به نام خدا

سازنده: سهراب نیازی

وب سایت: WwW.NiaziSoft.blogfa.CoM

ایمیل : NiaziSoft_Help@Yahoo.CoM

موضوع: امنیت اطلاعات

اصول مهم امنیت اطلاعات

تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از راز داری و امانت داری (Confidentiality) ، یکپارچگی (Integrity) و در نهایت در دسترس بودن همیشگی (Availability). این سه عامل (CIA) اصول اساسی امنیت اطلاعات - در شبکه و یا بیرون آن - را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است.

Confidentiality: به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و اینگونه تعریف شده است. بعنوان مثال از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات

Integrity: بیشتر مفهومی است که به علوم سیستمی باز می گردد و بطور خلاصه می توان آنرا اینگونه تعریف کرد:

- تغییرات در اطلاعات فقط باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد.

- تغییرات بدون اجاز و بدون دلیل حتی توسط افراد یا پروسه های مجاز نباید صورت بگیرد.

- یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج آن باید یکسان باشد و اگر تغییر می کند باید همزمان درون و برون سیستم از آن آگاه شوند.

Availability: این پارامتر ضمانت می کند که یک سیستم - مثلا" اطلاعاتی - همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مد نظر باشد اما عواملی باعث خوابیدن سیستم شوند - مانند قطع برق - از نظر یک سیستم امنیتی این سیستم ایمن نیست.

اما جدای از مسائل بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می شوند برای خود شخصیت جداگانه ای پیدا کرده اند. در این میان می توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authentication به معنی مشخص کردن هویت کاربر، Authorization به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountability به معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد.

هکر اغلب سعی در آسیب رساندن به شبکه را دارد

مهمترین وظیفه یک شبکه کامپیوتری فراهم سازی امکان برقراری ارتباط میان گره های آن در تمام زمانها و شرایط گوناگون است بصورتی که برخی از محققین امنیت در یک شبکه را معادل استحکام و عدم بروز اختلال در آن می دانند. یعنی Security=Robustness+Fault Tolerance . هر چند از زاویه ای این تعریف می تواند درست باشد اما بهتر است اضافه کنیم که امینت در یک شبکه علاوه بر امنیت کارکردی به معنی خصوصی بودن ارتباطات نیز هست. شبکه ای که درست کار کند و مورد حمله ویروسها و عوامل خارجی قرار نگیرد اما در عوض تبادل اطلاعات میان دو نفر در آن توسط دیگران شنود شود ایمن نیست.

فرض کنید می خواهید با یک نفر در شبکه تبادل اطلاعات - بصورت email یا chat و ... - داشته باشید، در اینصورت مصادیق امنیت در شبکه به این شکل است :

هیچ کس (فرد یا دستگاه) نباید بتواند

- وارد کامپیوتر شما و دوستتان شود،

- تبادل اطلاعات شما را بشنود و یا از آن کپی زنده تهیه کند،

- با شبیه سازی کامپیوتر دوست شما، بعنوان او با شما تبادل اطلاعات کند،

- کامپیوتر شما یا دوستتان را از کار بیندازد،

- از منابع کامپیوتر شما برای مقاصد خود استفاده کند،

- برنامه مورد علاقه خود - یا یک تکه کد کوچک - را در کامپیوتر شما نصب کند،

- در مسیر ارتباطی میان شما و دوستتان اختلال بوجود آورد،

- با سوء استفاده از کامپیوتر شما به دیگران حمله کند،

- و بسیاری موارد دیگر ...

اما ببینیم که چه کسانی - فرد، دستگاه، نرم افزار و ... - می توانند امنیت ارتباط برقرار شده شما را تهدید کنند.

هکر (Hacker)

در معنای لغوی به فردی گفته می شود که با ابزار به ساخت لوازم خانه (میز، مبل و ...) می پردازد. اما امروزه این اصطلاح بیشتر به افرادی اطلاق می شود که علاقمند به کشف رمز و راز برنامه های مختلف نصب شده روی کامپیوترها می باشند تا به این وسیله دانش و توانایی خود را بالا ببرند. اینگونه افراد معمولا" دانش زیادی از نحوه کار کامپیوتر و سیستم های شبکه ای دارند و اغلب بطور غیر مجاز سعی در ورود به سیستم های اطلاعاتی یا کامپیوتر های شخصی افراد می کنند.

اما معنی عمومی تر این لغت امروزه از موارد بالا نیز فراتر رفته و به افرادی گفته میشود که برای خرابکاری و یا سرقت اطلاعات و ... وارد کامپیوترها یا شبکه های کامپیوتری دیگران می شوند. قصد یا غرض این افراد از انجام اینکار ها می تواند تمام مواردی باشد که در مطلب قبل امنیت در دنیای واقعی به آن اشاره کردیم، باشد. امروزه فعالیت این افراد در بسیاری از کشورها در رده فعالیت های جنایی در نظر گرفته می شود.

ویروس (Virus)

همانطور که میدانید از لحاظ بیولوژیکی موجودات کوچکی که توانایی تکثیر در درون سلولهای زنده را دارند و اغلب باعث بروز بیماری ها مانند سرما خوردگی، سرخک، هپاتیت و ... می شوند، ویروس نام دارند. ویروس ها عموما" با استفاده از روشهای مختلف در جامعه انسانی - یا حیوانی - منتشر میشوند و در صورت عدم وجود کنترل و درمانها پزشکی خطرات جبران ناپذیری را به جامعه تحمیل می کنند.

با ایده برداری از همین روش یعنی زندگی در بدن یک میزبان و انتقال به هنگام تعامل میزبان با همسان خود، نرم افزارهای عموما" کوچکی تهیه شده است که می توانند در یک دستگاه کامپیوتر اجرا شوند و ضمن به خطر انداختن کار آن دستگاه به هنگام تبادل اطلاعات - به هر شکلی - با دیگر کامپیوتر ها خود را پخش کنند. این تبادل می تواند از طریق کپی کردن اطلاعات در روی دیسک باشد، یا اجرا برنامه های کامپیوتر و ...

کرم های شبکه (Worms)

همانطور که میدانید حیوانات کوچک، باریک و درازی که بدنی نرم دارند و اغلب در روی زمین، درختان و گیاهان یا حتی زیر خاک زندگی کرده و از برگ گیاهان، حشرات و ... تغذیه میکنند، کرم نامیده می شود.

اما در دنیای کامپیوتر و ارتباطات اینترنتی کرم به گونه ای از نرم افزارها گفته می شود که در گره های شبکه - مثلا" کامپیوتر - مستقر شده و می تواند علاوه بر زندگی و آسیب رسان به آن گره نسخه دیگری از خود را از طریق شبکه به سایر گره ها منتقل کند و آنها را نیز دچار مشکل سازد. بنابراین مشاهده می کنید که سرعت تولید مثل و انتشار یک کرم در شبکه بزرگ چه مقدار می تواند زیاد باشد.

کرم ها معمولا" علاوه بر آنکه باعث تخریب میزبان خود می شوند، با اشغال کردن فضای ارتباطی در شبکه، تاثیری چون ترافیک و کندی ارتباطات در شبکه را به همراه می آورند که این خود می تواند عوارض بعدی برای فعالیت سایر تجهیزات در شبکه و یا حتی بخش عمده ای از شبکه اینترنت شود.

بررسی نقاط ضعف امنیتی شبکه های وب

در ادامه بحث امنیت شبکه‌های وب، به بررسی عوامل تضعیف سرویس دهندگان وب و علل مهیا شدن زمینه نفوذ و تهاجم به سایت‌ها، بخصوص مراکز فعالیت‌های اقتصادی خواهیم پرداخت.

همانطور که می‌دانیم ایجاد امکان مراودات الکترونیکی در اینترنت با احتساب مزایا و محاسن بیشمار خود، مشکلات عدیده ای را نیز به همراه داشته است .در حقیقت هر یک از طرفین (سرویس دهندگان و سرویس

گیرندگان) با نگرانی های جدی مواجه هستند و در همین راستا، جهت ایمن‌سازی مراودات خود از یکدیگر انتظاراتی را مطرح می‌نمایند.

ایجاد ایمنی و رفع هرگونه تهدید در انجام معلامات و یا تراکنش‌های اقتصادی، و نیز قانونمند و مطمئن بودن فعالیت و مخفی ماندن اطلاعات مربوطه به آن بعنوان توقعات مشتریان مطرح می‌شود و در مقابل فعالیت همراه با دقت کاربر، عدم انجام اعمال خلاف قوائد و قوانین شبکه و مراودات الکترونیکی و نهایتاً اجتناب از تخریب و یا صدمه‌زدن به سایت از انتظارات سرویس دهندگان می‌باشد.

در عین حال هر دو طرف از واسطه انتقال دهنده اطلاعات که همانا سیستم‌های مخابراتی هستند توقع جلوگیری از استراق اطلاعات و ... را خواهند داشت.

در حقیقت در مباحث مربوط به امنیت شبکه، ایمنی کاربر، ایمنی سرویس‌دهنده و ایمنی مخابراتی از رئوس مطالب مورد توجه می‌باشند.

در ادامه سعی در بررسی کاستی‌های مجموعه خواهیم نمود :

1 عدم نصب صحیح سسیتم عامل‌های اصلی شبکه

یکی از اصلی‌ترین دلائل بروز حمله به سایت‌های اینترنتی حفره‌های موجود در نرم‌افزارهای سیستم عامل به جهت عدم نصب اصولی و تکنیکی آنها می‌باشد. در حقیقت عدم شناخت و آگاهی کافی برخی از مسئولین سایت ها از امکانات، محاسن و معایب و حفره‌های موجود در سیستم عامل مورد استفاده موجب می شود مبحث انجام تنظیمات صحیح به دقت و درستی انجام نشده و به سادگی، زمینه جهت ورود غیر مجاز مهاجم مهیا شود. بسته نبودن Port های موجود در مجموعه سرویسهای یک Server به لحاظ امنیتی بسیار خطرناک می باشد که در بسیاری از موارد به جهت عدم دقت مسئولین مربوطه، مسیر هموار جهت ورود مهاجمین هکرها بوجود می‌آورد.

2 وجود کاستی‌های فراوان در ساختار سیستم عامل‌ها

متأسفانه علیرغم پیشرفت‌های شگرف دنیای سیستم عامل‌ها، متأسفانه علاوه بر مشکل عدم آگاهی نسبی برخی از متخصصین شبکه، وجود مشکلات بنیادی در بدنه نرم افزارهای Server نیز عامل ضعف دیگری برای آنها به شمار می‌رود. در حقیقت بسیاری از سیستم عامل های Server دارای نقایص فراوانی به لحاظ حفظ امنیت می‌باشند که بدیهی است با گذشت زمان نقاط ضعفشان شناسایی و رفع می‌گردد.

3 اجازه استفاده از سرویس‌های گوناگون درServer

اجازه استفاده از سرویس‌های گوناگونی همچون Telnet , FTP , IRC , HTTP و ... زمینه‌ساز هجوم‌های غیر مجاز فراوان در سرورها می‌باشد. در حقیقت هر یک از درگاههای ورودی مذکور (ports) ، مسیری هموار جهت نفوذهای غیرمجاز به داخل سرورها می‌باشد که می‌بایست با توجه به شرایط مورد نیاز کاربران در آنها محدودیت‌های لازم اعمال گردد و یا در صورت عدم توجیه امنیتی مناسب برای حضور هر یک، از آنها صرف نظر شود.

4 وجود مشکلات امنیتی در پروتکل‌ها

اتصال شبکه‌ها در اینترنت معمولاً با استفاده از پروتکلTCP/IPانجام می‌پذیرد. در همین راستا اجازه استفاده از امکانات HTTP بر روی TCP/IP با توجه به گستردگی سرویس‌های آن مورد توجه قرار گرفته است و لذا وجود حفره‌های فراوان و بسترسازی مناسب برای مهاجمین در این پروتکل مشهور، موجبات پدید آمدن اختلالات امنیتی فراوان در شبکه می‌گردد.

5 عدم رعایت تدابیر امنیتی در نرم‌افزارهای نصب شده بر روی سرور

معمولاً سرویس دهندگان وب جهت سهولت دسترسی و یا انجام امور کاربران و مشتریان خود اقدام به نصب نرم‌افزارهای کاربردی بر روی سیستم خود می‌نمایند که غالباً فاقد تدابیر ملزوم امنیتی می‌باشند. لذا بررسی و

پیش‌بینی اقدامات تأمین در نصب و استفاده از این نوع برنامه‌ها بسیار پراهمیت به نظر می‌رسد. بطور مثال برنامه های تهیه شده بصورت ASP نمونه‌ای از این موارد می‌باشد.

6 عدم استفاده از گزارش فعالیت‌های سیستم و یا کنترل عملکرد کاربران

یکی از مسائلی که باید مورد توجه سرویس دهندگان وب قرار گیرد، نصب و راه‌اندازی نرم‌افزارهای Captureو یا ذخیره کننده Log بر روی سرور می‌باشد. حضور این نوع از قابلیت‌ها بر روی سرور موجب می‌شود تا حرکات مشکوک و خزنده و در عین حال دور از فعالیت‌های معمول روزانه، ثبت و مورد بررسی قرار گیرد. براساس شواهد موجود، مهاجمین قبل از انجام مأموریت اصلی خود، به بررسی وضعیت سرورها پرداخته و جنبه‌های مختلف و امکانات آنها را مورد بررسی قرار می‌دهند. این نوع حرکات در فایلهای Log ثبت می‌شود و با کنترل و بررسی آنها می‌توان اقدامات امنیتی و باز دارنده مناسب قبل از حمله اصلی را اعمال نمود.

متأسفانه با توجه به کثرت مشتریان و کاربران وب، کنترل گزارشهای سیستم برای مسئولین شبکه امری بس مشکل و خسته کننده به نظر آمده و نهایتاً احتمال بروز مشکلات مذکور را افزایش می‌دهد.

7 اعتماد به عملکرد مشتری

یکی دیگر از کاستی‌های سرویس دهندگان در ارائه سرویس‌های آنلاین اعتماد به عملکرد قانونی و صحیح کاربران می‌باشد. در حقیقت همین ذهنیت موجب عدم کنترل کاربران خواهد بود. البته زمینه این مشکل

مشابه مورد ششم این مبحث است اما در اینجا تراکم عملیات‌های انجام شده و درصد محدود بروز خطر برای سرویس دهندگان موجب عدم کنترل عملکرد و تراکنش‌های اقتصادی کاربر می‌گردد. لذا هیچگاه نباید به عملکرد کاربران یک سایت اعتماد کامل داشت.

8 عدم وجود روشهای مناسب شناسایی کاربر

یکی دیگر از نقاط ضعف سرویس دهندگان، عدم استفاده از روشهای مناسب شناسایی کاربران مجاز به استفاده از امکانات سیستم می‌باشد. امروزه شاید عمده‌ترین روش شناسایی کاربرنام شناسایی «User name)و کلمه عبور (Password» او باشد، که براساس آمار یکی از مهمترین راههای سوءاستفاده از سایت‌ها به دست آوردن و استفاده از مورد ذکر شده می‌باشد. در حقیقت نرم‌افزارهائی که به همین جهت (به دست آوردن و یا حدس زدن کلمه عبور) تهیه شده‌اند، به سادگی می‌توانند احتمالات گوناگون کلمات عبور را در زمان بسیار کوتاهی بر روی سرورها بررسی نموده و مقصود را به سرعت بیابند.

در این راستا پیش‌بینی امکانات لازم جهت ایجاد کلمات عبور پیچیده بر روی سرورها از تدابیری است که می‌تواند احتمال بروز اختلال از این طریق را به حداقل برساند .

در حقیقت کاربران ملزم به استفاده از کلمات عبوری باشند که به لحاظ ساختاری نتوان به سادگی به آنها دست یافت.

البته در محافل و انجمن‌های علمی امنیت کامپیوتر و شبکه‌ها ، در این زمینه استانداردهایی تعیین شده است که هم اکنون در سایتهای مشهور مورد استفاده قرار می‌گیرند که خود موجب کاهش یورشهای احتمالی می‌گردد.

9 عدم استفاده از تدابیر امنیتی مناسب و نرم‌افزارهای Firewall وProxy

با توجه به موار ذکر شده در مباحث نقاط ضعف سیستم‌های عامل و پروتوکل‌ها، وجود و استفاده از شیوه‌های نرم‌افزاری بازدارنده بسیار مورد توجه قرار گرفته است.

ایجاد و تهیه نرم‌افزارهایی که با لفظ دیواره آتش Firewall شناخته می‌شوند و نهایتاً نصب و استفاده از آنها بر روی سرور و یا در مسیر حرکت اطلاعات موجب کاهش احتمال یورش و نفوذ به حفره‌های موجود می‌گردد. در حقیقت این نوع نرم‌افزارها بصورت یک سد محکم و یا یک فیلتر در مسیر کاربران واقع می‌گردد و بطور دقیق نحوه عملکرد و مسیر حرکت کاربران و نحوه نقل و انتقالات اطلاعات را کنترل می‌نمایند.

بدیهی است با توجه به پیشرفت تکنیک‌های یورش در بعضی مواقع شاهد پشت سر گذاشتن Firewall ها نیز می‌باشیم و همین موارد موجب می‌گردد تا شرکت‌های نرم‌افزاری در کوتاهترین زمان ممکن در به روز رسانی و رفع نواقص Firewall های خود اقدام نمایند و آنها را در مقابل تهدیدها آماده سازند.

10 عدم شناخت کافی از صحت اطلاعات دریافتی (عدم کنترل اطلاعات)

یکی دیگر از نقاط ضعف موجود در سرویس دهندگان، عدم کنترل اطلاعات دریافتی و ارسالی از سوی کاربران می‌باشد. در حقیقت شیوه‌ای مرسوم که توسط مهاجمان مورد استفاده قرار می‌گیرد، ارسال Script و یا برنامه‌های پس از نفوذ بر روی سرورها می‌باشد که پس از دریافت‌های مذکور، مهاجم به سهولت قابلیت تخریب، تغییر و نهایتاً ایجاد اختلال در سایت را خواهد داشت.

نصب ویروس‌یاب و Firewall های مناسب از این نوع تهدیدها جلوگیری می‌نماید.

11 عدم محافظت از اطلاعات حساس

بسیاری از سرویس دهندگان جهت حفظ اطلاعات حساس خود اقدام به مخفی‌سازی encryption می‌نمایند. البته شکل ساده و تئوریکال قضیه، دور از دسترس قرار دادن اطلاعات است ولیکن روشهای گوناگون جهت انجام این مهم مورد استفاده قرار می‌گیرد که با توجه به اهمیت آن در آینده به آن پرداخته خواهد شد.

عناوین یازده گانه مطروحه، حاکی از اهم نقطه ضعف‌های موجود در سرویس دهندگان وب بوده و سعی در بررسی حفره‌های عمومی موجود در سایت‌های وب داشت ولیکن طرح این سئوال که:

"چرا دیگران علاقمند به نفوذ و خرابکاری در سایت مطلوب ما هستند؟"

بتواند در شناخت عوامل گوناگون و مطرح برای مهاجمین یاری رسان باشد.در نهایت همواره باید به خاطر داشت:

"ایمنی مطلوب امروز، همواره بهتر از ایمنی کامل فرداست"

امن سازی شبکه های بیسیم:

با وجود امکاناتی که در شبکه های مبتنی بر 802.11 ارائه شده است ولی این واقعیت وجود دارد که، چون برای انتقال اطلاعات در این شبکه ها هیچ حد و مرز فیزیکی وجود ندارد و این ترافیک توسط هوا منتقل می شود به این دلیل این نوع شبکه ذاتاً نا امن هستند.

از تمام عناصری که برای ایجاد امنیت در شبکه سیم کشی شده استفاده شده می توان در شبکه های بیسیم نیز برای برقراری امنیت استفاده نمود. نکته مهمی که در شبکه های بیسیم از لحاظ امنتی دارای اهمیت می باشد طراحی این گونه از شبکه های می باشد. در ادامه به چگونگی طراحی امن شبکه های بیسیم می پردازیم.

طراحی شبکه:

یکی از موارد مهم که در طراحی شبکه می بایست در نظر گرفته شود، چگونگی طراحی و نحوه ارتباط با شبکه سیم کشی شده است.

راههای زیادی جهت امن کردن شبکه و همین طور برای به خطر انداختن امنیت آن وجود دارد.

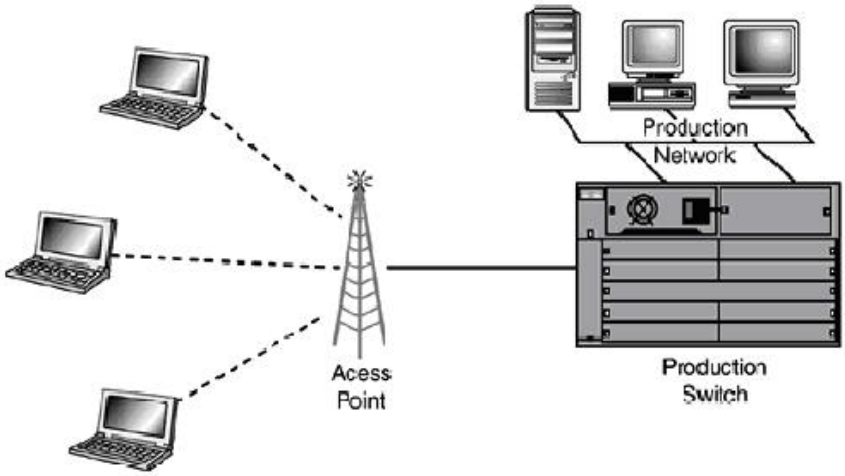
با طراحی و بکار گیری یک استراتژی محکم در شبکه های بیسیم میتوان از دسترسی هکرها به شبکه جلوگیری بعمل آورد همچنین با اعمال کنترل های بیشتر روی بخش بیسیم شبکه، شبکه سیم کشی شده را نیز محافظت نمود تا هکرها از این طریق نیز نتوانند وارد شبکه شوند. استفاده از فایروال و روتر در شبکه بیسیم همانند شبکه های سیم کشی شده نیز توصیه می شود.

جداسازی توسط مکانیزم های جداسازی:

بهدلیل اینکه معمولاً AP ها رابط بین شبکه بیسیم و سیم کشی شده هستند، ایستگاه های کاری موجود در دو طرف این AP ها معمولاً در یک Broadcast Domain می باشند. با این توضیحات، هکر شبکه بیسیم میتواند با استفاده از روشهای موجود روی شبکه های سیم کشی شده مانند ARP cache Poisoning نسبت به اجرای Exploit روی ترافیک Broadcast اقدام نماید. همچنین هکر می تواند ایستگاه های بیسیم دیگری را که به AP متصل هستند را مورد حمله قرار دهد. این اتفاق در مورد ایستگاه های کاری موجود روی شبکه سیم کشی شده که به شبکه بیسیم متصل هستند روی خواهد داد.

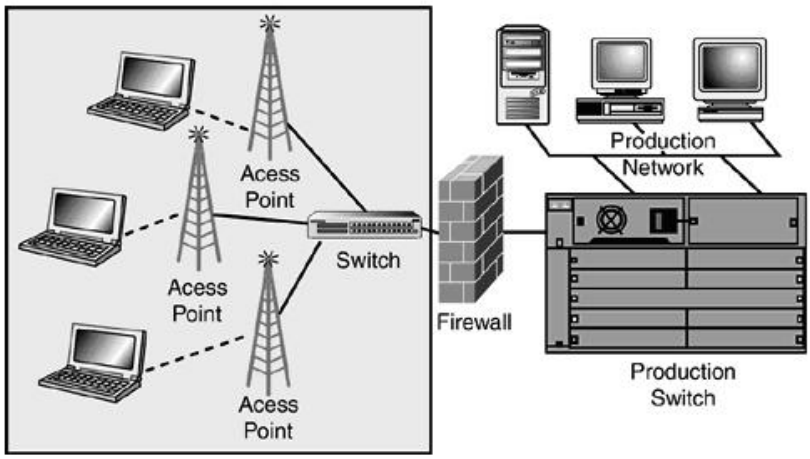
به دلیل آسیب پذیری های زیادی که در شبکه های بیسیم و با توجه به نحوه پیاده سازی این شبکه ها، این فکر در ذهن ایجاد می شود که شبکه های سیم کشی ایزوله شده از این شبکه ها امن تر می باشند.

همانطوری که در شکل زیر مشاهده میشود، طراحی ساده ولی با یک نکته اصلی و آن اینکه، در این طرح، دسترسی مستقیم لایه 2 و اتصال به منابع شبکه برای تمامی ایستگاه های کاری بیسیم میسر می شود و این امر مشکلات امنیتی را در پی خواهد داشت. حداقل پیشنهادی که برای امنیت در این طرح مورد نظر می باشد، جدا سازی و ایزوله کردن شبکه بیسیم از شبکه داخلی در VLAN جداگانه و با قرار دادن مکانیزم های لایه 3 در شبکه می باشد.



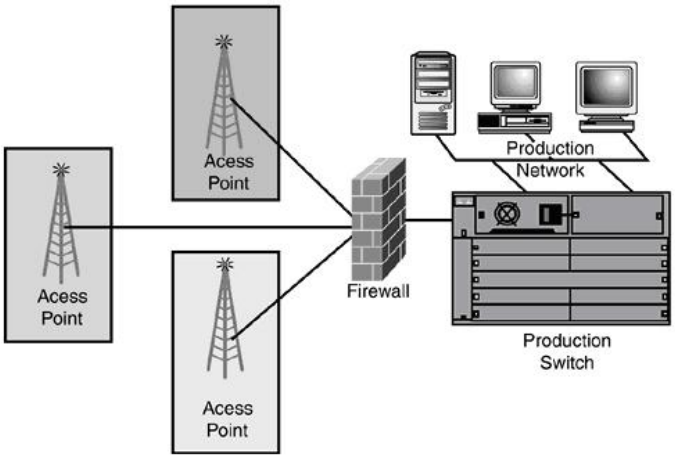
طراحی بهتر شبکه با درک مفهوم Wireless-DMZ که در شکل زیر نشان داده شده است انجام خواهد شد. با قرار دادن APها در ناحیه امنیت خاص، پیاده سازی کنترل های لایه3 و کنترل های دسترسی مانند پیاده سازی فایروال می توان به امنیت بالاتری دست یافت.

به طور مثال اگر تمام AP ها به یک سوئیچ (یا دو سوئیچ برای افزونگی(Redundancy)) متصل و سپس سوئیچ به فایروال متصل شود، ما یک نقطه کنترلی یا Layer 3+ بین شبکه داخلی و شبکه AP خواهیم داشت.



با توجه به شبکه فوق، اگر هکری ایستگاه های بیسیم و یا حتی AP ها را تحت کنترل خود در آورد، محدود به شبکه خود (شبکه خارج از فایروال) و به سرویسهایی که در فایروال باز گذاشته شده می باشد. بعلاوه هرگونه ترافیک ورودی و خروجی در فایروال ثبت شده و بدین ترتیب ما رد ممیزی حتی و با بررسی این گزارشات شانس بیشتری برای جلوگیری از حملات خواهیم داشت.

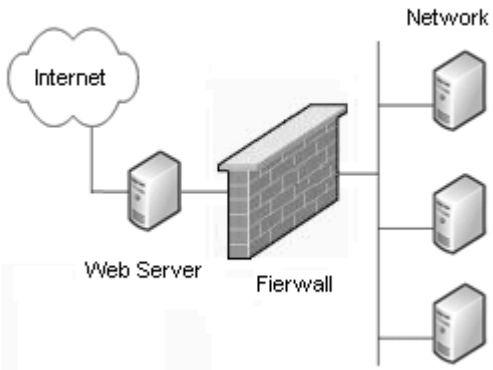
و اگر AP ها دارای رده امنیت مختلفی باشند می توان هرکدام را در ناحیه امنیتی خود قرار داده و به فایروال مربوطه با چند interface مطابق شکل زیر متصل نمود. با این طرح منابع هرکدام از شبکه های بیسیم در مقابل شبکه های دیگر محافظت می شود.



طراحی فوق برای محیط های آموزشی که استاد و دانشجویان دارای دسترسی های مختلفی به منابع شبکه می باشند مناسب است.

در قسمت بعد طراحی های دیگر و همچنین انواع رمزنگاری روی شبکه های بیسیم و محکم سازی AP ها را بررسی خواهیم کرد.

با کاربرد فایروال آشنا شویم



در این حالت وب سرور بیرون فایروال قرار دارد و امنیت شبکه بطور کامل توسط فایروال کنترل می شود و وجود وب سرور خطری برای شبکه ندارد.

Firewall دستگاهی است در درون شبکه یک شرکت قرار می گیرد و شبکه را از محیط اینترنت و یا دسترسی های بیرونی ایزوله می کند. فایروال با کنترل دسترسی ها به شبکه، به برخی از درخواستها اجازه ورود به شبکه را داده و مانع ورود برخی دیگر درخواستها می شود. معمولاً برنامه ریزی و سیاستگذاری یک فایروال اینگونه است که کلیه دسترسی ها از بیرون به داخل شبکه شرکت از محیطی عبور می کند که کاملاً در حال کنترل و مونیتور کردن است. این موضوع دقیقاً همانند قسمتی است که شما هنگام ورود به یک ساختمان مهم باید از آن عبور کنید که در آن نیروهای امنیتی شما را بازرسی بدنی می کنند و یا شما را از X-Ray عبور می دهند.

اما از آنجایی که فایروالها اغلب به دلیل انجام تنظیمات نادرست خوب عمل نمی کنند، امروزه بسیاری از مدیران شرکت ها به آنها اعتماد ندارند و عملکرد مثبت آنها به هنگام بروز خطر یا حمله یک هکر را پنجاه پنجاه می دانند. بعنوان مثال همانطور که می دانید یکی از مهمترین منابع حملات شبکه ای از ناحیه کارکنان ناراضی شرکت ها است، این در حالی است که فایروال ها معمولاً طوری تنظیم می شوند که مراقبت شبکه را از تهدیدهای بیرونی به عهده بگیرند.

کاربرد پراکسی در امنیت شبکه

HTTP Proxy

این پراکسی بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به World Wide Web ایجاد شده، نظارت می کند. این پراکسی برای مراقبت از کلاینت های وب شما و سایر برنامه ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می کند. بعضی از قابلیتهای آن اینها هستند:

- برداشتن اطلاعات اتصال کلاینت: این پراکسی می تواند آن قسمت از دیتای header را که نسخه سیستم عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟

- تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب: در بسیاری از حمله ها، هکرها بسته های تغییرشکل داده شده را ارسال می کنند که باعث دستکاری عناصر دیگر صفحه وب می شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی کردند، وارد می شوند. پراکسی HTTP این اطلاعات بی معنی را نمی پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می کند.

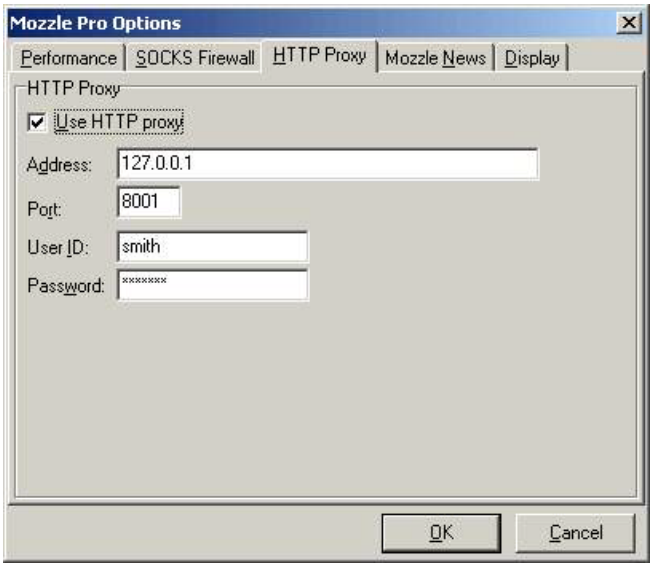
- فیلترکردن محتوای از نوع MIME : الگوهای MIME به مرورگر وب کمک می کنند تا بداند چگونه محتوا را تفسیر کند تا با یک تصویرگرافیکی بصورت یک گرافیک رفتار شود، یا .wav فایل بعنوان صوت پخش شود، متن نمایش داده شود و غیره. بسیاری حمله های وب بسته هایی هستند که در مورد الگوی MIME خود دروغ می گویند یا الگوی آن را مشخص نمی کنند. پراکسی HTTP این فعالیت مشکوک را تشخیص می دهد و چنین ترافیک دیتایی را متوقف می کند.

- فیلترکردن کنترلهای Java و ActiveX: برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند بصورت خودکار آن صفحه را صفحه خانگی مرورگر آن فرد نماید). پراکسی می تواند این برنامه ها را مسدود کند و به این ترتیب جلوی بسیاری از حمله ها را بگیرد.

- برداشتن کوکی ها: پراکسی HTTP می تواند جلوی ورود تمام کوکی ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.

- برداشتن Headerهای ناشناس: پراکسی HTTP ، از headerهای HTTP که از استاندارد پیروی نمی کنند، ممانعت بعمل می آورد. یعنی که، بجای مجبور بودن به تشخیص حمله های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می ریزد. این رویکرد ساده از شما در مقابل تکنیک های حمله های ناشناس دفاع می کند.

- فیلترکردن محتوا: دادگاه ها مقررکرده اند که تمام کارمندان حق برخورداری از یک محیط کاری غیر خصمانه را دارند. بعضی عملیات تجاری نشان می دهد که بعضی موارد روی وب جایگاهی در شبکه های شرکت ها ندارند. پراکسی HTTP سیاست امنیتی شرکت شما را وادار می کند که توجه کند چه محتویاتی مورد پذیرش در محیط کاریتان است و چه هنگام استفاده نامناسب از اینترنت در یک محیط کاری باعث کاستن از بازده کاری می شود. بعلاوه، پراکسی HTTP می تواند سستی ناشی از فضای سایبر را کم کند. گروه های مشخصی از وب سایتها که باعث کم کردن تمرکز کارمندان از کارشان می شود، می توانند غیرقابل دسترس شوند.



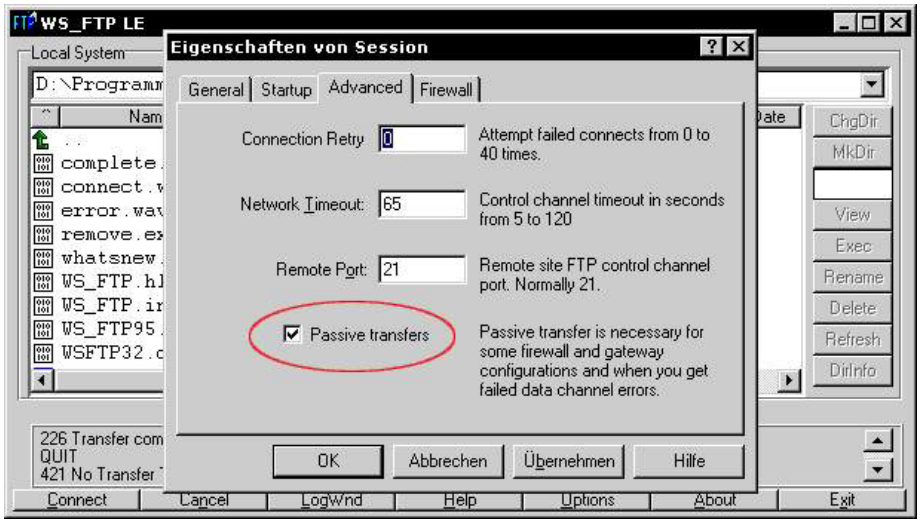
FTP Proxy

بسیاری از سازمان ها از اینترنت برای انتقال فایل های دیتای بزرگ از جایی به جایی دیگر استفاده می کنند. در حالیکه فایل های کوچک تر می توانند بعنوان پیوست های ایمیل منتقل شوند، فایل های بزرگ تر توسط FTP (File Transfer Protocol) فرستاده می شوند. بدلیل اینکه سرورهای FTP فضایی را برای ذخیره فایل ها آماده می کنند، هکرها علاقه زیادی به دسترسی به این سرورها دارند. پراکسی FTP معمولاً این امکانات را دارد:

- محدودکردن ارتباطات از بیرون به «فقط خواندنی»: این عمل به شما اجازه می دهد که فایل ها را در دسترس عموم قرار دهید، بدون اینکه توانایی نوشتن فایل روی سرورتان را بدهید.
- محدود کردن ارتباطات به بیرون به «فقط خواندنی»: این عمل از نوشتن فایل های محرمانه شرکت به سرورهای FTP خارج از شبکه داخلی توسط کاربران جلوگیری می کند.

- مشخص کردن زمانی ثانیه های انقضای زمانی: این عمل به سرور شما اجازه می دهد که قبل از حالت تعلیق و یا Idle request ارتباط را قطع کند.

- ازکارانداختن فرمان FTP SITE : این از حمله هایی جلوگیری می کند که طی آن هکر فضایی از سرور شما را تسخیر می کند تا با استفاده از سیستم شما حمله بعدی خودش را پایه ریزی می کند.



DNS Proxy

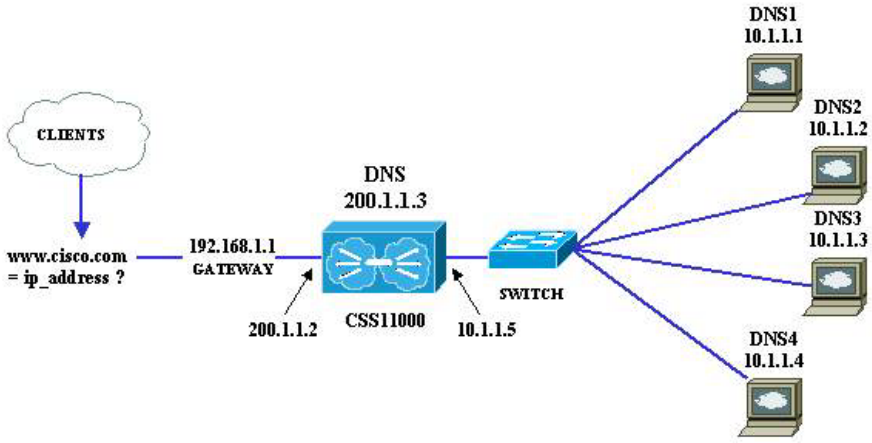
DNS (Domain Name Server) شاید به اندازه HTTP یـا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانندhttp://www.ircert.com در مرورگر وب خود تایپ کنید و وارد این سایت شوید – بدون توجه به اینکه از کجای دنیا به اینترنت متصل شده اید. بمنظور تعیین موقعیت و نمایش منابعی که شما از اینترنت درخواست می کنید، DNS نام های دامنه هایی را که می

توانیم براحتی بخاطر بسپاریم به آدرس IP هایی که کامپیوترها قادر به درک آن هستند، تبدیل می کند. در اصل این یک پایگاه داده است که در تمام اینترنت توزیع شده است و توسط نام دامنه ها فهرست شده است.

بهرحال، این حقیقت که این سرورها در تمام دنیا با مشغولیت زیاد در حال پاسخ دادن به تقاضاها برای صفحات وب هستند، به هکرها امکان تعامل و ارسال دیتا به این سرورها را برای درگیرکردن آنها می دهد. حمله های برپایه DNS هنوز خیلی شناخته شده نیستند، زیرا به سطحی از پیچیدگی فنی نیاز دارند که بیشتر هکرها نمی توانند به آن برسند. بهرحال، بعضی تکنیک های هک که میشناسیم باعث می شوند هکرها کنترل کامل را بدست گیرند. بعضی قابلیت های پراکسی DNS می تواند موارد زیر باشد:

- تضمین انطباق پروتکلی: یک کلاس تکنیکی بالای اکسپلویت می تواند لایه Transport را که تقاضاها و پاسخ های DNS را انتقال می دهد به یک ابزار خطرناک تبدیل کند. این نوع از حمله ها بسته هایی تغییرشکل داده شده بمنظور انتقال کد آسیب رسان ایجاد می کنند. پراکسی DNS، headerهای بسته های DNS را بررسی می کند و بسته هایی را که بصورت ناصحیح ساخته شده اند دور می ریزد و به این ترتیب جلوی بسیاری از انواع سوء استفاده را می گیرد.

- فیلترکردن محتوای headerها بصورت گزینشی: DNS در سال ۱۹۸۴ ایجاد شده و از آن موقع بهبود یافته است. بعضی از حمله های DNS بر ویژگی هایی تکیه می کنند که هنوز تایید نشده اند. پراکسی DNS می تواند محتوای header تقاضاهای DNS را بررسی کند و تقاضاهایی را که کلاس، نوع یا طول header غیرعادی دارند، مسدود کند.



نتیجه گیری

با مطالعه این مجموعه مقالات، تا حدی با پراکسی ها آشنا شدیم. پراکسی تمام ابزار امنیت نیست، اما یک ابزار عالیست، هنگامی که با سایر امنیت سنج ها! مانند ضدویروس های استاندارد، نرم افزارهای امنیتی سرور و سیستم های امنیتی فیزیکی بکار برده شود.