کاربرد Proxy در شبکه

منبع : گروه امداد امنیت کامپیوتری ایران www.ircert.com

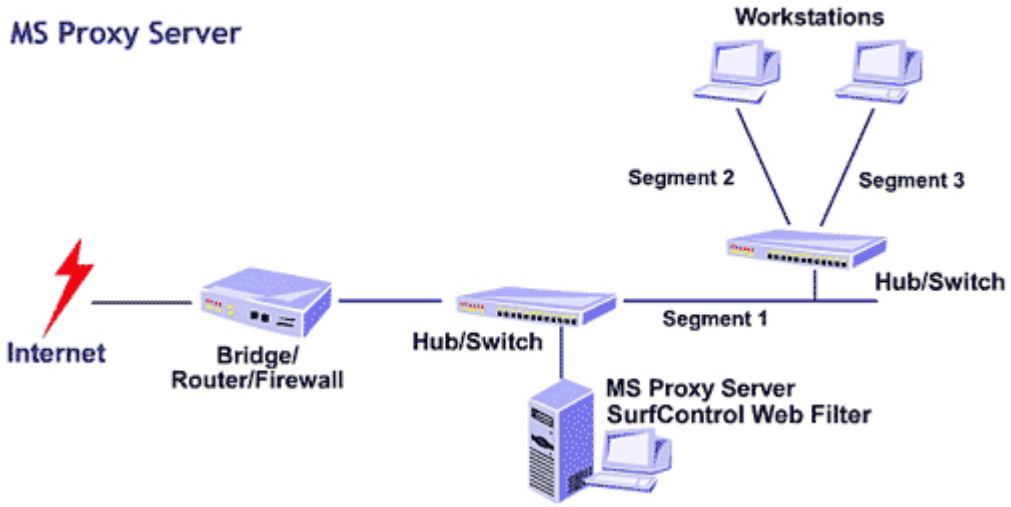
بعد از آشنایی با پراکسی در مقاله «پراکسی سرور» در این مقاله به این مطلب می پردازیم که از دیدگاه امنیتی پراکسی چیست و چه چیزی نیست، از چه نوع حملاتی جلوگیری می کند و به مشخصات بعضی انواع پراکسی پرداخته می شود. البته قبل از پرداختن به پراکسی بعنوان ابزار امنیتی، بیشتر با فیلترها آشنا خواهیم شد.

پراکسی چیست؟

در دنیای امنیت شبکه، افراد از عبارت «پراکسی» برای خیلی چیزها استفاده می کنند. اما عموماً، پراکسی ابزار است که بسته های دیتای اینترنتی را در مسیر دریافت می کند، آن دیتا را می سنجد و عملیاتی برای سیستم مقصد آن دیتا انجام می دهد. در اینجا از پراکسی به معنی پروسه ای یاد می شود که در راه ترافیک شبکه ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار می گیرد و آن را می سنجد تا ببیند با سیاست های امنیتی شما مطابقت دارد و سپس مشخص می کند که آیا به آن اجازه عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور مورد نظر ارسال و بسته های ردشده دور ریخته می شوند.

پراکسی چه چیزی نیست؟

پراکسی ها بعضی اوقات با دو نوع فایروال اشتباه می شوند «Packet filter و Stateful packet filter» که البته هر کدام از روش ها مزایا و معایبی دارد، زیرا همیشه یک مصالحه بین کارایی و امنیت وجود دارد.



پراکسی با Packet filter تفاوت دارد

ابتدایی ترین روش صدور اجازه عبور به ترافیک بر اساس TCP/IP این نوع فیلتر بود. این نوع فیلتر بین دو یا بیشتر رابط شبکه قرار می گیرد و اطلاعات آدرس را در IP header ترافیک دیتایی که بین آنها عبور می کند، پیمایش می کند. اطلاعاتی که این نوع فیلتر ارزیابی می کند عموماً شامل آدرس و پورت منبع و مقصد می شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و بر اساس قوانین ایجاد شده توسط مدیر شبکه بسته را می پذیرد یا نمی پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می شود. و عیب اصلی ان این است که هرگز آنچه را که در بسته وجود دارد نمی بیند و به محتوای آسیب رسان اجازه عبور از فایروال را می دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می کند و وضعیت (State) ارتباط را دنبال نمی کند.

پراکسی با Stateful packet filter تفاوت دارد

این فیلتر اعمال فیلتر نوع قبل را انجام می دهد، بعلاوه اینکه بررسی می کند کدام کامپیوتر در حال ارسال چه دیتایی است و چه نوع دیتایی باید بیاید. این اطلاعات بعنوان وضعیت (State) شناخته می شود.

پروتکل ارتباطی TCP/IP به ترتیبی از ارتباط برای برقراری یک مکالمه بین کامپیوترها نیاز دارد. در آغاز یک ارتباط TCP/IP عادی، کامپیوتر A سعی می کند با ارسال یک بسته SYN (synchronize) به کامپیوتر B ارتباط را برقرار کند. کامپیوتر B در جواب یک بسته Acknowledgement SYN/ACK)) برمی گرداند، و کامپیوتر A یک ACK به کامپیوتر B می فرستد و به این ترتیب ارتباط برقرار می شود. TCP اجازه وضعیتهای دیگر، مثلاً FIN (finish) برای نشان دادن آخرین بسته در یک ارتباط را نیز می دهد.

هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما می پردازند. یک روش معمول ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، می فرستند. معمولاً، کامپیوتر دریافت کننده بیاید پیامی بفرستد و بگوید "I don't understand" . به این ترتیب، به هکر نشان می دهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ می تواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط TCP/IP را می فهمد و می تواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ـــ آنچه که یک فیلتر packet ردگیری نمی کند و نمی تواند انجام دهد. فیلترهای Stateful packet می توانند در همان لحظه قواعدی را مبنی بر اینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکم تر است. این امنیت محکم تر، بهرحال، تا حدی باعث کاستن از کارایی می شود. نگاهداری لیست قواعد ارتباط بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

پراکسی ها یا Application Gateways

Application Gateways که عموماً پراکسی نامیده می شود، پیشرفته ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال ها هستند. پراکسی بین کلاینت و سرور قرار می گیرد و تمام جوانب گفتگوی بین آنها را برای تایید تبعیت از قوانین برقرار شده، می سنجد. پراکسی بار واقعی تمام بسته های عبوری بین سرور و کلاینت را می سنجد، و می تواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط headerها را می سنجند، در حالیکه پراکسی ها محتوای بسته را با مسدود کردن کدهای آسیب رسان همچون فایلهای اجرایی، اپلت های جاوا، ActiveX و ... غربال می کنند.

پراکسی ها همچنین محتوا را برای اطمینان از اینکه با استانداردهای پروتکل مطابقت دارند، می سنجند. برای مثال، بعضی اَشکال حمله کامپیوتری شامل ارسال متاکاراکترها برای فریفتن سیستم قربانی است؛ حمله های دیگر شامل تحت تاثیر قراردادن سیستم با دیتای بسیار زیاد است. پراکسی ها می توانند کاراکترهای غیرقانونی یا رشته های خیلی طولانی را مشخص و مسدود کنند. بعلاوه، پراکسی ها تمام اعمال فیلترهای ذکرشده را انجام می دهند. بدلیل تمام این مزیتها، پراکسی ها بعنوان یکی از امن ترین روشهای عبور ترافیک شناخته می شوند. آنها در پردازش ترافیک از فایروالها کندتر هستند زیرا کل بسته ها را پیمایش می کنند. بهرحال «کندتر» بودن یک عبارت نسبی است.

آیا واقعاً کند است؟ کارایی پراکسی بمراتب سریعتر از کارایی اتصال اینترنت کاربران خانگی و سازمانهاست. معمولاً خود اتصال اینترنت گلوگاه سرعت هر شبکه ای است. پراکسی ها باعث کندی سرعت ترافیک در تست های آزمایشگاهی می شوند اما باعث کندی سرعت دریافت کاربران نمی شوند. در شماره بعد بیشتر به پراکسی خواهیم پرداخت.

در مقایسه فایروال‌ها، ما مفهومی از پراکسی ارائه می‌دهیم و پراکسی را از فیلترکننده بسته‌ها متمایز می‌کنیم. با پیش‌زمینه‌ای که از پراکسی در شماره قبل بیان کردیم، می‌توانیم در اینجا مزایای پراکسی‌ها بعنوان ابزاری برای امنیت را لیست کنیم:

- با مسدود کردن روش‌های معمول مورد استفاده در حمله‌ها، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با پنهان کردن جزئیات سرورهای شبکه شما از اینترنت عمومی، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با جلوگیری از ورود محتویات ناخواسته و نامناسب به شبکه شما، استفاده از پهنای باند شبکه را بهبود می‌بخشند.
- با ممانعت از یک هکر برای استفاده از شبکه شما بعنوان نقطه شروعی برای حمله دیگر، از میزان این نوع مشارکت می‌کاهند.
- با فراهم‌آوردن ابزار و پیش‌فرض‌هایی برای مدیر شبکه شما که می‌توانند بطور گسترده‌ای استفاده شوند، می‌توانند مدیریت شبکه شما را آسان سازند.

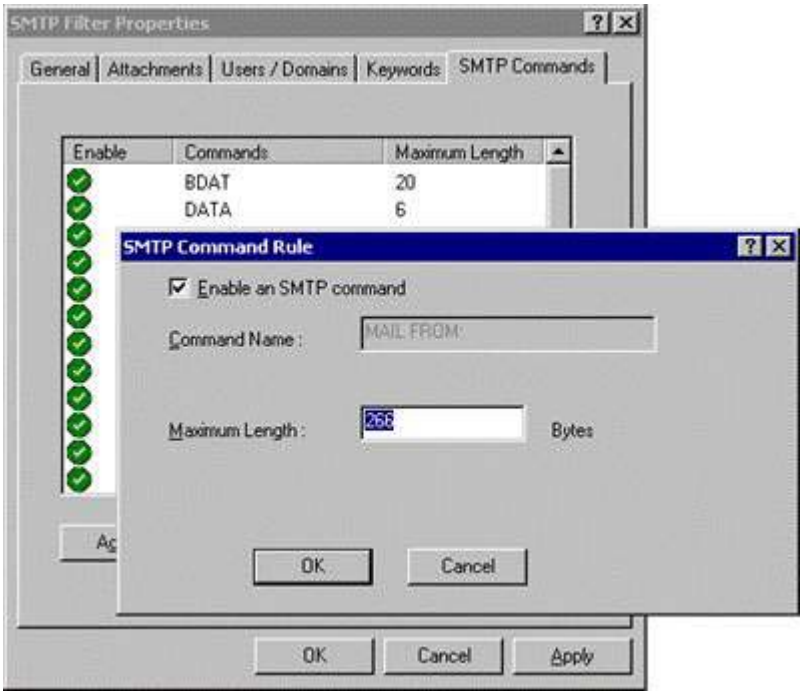
بطور مختصر می‌توان این مزایا را اینگونه بیان کرد؛ پراکسی‌ها به شما کمک می‌کنند که شبکه‌تان را با امنیت بیشتر، موثرتر و اقتصادی‌تر مورد استفاده قرار دهید. بهرحال در ارزیابی یک فایروال، این مزایا به فواید اساسی تبدیل می‌شوند که توجه جدی را می‌طلبند.

برخی انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند.

البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد. در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

- SMTP Proxy
- HTTP Proxy
- FTP Proxy
- DNS Proxy



SMTP Proxy

پراکسی SMTP (Simple Mail Transport Protocol) محتویات ایمیل‌های وارد شونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از تواناییهای آن اینها هستند:

- **مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام**: این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.
- **مشخص کردن بزرگترین اندازه پیام:** این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.
- **اجازه دادن به کاراکترهای مشخص در آدرسهای ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده است:** چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرسها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.
- **فیلترکردن محتوا برای جلوگیری از انواعی محتویات اجرایی:** معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.
- **فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول\مردود:** هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.
- **فیلترکردن Headerهای ایمیل:** Headerها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات Header برای حمله به سرورهای ایمیل یافته‌اند. پراکسی مطمئن می‌شود که Headerها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده headerهای تغییرشکل‌داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.
- **تغییردادن یا پنهان‌کردن نامهای دامنه و IDهای پیام‌ها:** ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای header هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

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.

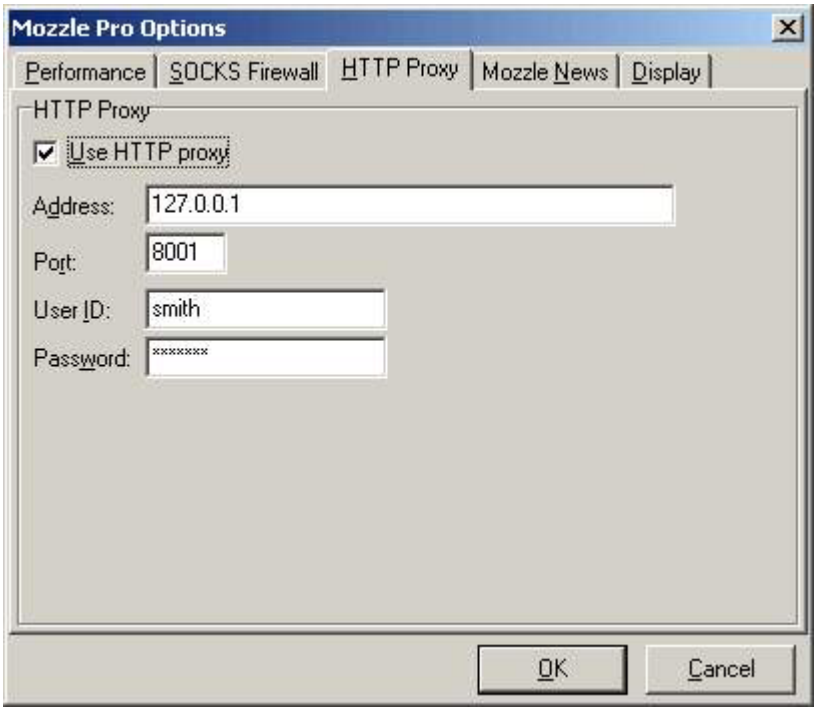
- **فیلترکردن کنترلهای Java و ActiveX**: برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند بصورت خودکار آن صفحه را صفحه خانگی مرورگر آن فرد 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

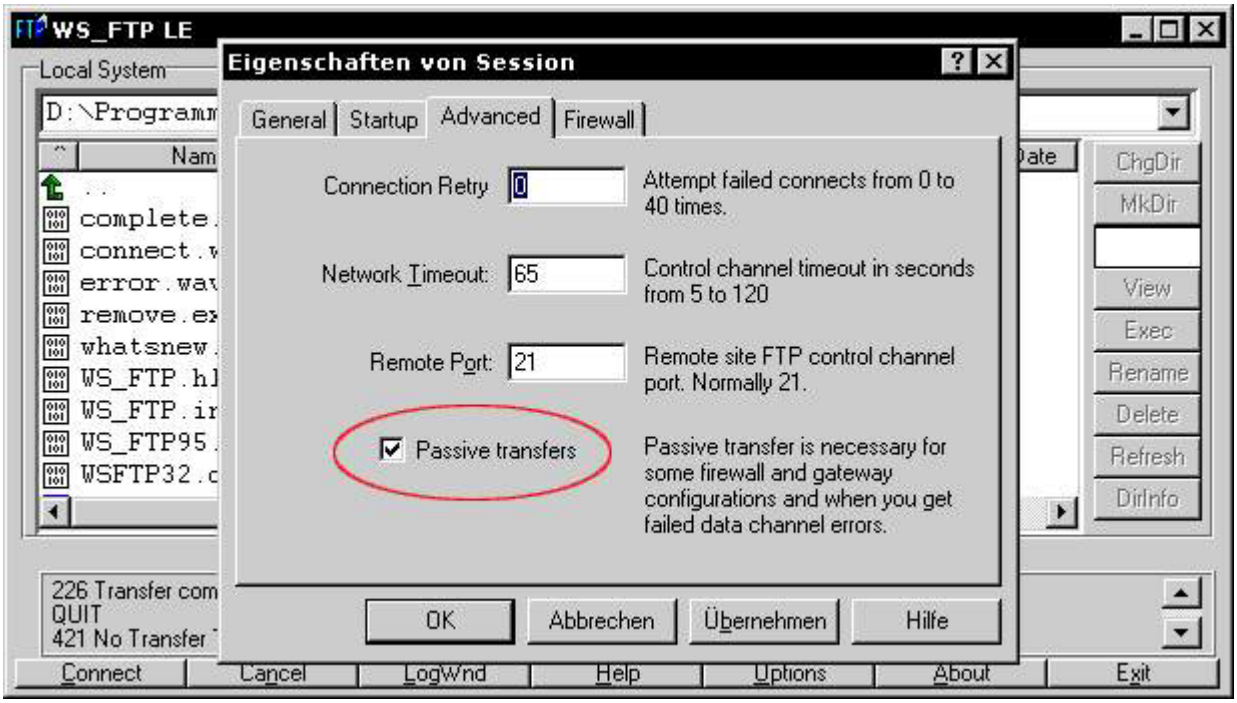
فضای سایبر را کم کند. گروه های مشخصی از وب سایتها که باعث کم کردن تمرکز کارمندان از کارشان می شود، می توانند غیرقابل دسترس شوند.



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.

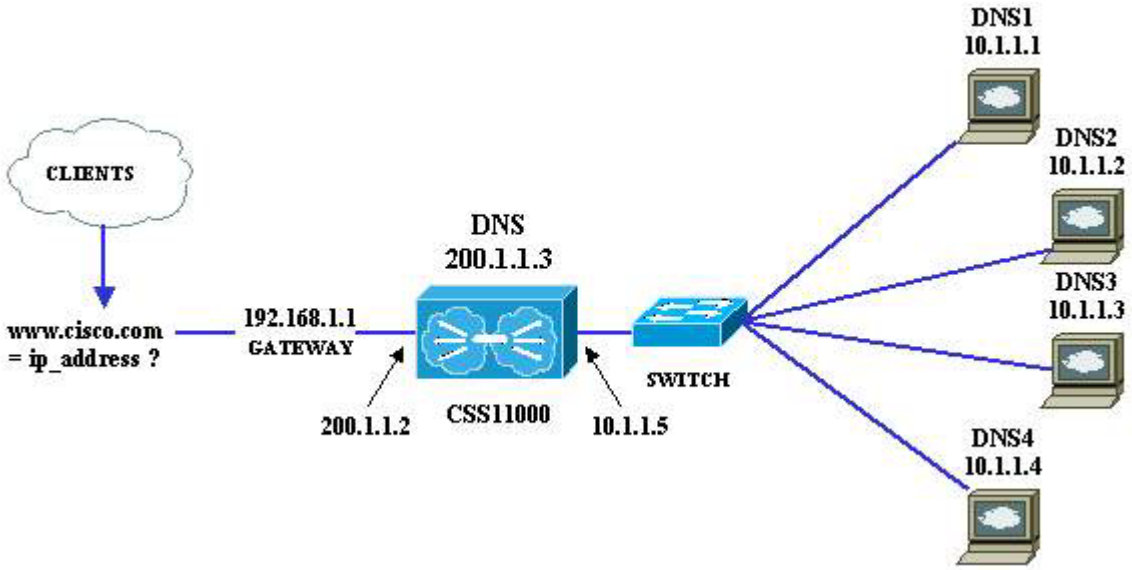


DNS Proxy

DNS (Domain Name Server) شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانند http://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.