صافی کردن در ISP و در مسیریابهای حاشیه ای دیواره های آتش مقصد
- حملات لایه برنامه های کاربردی . بواسط وجود IDS در میزبان و لایه های شبکه می تواند کاهش پیدا کند .
- Virus and Trojawhous (ویروس و T .H) بواسطه تصفیه مندرجات نامه های الکترونیکی و سیستمهای کشف نفوذپروری میزبان

- حملات برای پیدا کردن pasword سرویسهای آماده ای که برای استفاده ناشیانه هستند محدود شده IDS, os, میتوانند این تهدیدات را شناسایی کنند .
- Denial Of Service(عدم پذیرش سرویس) – CHR در ISP حاشیه ای و تنظیم کردن کنترلهای ICP در ایراد آتش .
- IP spoofing (IPهای تقلبی) – (Requet for comment) – 1418, 2827 RFC . در ISPهای حاشیه ای ومسیریابهای حاشیه ای صافی می کند .
- Packet sniffer – شناسایی شبکه (جاسوسی شبکه) IDS جاسوس راشناسایی میکند و پرتکلها باری محدود کردن تاثیر آنها را تصفیه می کنند .
- Trust Exploitation (قلب اعتماد) – محدود کردن مدلهای معتمد و شبکه های مجازی خصوصی حملات برپایه اعتماد را محدود می کنند .
- Port Redirection(مسیریابی پورت) – جلوگیری و تصفیه کردن و IDS میان حملات را محدود می کنند .



شکل ۲۰- قوانین کاهش حملات برای ماژولهای اینترنتی متحد

نکات راهنمای طراحی

قلب این ماژول یک جفت دیواره آتش مدول کننده است که حفاظت رامهیا می کند برای سرویسهای عمومی اینترنت و کاربران داخلی کیفیت بهتر بازرسی رسیدگی کردن به ترافیک و تردد در همه جهات حفاظت میکند که تنها ترافیک مجاز از دیواره آتش عبور کند .

تمام ملاحظات طراحی دیگر متمرکزی می شود مدل امنیت وکاهش حمله

شروع در مسیر یاب حاشیه ای مستدی در این ISP سرعت خروجی از ISP تردد غیر ضروری را محدود می کند همچنین در خروجی مسیریاب ISP ,RFC1418 ,RFC2827 باعث تصفیه و کاهش علامت به آدرسهای منابع در مدخل ورودی اولین مسیریاب در شبکه های تهورآمیز یا مهم میباشد .

تصفیه سازی اصلی تردد را محدود میکند به آن ترددی که توقع داریم و تهیه کردن یک صافی غلیظ برای اکثر حملات پایه ای RFC 1418 ,2827 نیز اینجا ضروری بنظر میرسند که مانند فیلتر تصدیقی برای فیلترهای ISP هستند به علاوه بدلیل امنیت مفرط تهدیداتی که آنها بوجود می آورند و مسیریابها اینگونه تنظیم شده اند که آثار بسته هایی را که عموما در نمونه های ترافیکی استاندارد بر روی اینترنت دیده شوند را حذف میکنند . هر ترافیک مشروعی کم میشود بخاطر اینکه این تصفیه سازی قابل قبول بنظر میرسد وقتی که قابل مقایسه با تصدیق اینچنین ترافیکهای همراه باشد .

سرانجام ترافیک تردد IPSEC برای VPN در نظر گرفته میشود وماژولهای دیستری از راه دو بجوار مناسب مسیریابی میشوند . صافی کردن در واسطه های متصل به ماژولهای VPN طوری تنظیم میشود تا تنها ترددهای SPEC عبور کنند و تنها از وقتی سرچشمه میگیرند و ارسال میشوند که برای شناسایی اعضایشان باشد .

با دسترسی از راه دور VPN شما عموما آدرس IP سیستمی که وارد میشوند را نمیدانید بنابراین تصفیه کردن میتواند تنها مخصوص اعضای ابتدایی و انتهایی باشد که به اعضای دوردست ابلاغ میشود .

اسباب NIDS در بخش عمومی دیواره آتش برای کنترل و نظارت حمله هایی است که بر پایه لایه چهارم به تجزیه لایه هفتم ومقایسه برعلیه علائم شناخته شود .

بدلیل اینکه ISP و مسیریابهای حاشیه ای مهم آدرس و پورت معینی را تصفیه می کنند . این به وسائل NIDS باید یک ابزار آگاه کننده اخطار دهنده به سطح پایین تر از سطح آن وسایل که در داخل دیواره آتش هستند داشته باشد و بخاط راینکه در اینجا خبر دادن بنظر میرسد که نتواند خطر واقعی را مهم کند اما صرفا تلاش می کند .

دیواره آتش یک حالت اتصال اجباری را فراهم میکند جلساتی که در طول دیواره آتش راه اندازی میشود را جزجز تصفیه می کنند .

- سرویس دهنده های قابل آدرس دهی آشکارا سیستم حفاظتی دارند بر ضر جریان ICPSYN که بواسطه بکارگیری محدودیت اتصال غیر باز بر روی دیواره آتش
- از نقطه نظر تصفیه سازی و علاوه بر محدود کردن ترافیک بر روی مقطع سرویس دهنده های عمومی برای روی پورتها و آدرسهای مناسب تصفیه کردن در جهت معکوس هم جایگاه ویژه ای دارد .
- اگر یک حمله با یکی از سرویس دهنده های عمومی مطالعه کند (بوسیله گول زدن دیواره آتش IDS مبنی بر شبکه) آن سرویس دهند قادر نخواهند بود که بیشتر به شبکه حمله کند .

- برای کاهش اینگونه حملات و تصفیه سازی مخصوص از هر درخواست غیرمجازی که توسط سرویس دهنده های عمومی بر علیه هر مکان دیگر تولید میشود جلوگیری می کند .(محافظت میکند .)
- به عنوان مثال و یک سرویس دهنده وب باید صافی شود بنابراین نمیتواند بخودی خود درخواست ایجاد کند اما صرفا به خواستهای پاسخ می دهد .
- این کمک از دریافت اطلاعات امکانات اضافی یک هکر در طول مدت سازش و مصالحه بعد از اینکه حمله تشخیص داده شد جلوگیری می کند .
- همچنین کمک می کند به توقف جلسات ناخواسته که بوسیله هکرها راه اندازی می شوند در طول حمله اولیه
- حمله ای که باعث تولید xterm از سرویس دهنده وب بواسطه دیواره آتش به طرف دستگاه هکر میرود نمونه ای از این حمله است .
- به علاوه شبکه های مجازی خصوصی از حمله کردن سرویس دهنده های عمومی سازشگر به سایر سرویس دهنده هایی که در یک بخش هستند جلوگیری و محافظت میکند .
- این تردد حتی با دیواره آتش هم قابل شناسایی نیست و که در اینجا است در حضور شبکه های مجازی خصوصی بنظر می رسد .
- ترافیک روی وسعت بحث بازدید محدود شده است به تصفیه کردن درخواستهای URL (Uriform, Resources Localer) از دیواره آتش به طرف ابزار تصفیه URL
- به علاوه درخواستهای صحیح اجازه داده میشود تا از ابزارهای مهم تصفیه سازی URL خارج شده و به سرویس دهنده های پایه جهت بروز درآوردن بانکهای اطلاعاتی وارد شود .
- ابزارهای تصفیه سازی URL ترافیک های غیرمعمول را برای حفاظت از درخواستهای غیر مجاز وب بازرسی می کنند .
- این مستقیما بوسیله دیواره آتش منتقل میشود و تصویب یا رد خواستهای URL خارج شده و به سرویس دهنده های پایه جهت بروز درآوردن بانکهای اطلاعاتی وارد شود .
- ابزارهای تصفیه سازی URL ترافیک های غیرمعمول را برای حفاظت از درخواستهای غیرمجاز وب بازرسی می کنند .
- تصمیم این بر پایه روشهای مدیریتی است که بوسیله کاربرد مهم اطلاعات طبقه بندی شده WWW مهیا شده بوسیله سوم خدمات تهیه میشود .

- بازدید URL بر تصفیه دسترسی استاندارد تقدم دارد بخاطر اینکه آدرسهای IP بارها برای سایتهای غیرمجاز وب تغییر پیدا می کند و چنین صافیهایی میتوانند اثر پیدا کرده و خیلی بزرگ شود .
- IDS های مبتنی بر میزبان بر روی این سرویس دهنده بر ضد حملات موجود محافظت میکند بطریقی که دیواره آتش را گول میزند .
- بخشهای سرویس دهنده های عمومی شامل یک اسباب NIS برای شناسایی حملات بر روی پورتها هستند که دیواره آتش به آنها مجوز داده است .
- شما احتیاج دارید که این MDS را در حالات محافظتی بیشتری نسبت به NIDS بیرونی دیواره آتش تنظیم کنید زیرا علامتهایی که در اینجا جور میشوند از میان دیواره آتش با موفقیت عبور می کند .
- در هر کدام سرویس دهنده ها دارای نرم افزار شناسایی نفوذ بر روی میزبان هستند برای کنترل علیه فعالیتهای مرموز در سطح os و همانند فعالیتهای معمول سرویس دهنده (SMTP, FTP, HTTP) و چیزهای دیگر .
- ضربان DNS باید محدود شود که تنها به فرمانهای مطلوب پاسخ دهند و پاسخهای غیر ضروری را حذف کرده که ممکن است باعث شناسایی شبکه توسط هکرها شود .
- شامل این است که منطقه رد و بدل انتقال از هر جای دیگری جدا کنیم بجز سرویس دهنده های DNS داخلی
- سرویس دهنده SMTP شامل سرویسهای بررسی محتوی نامه است که باعث ویروسها حملات Trojnal که برعلیه شبکه های داخلی تولید میشود راکاهش داده که معمولا بواسطه سیستمهای ستی داخل میشوند .

ابزارهای WIDS در داخل واسط دیواره آتش آخرین تجزیه و تحلیل حملات است .

حملات بسیار کمی باید در این بخش شناسایی شود و بخاطر اینکه تنها به درخواستهای (تازه واحد) حساسیت نشان می دهد .

تنها حملات فریبنده باید در این بخش دیده شود آنها بطور کلی به معنی سیستمی است بر روی بخشهای سرویس دهنده های عمومی که سازش میکنند و هکرها تلاش میکنند که بر این پایه نفوذ کنند . واداشتن به حمله به شبکه های داخلی برای مثال اگر سرویس دهنده SMTP با یک هگر سازش کند ممکن است هکر تلاش کنند که به سرویس دهنده پست داخلی از طریق پورت ICP۲۵ حمله کند که به آن اجازه داده میشود که بین دو میزبان انتقال نامه انجام دهد .

اگر حملات در این بخش دیده شود به این حملات باید حساسیت شدیدتری ابراز شود نسبت به آنهایی که روی بخشهای دیگر هستند بخاطر اینکه شاید آنها اشاره کنند به سازشی که قبلا رخ داده به کارگیری راه اندازی مجرد ICP برای بی نتیجه کردن آنها و برای مثال و حمله SMTP که در بالا ذکر شد باید جدا مورد توجه قرار بگیرد .

انتخابها

طراحی مختلفی اختیاری برای این ماژول وجود دارد برای مثال ابزارهای NIDS ممکن است در جلوی دیواره آتش لازم نباشد که بتسگی به طرز برخورد شما مطلع شدن از حمله باشد .

در واقع جز تصفیه سازی اساسی بر روی مسیریابهای نزدیک (قابل دسترسی) این نوع کنترل و نظارت پیشنهاد نمیشود . با یک تصفیه سازی اسای ومناسب که در این طراحی موجود است و IDS که در بیرون دیواره آنت قرار دارد میتواند اطلاعات مهمی را آشکار سازی که به نوعی توسط دیواره آنتن حذف شده بخاطر اینکه نتیجه اخطار بوجود آمده در این بخش واقعا عظیم اس . اخطار تولید شده در اینجا باید شدت کمتری نسبت به اخطار تولید شده در پشت دیواره آتش داشته باشد .

توجه به علائم ورودی از این بخش به مرکز کنترل و تشخیص باعث میشود که به اخطارهای مجاز و مشروع که از بخشهای دیگر می رسد توجه کافی شود .

روشن است که NIDS در بیرون دیواره آتش مهیا میکند نوع حملات راکه سازمان شما میتواند جذب کند تا بهتر جلوه کند را ارزیابی مینماید . به علاوه ارزیابی تاثیر ISP و تصفیه کردن حاشیه ای مهم میتواند انجام دهد .

راه ممکن دیگر برای طراحی پیشنهاد میشود حذف مسیریاب بین دیواره آتش و ماژولهای گسترده حاشیه ای است هر چند که توابع آن میتوانند مرکب از ماژولهای گسترده حاشیه ای شوند .

توابع مجزا بین ماژولها که خواهد شد بخاطر اینکه سوئیچهای گسترده حاشیه ای لازم خواهد بود که از تمام توپولوژی ماژولهای اینترنیتی متحد آگاه باشد تا مسیریابی درستی را مهیا کند .

به علاوه این توانایی شما را در به صف درآوردن این مدل ماژولار محدود میکند .

اگر یک هسته مهم جاری در لایه و برای مثال مسیریابی مهیا شده در ماژولهای اینترنیتی متحد ضروری خواهد بود .

مقاصد معماری

پیشرفت تکنولوژیهای دیواره آتش ciseo که میتواند مستقیما به دیگر ابزارهای بازرسی محتوا متصل میشود(بطور مثال واریس یابهای براساس شبکه) الان تصفیه سازی URL میتواند کار تصفیه سازی محتوا را

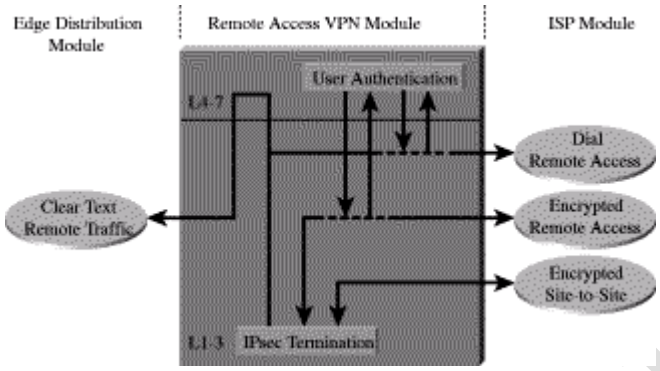
انجام دهد که مستقیما با تکنولوژی دیواره آتش Cisco کامل میشود .

VPN و ماژولهای دسترسی از راه دور

شبکه های خصوصی مجازی از آنجایی که نامش دلالت میکند هدف اولیه این ماژول سه نکته است: پایان دان تردد شبکه های خصوصی مجازی از دست کاربران راه دور

تهیه هاب (HUB) برای پایان دادن به ترافیک سایتهای راه دور – پایان دادن به کاربران که شماره گیری میکنند .

همه ترافیکها حار هستند در گسترده حاشیه ای از کاربران متحد راه دوری که به شکل واقعی و صحیح ترکیب شده اند قبل از اینکه اجازه عبور از دیواره آتش را دارا باشند .



شکل ۲۱ – جریان ترافیکی ماژولهای VPN و دسترسی از راه دور

ابزارهای کلیدی

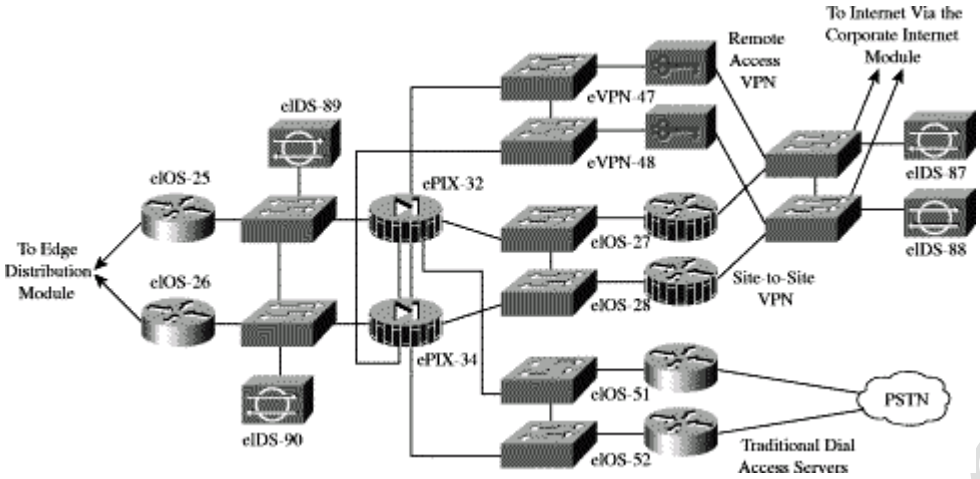
اصلاحیه کننده شبکه های خصوصی مجازی – به کاربران دور و منحصر بفرد اعتبار میدهد تا بطور معتبر گسترش یابند و به مجرای Ispec (امنیت IP) آنها را خاتمه میدهد .

مسیریاب شبکه خصوصی مجازی – سایتهای دور و صحیح و قابل اعتماد میکند و برای ارتباط از تونلهای Crel Ipsec بهره می برد .

سرویس دهنده های شماره گیر – به کاربران و منحصر بفرد اعتبار میدهد تا استافده کننده از TACACST به ارتباطات آنالوگ پایان دهد .

دیواره آتش: برای سه نوع مختلف دسترسی از خارج سطوح محافظتی مختلفی را فراهم میکند .

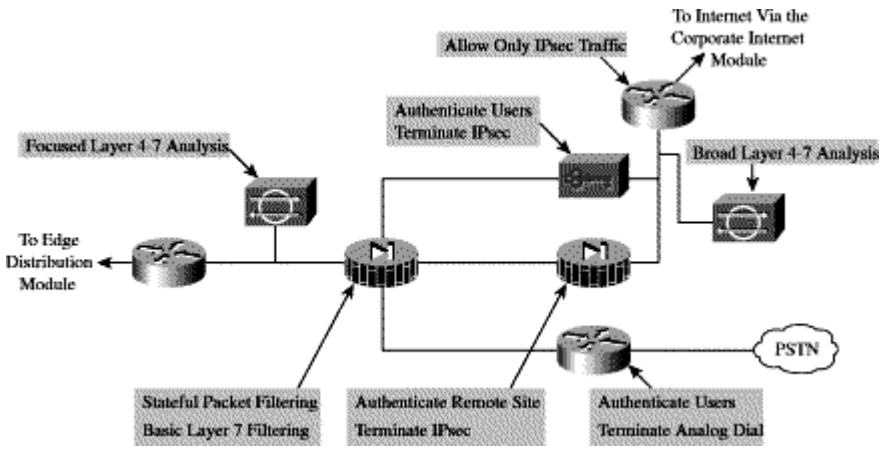
ابزارهای NIDS در لایه ۴ کنترل و نظارت بر بخشهای کلیدی شبکه در لایه ۷ ماژول را فراهم میکنند .



شکل ۲۲ –جزئیات ماژولهای VPN و دسترسی از راه دور

کاهش حملات

- کشف توپولوژی شبکه فقط نقاط کلیدی تبادل اینترنت (IKE) و محفظه امنیتی قابل حمل و نقل (ESD) اجازه دارند که به این بخش از طریق اینترنت وارد شوند .
- حملات به رفر عبور – اعتبار OTP باعث کاهش احتمالی یک حمله موفق رفر عبور میشود .
- دسترسی غیرمجاز – سرویس های دیواره آتش بعد کشف رفر بسته ها از ترافیک پورتهای غیرمجاز جلوگیری میکند .
- Man in the midle بواسطه پنهان کردن ترددهای خارجی کاهش می یابد .
- Packet sniffersیک سوئیچ زیرساختاری تاثیر Shilling راکاهش میدهد .



شکل ۲۳ – قوانین کاهش حملات ماژولهای دسترسی از راه دور ایVPN

نکات راهنمای طراحی

هسته اصلی نیازمندیهای این ماژول این است که سه نوع سرویس اصلی کاربر خارجی و نقاط پایانی انتهایی جدا از هم دارد . بخاطر اینکه ترافیک بوجود آمده از منابع مختلف خارجی به شبکه های اصلی (مهم) و این تصمیم رابوجود آورد کهٔک رابط جدا از هم بر روی دیواره آنتن برای هر یک از سه سرویس مهیا شود . مطالعات طراحی هر یک از این سرویسها در زیر نشان داده شده است .

دسترسی دور به شبکه خصوصی مجازی (VPN)

ترافیک در VPN از مسیریابهای دسترسی ماژولهای اینترنیتی بیشتر بهم فرستاده میشوند که اولین بار در نقاط خروجی تصفیه شدند که بهٔک آدرس IP مخصوص و قراردادهای که جزئی از سرویسهای VPN است .

امروزه برای دسترسی از راه دور به VPN میتوان مجراهای مختلف و پروتکلهای امنیتی مختلف بهره برد .

اگر چه IPSEC یک مجرای قراردادی انتخابی است واما بیشتر سازمانها تونل قراردادی نقطه به نقطه (قرارداد نقطه به نقطه PPTP) و پروتکل مجرای لایه ۲ (L2TP) را انتخاب میکنند . بخاطر اینکه آنها بطور طبیعی سیستم عاملهای مشهور پشتیانی میشوند .

در Safe و Ipsec انتخاب شود وبخاطر اینکه کاربران تنظیمات کمتری نیاز دارد ودر ضمن امنیتی خوبی را هم مهیا میکند .

ترافیک دسترسی از خارج شبکه UPN به سوی یک آدرس عمومی خاصی هدایت میشود که از پروتکل IKE استفاده میکند (UDP50) بخاطر اینکه ارتباط IKE کامل نخواهد شد تا وقتی که اطلاعات موقتی و صحیح تهیه شود .بعنوان قسمتی از (نسخه) وسعت IKE (طرح پیشنهادی KFCS و Xauth یک مکانیزم کاربرد صحیحی اضافی را مهیا میکند قبل از اینکه کاربران خارجی یک پارامتر IP را معین کنند .متمرکز کننده VPN بهٔک سرویس دهنده (سرور) کنترل کننده دسترسی بر روی زیر شبکه کنترل و نظارت متصل است بوسلیه کد رابط کنترل کننده ونظارت .کلمات عبور مطمئنی فراهم میشود بوسیلهٔک سرویس دهنده کلمه عبور .

کاربران خارجی بوسیله دسترسی فراهمی خواهند داشت میشود با دریافت یک پارامتر IP تا و بکار گیر یک نسخه دیگر IKE یعنی maDCFE جدا از یک آدرس IP محل سرویس دهنده های نام (Wils, DUS) و MoDCFC سرویسهای مجازی را برای کنترل دسترسی کاربران خارجی فراهم میکند .بطور مثال در Safe کاربران از شکافتن تونلها منع شده اند در نتیجه

کاربران مجبور میشوند که به اینترنت از طربق اتصالات متشابه دسترسی پیدا کنند .پارامترهای Ipsec که در اینجا استفاده میشوند برای رمزگزاری SHA-HMAC برای تمرکز داده سه برابر هستند . سخت افزاری که ماژولهای رمزگذاری را در UPN متمرکز میکند به سرویس های خارجی دسترسی به UPN اجازه می دهد تا هزاران دنبال کردن نقاط پایانی تونلهای UPNترافیک از میان یک دیواره آتش ارسال میشود تا مطمئن شود که کاربران UPN کاملا تصفیه شده اند .

مدیریت مطمئن و امن این سرویسها بدست می آید با اعمال کردن تمام Ipsec و پارامترهای امنیتی به کاربران خارجی از طریق سایت مرکزی به علاوه و اتصال به تمام توابع کنترلی و نظارتی بر روی یک رابط کنترلی وجود دارد .

کاربرانی که با شماره گیر وارد میشوند .

- کاربران (dial-in) سابق در یکی از دو مسیریاب دسترسی متوقف میشوند بوسیله مودمهای داخلی وقتی که برای اولین بار ارتباط بین کاربران و سرویس دهنده در لایۀک برقرار شد سه روس chap باری کاربران مجاز بکار می رود .

همانند آنچه که در سرویسهای دسترسی VPN خارجی وجود دارد که AAA و سرویسهای کلمه عبور یک مرتبه ای alve) (time PW بکار گرفته می شوند برای مجاز شمردن برقرار کردن کلمات عبور

بوسیله آدرس IP هم میتوان کاربران اجازه عبور داد بوسیله گذراندن IP از میان PPP

شبکه های خصوصی مجازی سایت به سایت

ترافیک UPN با ارتباط یک سایت به سایت پیوسته شده که شامل تونلهای QRF محافظت شده هستند بوسیلۀک پرتکل Ipsec در حالت انتقال که از ESP استفاده می شود . (Encopsulating security poyload)

بنابراین در حالت دسترسی خارجی ترافیکی که بوسیله ماژولهای انتهایی متشابه هدایت میشوند می توانند به مقصد خاصی محدود شوند که مشخص شده دو مسیریاب UPN و آدرس منبعی که از سایت خارجی انتظار داریم .پرتکل ESP (IP50) و پرتکل IKE و تنها دو ارتباطی خواهد بود که توقع داری .

GRE بکار میرود تا یک سرویس کامل مسیریابی را فراهم کند که چند پروتکلی خواهد بود پروتکل مسیریابی و ترافیک چند حالته بخاطر اینکه پروتکلهای مسیریابی (EIGRP) که بین دوسایت دور بکار می رود) میتواند خرابی ارتباط و اتصال را شناسایی کند و تونلهای GRE مکانیزم ارتجاعی را برای سایتهای دور برقرار کند اگر آنها دو مسیریابی جامع را برای ارتباط هر یک از مسریابهای مرکزی VPN بکار برند .

چنانچه دسترسی خارجی VPN و IDES و SHA, HAMC برای IKE و پارامترهای Ipsec بکار میروند تا بالاترین امنیت را با کمترین تاثیر منفی در کارایی مهیا کنند .

سخت افزارهای تسریع کننده Ipsec در مسیریابهای VPN بکار برده میشوند .

نتیجه ماژول

ترافیک بوجود آمده از سه سرویس بوسیله دیواره آتش متراکم میشود بر روی یک رابط خصوصی قبل از اینکه به ماژول گسترده حاشیه ای بوسیلهٔک جفت مسیریاب ارسال شود .

دیواره آتش باید با یک نوع صحیحی از تحمیل کنترل و دسترسی تا متنها به ترددهای مناسب هر یک از سرویسها اجازه داده شود که از طریق رابط داخلی دیواره آتش عبور کنند .

یک جفت از ابزارهای NIDS در طرف عمومی این ماژول قرار میگیرند تا هر نوع فعالیت شناسایی شبکه در شبکه های خصوصی مجازی را به وسیله ابزارهای پایان دهنده تشخیص دهند .

در این بخش نقطه Ipsec (IKE/ ESP) باید دیده شود . بخاطر اینکه سیستم NIDS بعد از دیواره آتش قرار دارد تا هر حمله ای را مرکز باقیمانده ماژول بوجود می آید شناسایی کند . این ابزارهای WIDS همچنین سیاست محدود کنندگی در مکان را دارند .

تمام کاربرانی که از این بخش عبور میکنند باید محدود شوند بهٔا آنهایی که از مکانهای دور و خارج وارد میشوند بنابراین هرگونه پرهیزی یا راه اندازیه دوباره ICP تنها بر این کاربران تاثیر میگذارد .

انتخابها

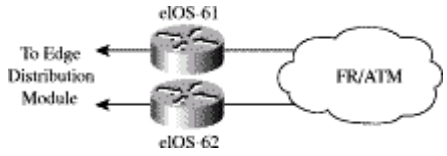
در شبکه های خصوصی مجازی و تکنولوژی هستند و اینها انتقالهای زیادی هستند که بسته به نیازهای شبکه آماده هستند .

این انتخابها در زیر بطور مرجع لیست شونده و اما جزئیات در این مقاله مشخص نمی شوند .

- کارت هوشمند مستند مربوط به سیستم متریک
- L2TP و یا PPTP و تونلهای دسترسی شبکه خصوصی مجازی از راه
- گواهینامه معتبر
- IKE مکانیزم ارتجاعی را معتبر نگه میدارد .
- پروتکلهای چندگانه سوئیچینگ در شبکه های خصوصی مجازی

ماژول شبکه گسترده

ترجیحا اگر همه آنها شامل طراحی نهایی WAN باشند واین ماژول حالت ارتجاعی و امنیتی نقاط پایانی شبکه های گسترده را نشان می دهد . بکارگیری و بخش نهایی کپسوله شده ترافیک بین سایتهای دور و سایتهای مرکزی هدایت میشود .



شکل ۲٤ – جزئیات ماژولهای WAN

ابزارهای کلیدی

- مسیریابهای IOS – مسیریابی , کنترل دسترسی و مکانیزمهای QOS را بکار می برند .

کاهش تهدیدات

- IP SPOOFING – با تصفیه سازی در طی لایه ۳ کاهش می یابد .
- Unauthorized Access (دسترسی غیر مجاز) – کنترل ساده دسترسی بر روی مسیریاب می تواند انواع پروتکلها را محدود که به کدام شاخه می توانند دسترسی پیدا کنند .

شکل ۲۵ – قوانین کاهش حملات برای ماژول شبکه گسترده

نکات راهنمای طراحی

حالت ارتجاعی مهیا میشود بوسیلهٔک ارتباط دوطرفه از فراهم کننده سرویسها بوسیله مسیریاب و ماژولهای گسترده حاشیه این امنتیت مهیا میشود بوسیله بکارگیری ترکیبات امنیتی 105- لیست دسترسی ورودی برای متوقف کردن ناخواسته از شاخه های دور بکار میرود .

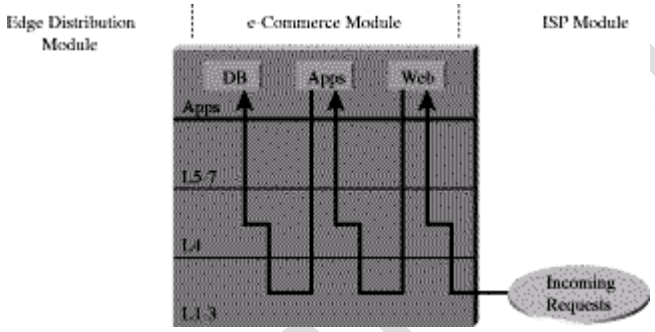
اختیارات

بعضی سازمانها که درباره اطلاعات خصوصی شان خیلی نگران هستند ترافیک بسیار محرمانه را از نقاط ارتباطی با شبکه های گسترده بطور متشابه در شبکه های خصوصی مجاری سایت به سایت میتوانید با بکارگیری Ipsec این اطلاعات پنهانی را بدست آورید .

ماژولهای تجارت الکترونیکی

بخاطر اینکه تجارت الکترونیکی هدف اصلی این ماژول است از بین دسترسی و امنیت باید به دقت رفع شود .

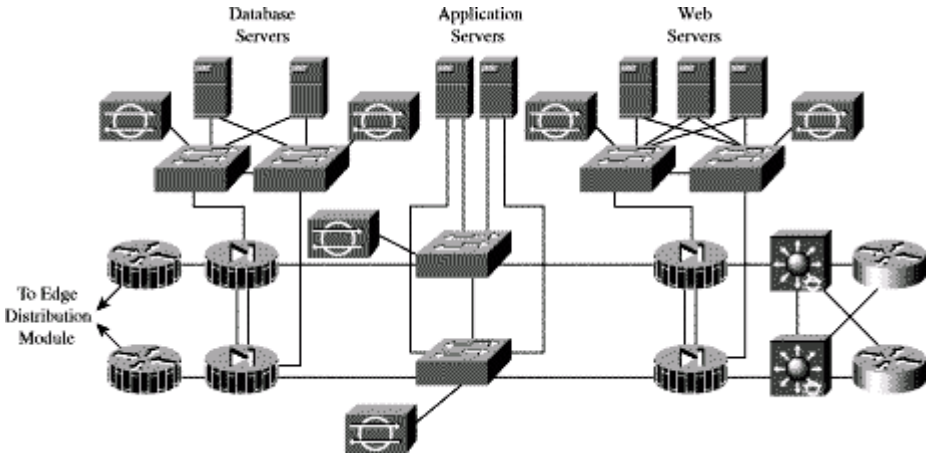
تقسیم مسئله تجارت الکترونیک به سه مقسمت به طراحان معماری اجازه میدهد که سطوح مختلف امنیتی را بدون ممانعت از دسترسی مهیا کنند .



شکل ۲۶ - جریان ترافیکی تجارت الکترونیک

ابزارهای کلیدی

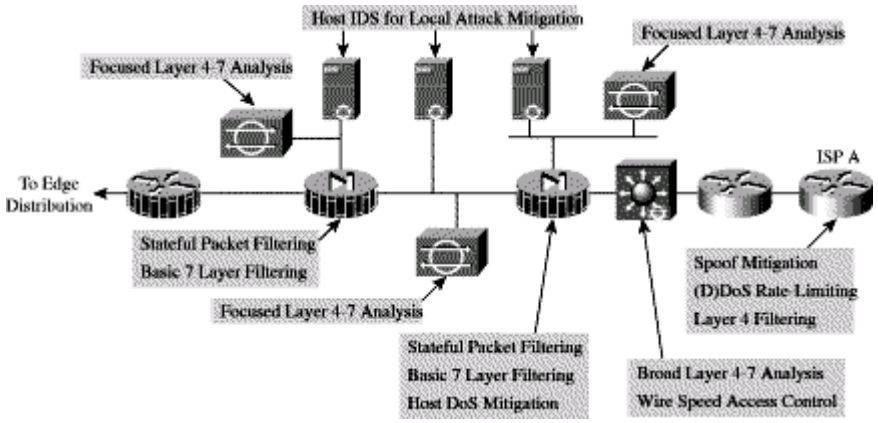
- سرویس دهنده وب(Webserver) – بعنوان یک رابط کاربرد اصلی برای هدایت به منبع تجارت الکترونیک عمل میکند .
- (Application server) سرویس دهنده بانک اطلاعاتی – اطلاعات حساسی است که قلب حرفه تجارت الکترونیکی را پیاده سازی میکند .
- FierWall – ارتباط را بین سطوح مختلف حفاظتی را کنترل می کنند و سیستم را مطمئن می کنند .
- ابزارهای NIDS (NIDS applience) – کنترل و نظارت بر بخشهای کلیدی شبکه را در ماژول فراهم میکند .
- سوئیچهای لایه ۳ در ماژول IDS – ابزارهای ورودی طبقه بندی شده تجارت الکترونیکی با کنترل حفاظتی



شکل ۲۷ – جزئیات ماژول E-Commerce

کاهش تهدیدات

- unewthorized Access – دسترسی غیرمجاز
- حملات به لایه برنامه های کاربردی (Application layer Attack) – با استفاده از IDS حملات کاهش پیدا میکنند .
- رد سرویس(Denial servis) - تصفیه سازی ISP و سرعت محدود باعث کاهش DOSP پنهانی میشود .
- IPSpoofing – RFC 1918, 2827, بسته های تقلبی تولدی شده را جلوگیری کرده و تلاشهای تقلبی خارجی را محدود میکند .
- Packetshitte – (بسته های نفوذی) سوئیچهای زیرساختاری و HIDS تاثیر نفوذ را محدود میکند
- شناسایی شبکه (network Reconnaissawce) – پورتها محدود می شوند به چیزهایی که فقط ضروری هستند و ICMP هم محدود میشود .
- Trust exploitetion (بهره برداری از اعتماد) – دیواره آتش جریان ارتباطات را تامین می کند فقط در جهت صحیح و بر روی سرویسها ی صحیح
- Port Redirection (تعیین جهت و پورت) – HIDS و دیواره آتش محدود می کند برای این حملات



شکل ۲۸ – قوانین کاهش حملات برای ماژول E-Commerce

شرح پیاده سازی طراحی

دو جفت دیواره آتش عدول کننده قلب قسمت اصلی این ماژول هستند که امنیت را برای سه نوع از سرویس دهنده های وب و برنامه های کاربردی و بانکهای اطلاعاتی تامین میکنند .

نکات امنیتی بیشتر توسط مسیریابهای حاشیه ای ISP در ISP فراهم میشود و ...

این طراحی بهتر فهمیده میشود با مطالعه ترتیب جریان ترافیک و جهت آن برای یک نمونه انجام شده تجارت الکترونیکی .مشتریان تجارت الکترونیک شناخته می‌شوند یک اتصال HTTP به سرویس‌دهنده وب بعد از اینکهٔک آدرس IP را دریافت کردند, یک سرویس‌دهنده DNS که در شبکه ISP میزبان می‌باشد DNS بر رد شبکه‌های مختلف‌وجود دارد تا حجم پروتکلهای موردنیاز برنامه‌های تجارت الکتریکی راکاهش دهد. اول باید یک تعداد دیواره آتش (فایر وال) باید تنظیم شوند تا به طریق پروتکل اجازه دهند که به آدرس مشخصی برود . به ترافیک بازگشتی برای این ارتباط اجازه عقب‌نشینی داده می‌شود و اما نیازی نیست که برای هر ارتباط که بوسیله سرویس دهنده‌های وب خارج از اینترنت شناخته شود فایروال باید این سهمیه را مسدود کند بجای اینکه اختیارات را محدود کند اگر آنها یکی از سرویس دهنده‌های وب را کنترل کنند -. اگرکاربرانی که بهٔک سایت هدایت می‌شوند انتخاب پیوند مطمئن باعث می‌شود که سرویس دهنده وب یک درخواست را به سرویس دهنده برنامه کاربران را در داخل رابط وارد کند. برقراری ارتباط باید بوسیله فایروال اول برقرار شود به همان خوبی که ترافیک‌برگشتی جمع می‌شود. بنابراین در این حالت با سرویس‌دهنده‌های وب و دلیلی نمی‌ماند برای سرویس‌دهنده برنامه کاربردی در یک ارتباط را با سرویس دهنده وب آغاز کند یا حتی بیرون از اینترنت. همچنین کاربران کل منطقه بر روی HIIPو SSL هدایت می‌شوند بدون اینکه‌توانایی ارتباط مستقیم با سرویس دهنده برنامه کاربردی یا بانک اطلاعاتی راداشته باشند .

به عنوان یک نکته ، کاربر می‌خواهد تراکنش اجرا کند . سرویس دهنده وب‌می‌خواهد در این تراکنش را محافظت کند و پروتکل SSL موردنیاز است ازطرف اینترنت به سرویس دهنده وب – در همان لحظه و سرویس دهنده برنامه‌کاربردی ممکن است بخواهد جستجو کند . با اطلاعاتی را به سرویس دهنده بانک اطلاعاتی انتقال دهد . اینها نمونه‌های واقعی SQL هستند ، که از طرف سرویس دهنده برنامه کاربردی به طرف سرویس دهنده بانک اطلاعاتی اعمال می شوند و نه برعکس . این جستجوها ازمیان فایر وال دوم برروی سرویس دهنده بانک اطلاعاتی‌اجرا می‌شوند -. بسته به برنامه‌های کاربردی خامی که بکار می‌روند ، سرویس‌دهنده وب ممکن است نیازمند این باشد که بۀک سیستم back end ثابت شود . ماژولهای‌مهمم سرویس‌دهنده . بطور خلاصه و فایر والها تنها باید به سه نوع خاص اتصالات اجازه عبور دهند ، که هر کدام پروتکل مخصوص به خود دارد و تمام ارتباطهای دیگر را مسدود کند مگر اینکه سیم بسته‌هایی را که در سه مسیر اصلی متصل شده‌اند برگرداند.

سرویس‌دهنده‌ها به خودی خود باید کاملا محافظت شده باشند بخصوص‌سرویس دهنده‌های وب که به صورت عمومی میزبان قابل دسترسی هستند . برنامه‌های کاربرای سیستم عامل و سرویس دهنده‌های وب باید بوسیله آخرین‌نسخه اصلاح شوند (جایگزین). و بازرسی شوند بوسیله نرم‌افزارهای شناسایی محلی به میزبان این باید بسیاری ازمحلات اولیه و ثانویه به لایه نرم‌افزارهای کاربردی مانند جهت‌یابی پورتها را کاهش می‌دهند . سرویس‌دهنده‌های دیگر همه باید امنیت متشابهی داشته باشند . در این حالت و اولین سرویس‌دهندۀا فایروال بمخاطره می‌افتد .

آنسوی فایروا ل

فایروالهای تجارت الکترونیکی در ابتدا بوسیله مسیریابهای حاشیه‌ای مشتری در ISPمحافظت می‌شوند . در نقطه ورودی ISP می‌تواند ترافیک را محدود کند به تعداد پروتکلهای موردنیاز کمتری برای تجارت الکترونیک بوسیله آدرس مقصدسرویس دهنده‌های وب . پروتکلهای مسیریابی جدید برای مسیریابهای‌حاشیه‌ای ضروری است (مانند BGP) و تمام ترددهای دیگر باید متوقف شوند .ISP باید محدودیت سرعت دسترسی راپیاده‌سازی کند بطوری که در قواعدsale ذکر شده تا ازمحلات DOS را کاهش دهیم . بعلاوه تصفیه‌سازی برطبقRFC 2&2, RFC 1918 هم باید توسط ISP پیاده‌سازی شود .مسیریابهای نخستین فقط به عنوان یک رابط برای ISP عمل می‌کنند . سوئیچهای‌لایه ۳ تمام پردازشهای شبکه را انجا می‌دهد . بخاطر اینکه در آینده به پرداتکس‌سخت‌افزاری بار خواهد شد .سوئیچهای لایه ۳ در تصمیمات مسیریابی BGP کاملا دخالت دارند برای اینکه‌معین کنند کدام ISP مسیریابی بهتری را به کاربران اختصاصی خود می‌دهد .سوئیچهای لایه ۳ همچنین رسیدگی و تصدیق امر تصفیه‌سازی را مهیا می‌کنند که‌به وسیله صافیهای ISP نگهداری می‌شود که در بالا توضیح داده شود که این‌امنیت مفلاعفی را مهیا می‌کند. سوم و سوئیچهای ۳ کنترل IDS را فراهم می‌کنند . اگر اتصال به اینترنت بیشتر ازظرفیت کارت خطی

IDSشود شما ممکن است فقط احتیاج داشته باشد که به‌تقاضاهای وارد شونده از اینترنت از طریق کارت خطی IDS نگاه کنید . این‌ممکن است بعضی از اعلان‌های HTTP را گم کند (تقریبٌ ۱۰ درصد) که این‌بهتر است از اینکه تتمام مجرای ورودی و خروجی را نظارت کند و جایی که‌تعداد زیادی عدم موفقیت رخ می‌دهد . سایر ابزارهای NIDS درپشت‌واسطه‌های مختلف فایروال بخشهای مختلف بخاطر حمله‌هایی که امکان داردنفوذ کنند را در اولین خط دفاعی تشخیص و کنترل کند . برای مثال و اگر سرویس‌دهنده وب تاریخش بگذرد ، می‌توانند آن را به مخاطره بیندازند .بواسطه حمله به لایه نرم افزارهای کاربردی فرض کنید آنها قادر باشند HIPS رافریب دهند . بعنوان مثال در مماژلهای اینترنتی متصد ، خطای مسلم باید حذف‌شود بنابراین تمام حملات ضعیفی که شناسایی می‌شوند با یک سطح تقدم‌درستی با آنها رفتار می‌شود . درواقع بخاطر اینکه نوع معین ترافیکهای موجود برروی بخشهای معین ، شما می‌توانید به سختی NIDS را وفق دهند .از نقطه نظر یک برنامه کاربردی و مسیر ارتباطی بین لایه‌های مختلف (وب (apps , dbaseباید حرف‌گزاری شود و معامله شود و بشدت تصحیح شود . به‌طور مثال اگر سرویس دهنده apps جایی که داده‌اند بانکهای اطلاعاتی دریافت‌می‌کنند بواسطه scriptهای فعال بخشها (telnet, FTP , SSH) یک مکس‌می‌تواند .با بکارگیری ارتباطات امن شما می‌توانید تهدیدات نهایی را محدود کند .سوئیچهای لایه ۲ که بخشهای مختلف فایروال را پشتیبانی می‌کنندامکان‌پیاده‌سازی شبکه‌های مجازی خصوصی را فراهم می‌کنند. در نتیجه پیاده‌سازی یک مدل صحیح که ارتباط مطلوبی را بوجود می‌آورد برروی یک بخش مخصوص و بقیه را بکلی حذف می‌کند .برای مثال ، معمولا دلیلی وجودندارد کهٔک سرویس دهنده وب با سرویس‌دهنده وب دیگری در ارتباط داشته باشد مدیریت کل ماژول کاملا انجام می‌شودهمانند اکثر معماری آن .**اختیارات** انتخاب عمده برای این توسعه و ترقی محل سیستم ISP است . اگرچه طراحی‌این‌چنین به نظر می‌رسد که دو اختلاف اساسی وجود دارد اول اینکه پهنای باندمعمولا عریض است . برای ISP و برای یک ارتباط شبکه‌ای بکار می‌رود . اماسفاش نمی‌شود که بالقوه احتیاج مسیریابهای حاشیه‌ای در نقشه طراحی رامختصر می‌کند . پهنای باند اضافی همچنین نیازمندیهای مختلفی را برای تخفیف DOSایجاد می‌کند . دوم اینکه نیازمند مدیریت از روشهای مختلف است .اختیارات شامل پنهان سازی و خطهای اختصاصی است .بکارگیری این تکنولوژی دقت امنیتی اضافی را بوجود می‌آورد .بر روی محل‌ارتباط و مقاصد بکارگیری اختلافات مختلفی برای طراحی مقدماتی این ماژول‌وجود دارد و در کنار شنیدن این اختیارات پیشتر دررابطه با وسعت این مقاله‌بحث می‌کنید. بکارگیری فایروالهای اضافی یک انتخاب است . ارتباط ساده مسیریاب حاشیه‌ای‌خواهد بود که فایروال سرویس دهنده فایر وال سرویس‌دهنده برنامه‌های کاربردی سرویس دهنده بانک اطلاعاتی این به دوفایروال اجازه می‌دهد که تنها ارتباط یک سیستم ابتدایی را کنترل کنند .تکنولوژی توازن بار کردن و پنهان سازی (caching) به طور اختصاصی در این‌مقاله بحث نمی‌شود. ۀ برای ملزومات امنیتی در حد بالا ، بکارگیری فایروالهای چندگانه ممکن است‌نیاز باشد . بیاد داشته باشید ایجاد کنترلهای اضافی روشهای دوگانه‌ای بر روی‌سیتم‌هایی مختلف ایجاد می‌کند . مقصود اصلی این فایروالهای مرکزی بیشتری و بطور مناسب فواید

IDSرادربرنمی‌گیرد و سایر تکنولوژیهای امنیتی ریسک طراحی جلوگیری ازآسیب‌پذیری یک فایروال برای فریب دادن امنیت کل سیستم استت . این نوع‌طراحی می‌شود . آسیب‌پذیری تک فایروالی راکاهش می‌دهد .

انتخابهای خارق‌العاده

پروسه طراحی همیشهٔ‌کسری کارهای تجاربتی است این بخش کوچک این‌مقاله بعضی از بخشهایی سطح بالای انتخابهایی را روشن می‌کند کهٔ‌ک طراح‌شبکه می‌تواند بکار ببرد وقتی که شما با کمبود بودجه اضطراری مواجه هستید .بعضی از این عملیات تجاری در سطح ماژول انجام می‌شود ، هنگامی که بقیه‌آنها در سطح اجزاء انجام می‌شود. اولین انتخاب تبدیل ماژولهای گسترده به ماژولهای هسته‌ای است که این باعث‌کاهش ۵۰ درصدی سوئیچهای لایه ۳ می‌شود . هزینه صرفه‌جویی شود ممکن‌است برای علیه ضروریات بازده بالا خرج شود در هسته شبکه و انعطاف‌پذیری‌برای پیاده‌سازی صافیهای امنیتی .

انتخاب دوم ادغام عملیاتی VPN و ماژول دسترسی از راه دور بوسیله ماژولهای‌اینترنتی متصد . ساختار آنها خیلی بهم شبیه است . بوسیلهٔ‌ک جفت فایروال درجواب یک ماژول ، که بوسیله ابزارهای NID احاطه شده‌اند. این ممکن است امکان‌پذیر باشد بدون از دست دادن کارایی اگر بهره‌وری اجزاءکه ترکیب ملزومات ترافیک ماژول را تشکیل می‌دهند . و اگر فایروال‌واسطه‌های کافی داشته باشند تا سرویسهای مختلفی ار تطبیق دهند . در ذهن داشته‌باشید که اگر فعالیتها در یک وسیله متراکم شوند توانایی بوجود آوردن خطافزایش می‌یابد. بعضی از سازمانها از این همه جلوتر رفتند و شامل وظایف تجارت الکترونیکی‌در مماژولهای متصد اینترنتی VPN هستند. نویسنده احساس می‌کند که ریسک انجام چنین کاری بالاتر از صرفه‌جویی‌هزینه است مگر اینکه نیازمندیها تجارت جهانی در حد مینیمم باشد .جداسازی ترافیک تجارت الکترونیکی از ترافیک عمومی اینترنت به پهنای باندتجارت الکترونیکی امکان می‌دهد که در بهتر بهینه شود . با دادن مجوزیه ISP تاصافیهای بیشتری را ایجاد کند و ایجاد محرومیتهای تکنولوژی برای کاهش‌حملات علیهDDOS .

انتخاب سوم این است که بعضی از ابزارهای WINDرا حذف کنید . بستگی داردبه استراتژی شما در پاسخگوئی به تهدیدات ، شما ممکن است به تعداد کمتری‌ابزار NIDS احتیاج داشته باشید . این تعداد همچنین تغییر پیدا می‌کند بواسطه‌گسترش متداد IDSهای خمیربان به خاطر اینکه ممکن است نیاز به NIDS را درمکانهای معلومی کاهش دهد .واضح است که طراحی شبکه دقیقا یک علم نیست انتخابها همیشه بستگی داردبه نیازهایی به خصوصی که طراح با آنها روبرو می‌شود . اما نویسنده پیشنهادنمی‌کند که هر طراحی از این معماری جزء به جزء در پیاده‌سازی استفاده کنند .اما طراحان تشویق خواهند شد تا انتخابهای تعلیم‌یافته‌ای را در امنیت شبکه درپیاده‌ساز ایشان بکار برند .

استراتژی مهاجرت

safe یک راهنما برای پیاده‌سازی امنیت در شبکه خارق‌العاده است . به معنی این‌نست که سرویس دهد برای هر شبکه خارق‌العاده‌ای و به این معنی هم نیست به‌کار گرفته شود بعنوان کل طرحی کامل برای فراهم‌کردن امنیتی کامل برای تمام‌شبکه‌های موجود ایجاد کند . ترجیحا و safe یک template است . که طراحان‌شبکه را قادر می‌سازد که چگونه شبکه خارق‌العاده‌شان را طراحی کرده وبسازند .پیاده‌سازی یک متد امنیتی باید اولین فعالیتی باشد که در مهاجرت شبکه بهٔک‌زیرساختار امنیتی انجام می‌شود .

پیشنهادات اساسی برای متد امنیتی ممکن است‌یافت شود در انتهای مقاله در قسمت B امنیت آغازین شبکه بعد از این که شبکه‌برقرار شد ، طراحان شبکه به قیمت آشکار توصیف شده در رابطه با امنیت را دربخش اول این مقاله بکار ببرند و ببینند که چگونه می‌توانند جزئیات بیشتری رابرای طراحی این متدها برروی شبکه‌های موجود اعمال کنند .

انعطاف کافی درمعماری و جزئیات safe وجود دارد تا با بیشتر شبکه‌های خارق‌العاده وفق‌پذیرباشد .برای مثال در ماژولهای VPNو دسترسی از دور ، جریانهای مختلف ترافیکی‌شبکه‌های عمومی فرستاده می‌شود به جفتهای جداگانه‌ای از ابزارهای خاتمه‌دهند و واسطه‌های جدا برروی فایر وا ل ترافیک VPN می‌تواند برروی یک‌جفت وسیله ترکیب شود اگر ابزار بارکردن آنها و متدهای امنیتی هر دو نوع‌ترافیک یکی باشد . در شبکه دیگر safe-به طراحان امکان می‌دهد که هر کدام از نیازمندیهای امنیتی هر قسمت ازشبکه را مستقل از بخشهای دیگر تعیین کنند .

در مدت آغازین پیاده‌سازی، safeماژول نظارت و کنترل باید به‌طور موازی با ساخت اولین ماژول پیاده‌سازی‌شود. وقتی که قسمت اعظم شبکه مهاجرت کرد ، ماژول نظارت و کنترل می‌تواند به دوقسمت قبلی متصل شود .

اولین نسخه معماری safe یعنی اینکه پیاده‌سازی امن یک شبکه خارق‌العاده‌نویسنده معتقد است که نواحی زیادی وجود دارد که جزئیات بیشتری را تشریع‌خواهند کرد مانند تحقیقات وپیاده‌سازی. ـ تعدادی از این نواحی در زیر عنوان شده است ، اما تنها به این نواحی محدودنمی‌شود.

- تجزیه و تحلیل پیاده‌سازی کنترل و امنیت در عمق(indepth)
- اطلاعات تخصصی طراحی شبکه‌های کوچکترشناسایی
- در عمق ، سرویسهای راهنما ، تکنولوژیهای ، AAA و گواهینامه‌محتسب تجزیه و تحلیل و پیاده‌سازی.
- نسخه‌های طراحی VPNابتدا ـ انتها و طراحی WAN

پیوست ب : امنیت ابتدایی شبکه

ضرورت امنیت شبکه :

اینترنت روش و راه اسم کار .زندگی . باذی و آموختن را تغییر داده . این تغییرات اتفاق می افتد در راهها و روشهایی که مه هم اکنون تجربه می کنیم (تجارت الکترووونیک ، دسترسی بلادرنگ به اطلاعات ، آموزش الکترونیکی ، گسترش ارتباطات اختیاری و مانند آن) .راه حلهایی که ما هم اکنون در حال آزمابش هستیم ، یک روزی راتصور کنید که شما بطور خارق العاده بتوانید تمام تلفنهای خود را از طریق اینترنت بطور رایگان انجام دهید .یا در بیشتر تفسیر های شخصی ، توجه کنید بۀک مراقب سایت مهیا کننده وب واردمیشوید تا بررسی کنید فرزند شما در طول روز چه کارهایی انجام داده است .بعنوان یک شرکت ، ما فقط مانع محبوس شدن امکانات اینترنت می شویم ، اما بواسطه رشد غیر معمول اینترنت امکان ارائه بی سابقه داده های شخصی و منابع خارق العاده بحرانی اسرار حکومتی و سایر چیزها بوجود می آید .

هر روزه Hacker ها تهدیدات خود را علیه این موجودات با افزایش انواع گوناگون حملات بیشتر کرده وبستوه می آورند .این حملات ، بطور مختصردر بعدی شرح داده می شود ، که هر دو برای پیاده سازی بسیار با Router ساده تر خواهد بود . در اینجا دو دلیل اولیه برای این مشکل وجود دارد .

- اول حضور همه جائی اینترنت است . بوسیله میلیونها ابزاری که در حال حاضر متصل به اینترنت هستند و بیشتر از میلیونها که راه هستند و دسترسی به ابزارهای قابل انتقاد مدام افزایش می یابد . خضور همه جانبه اینترنت به Hacker ها اجازه می دهد که اطلاعات و معلومات را در مقیاس عمومی به اشتراک بگذارند . یک جستجوی ساده اینترنتی بر روی کلمات Hack , Crack یا Phreak هزاران سایت را نشان می دهد که بیشتر آنها شامل کدهای بد خواه ومضری هستند و یا بمعنی آنهائی است که از این کدها استفاده می کنند .
- دوم بهم قوه سرایت آنهاست که به سادگی از سیستمهای راه انداز استفاده می کنند و در محیط گسترش می یابند . این فاکتور روی هم رفته استعداد ومعلومات نورد نیاز Hacker ها را کاهش می دهد . یک Hacker برجسته می تواند توسعه پیدا کند تا به سادگی از برنامه های کاربردی استفاده کند که میتواند مانند یک توده گسترش یابد . وسایل مختلف Hacker ها که در دامنه عمومی مهیا هستند فقط احتیاج بۀک آدرس IP یا نام میزبان و یک کلیک دکمه موس دارند تا یک حمله را به اجرا درآورند .

طبقه بندی حملات شبکه :

حملات شبکه می تواند به اندازه سیستمهای متنوعی که تلاش می شود به داخل آنها نفوذ یابند متنوع باشد . بعضی حملات بطور استادانه پیچیده هستند ، اگر چه بقیه ناشناس هستند و بوسیلۀک نیت معلوم راه اندازی می شوند .این خیلی مهم است که بعضی از این محدودیتهای ذاتی پروتکل TCP/IP را بفهمند هنگامی که نوع حملات را ارزیابی می کنیم . هنگامی که اینترنت شکل گرفت ، موجودیتهای گوناگون حکومتها و دانشگاهها را بۀکدیگر متصل کرد ، بوسیله آن اهداف یادگیری و

پژوهش و تحقیق بسادگی امکان پذیر است . معماری عمومی اینترنت هرگز محوه انتشار و اقتباس را مه اینترنت امروزه به آن رسیده را پیش بینی نمی کنیم . در نتیجه در روزهای کنونی پروتکل اینترنت (IP) ، امنیت بطور صحیح طراحی نشده است و برای این دلیل ، بیشتر IPهای پیاده سازی بطور ذاتی نا امن هستند . تنها بعد از سالهای زیاد و هزاران تقاضا برای نظریه ها (RFC) و ایا نا ابزارهایی برای شروع بکارگیری IP مطمئن داریم . بخاطر اینکه شرطهای بخصوص برای IP مطمئن از حملات طراحی نشده است و این مهم است که پیاده سازی IP بوسیله روشهای امنیتی شبکه ، سرویسها ، محصولات افزون شده تا ریسک ذاتی بکارگیری پروتکل اینترنتی را کاهش دهد .شرح زیرین یک بحث مختص انواع حملات معمولی است که در شبکه های IP دیده می شود و چگونه حملات را کاهش داد .