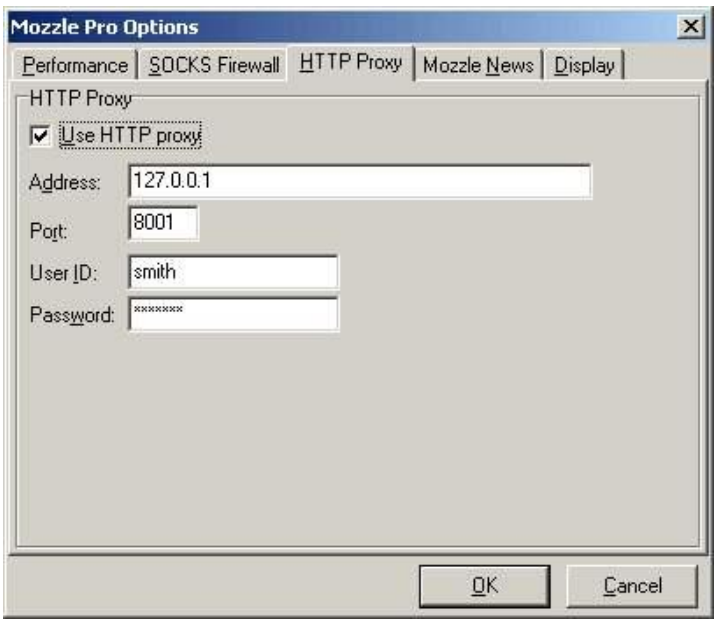
- **برداشتن Headerهای ناشناس:** پراکسی HTTP ، از headerهای HTTP که از استاندارد پیروی نمی کنند، ممانعت بعمل می آورد. یعنی که، بجای مجبور بودن به تشخیص حمله های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می ریزد. این رویکرد ساده از شما در مقابل تکنیک های حمله های ناشناس دفاع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

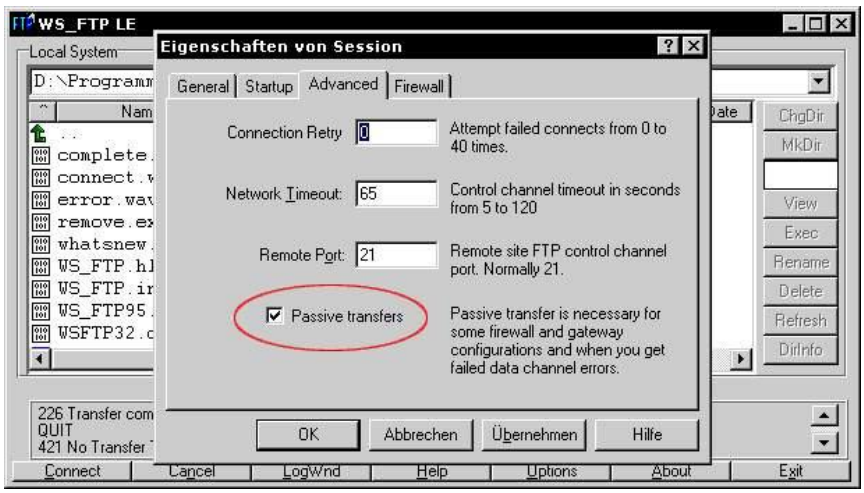


FTP Proxy

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 فضـایی از سرور شـــما را تسخیر می کند تا با استفاده از سیستم شما حمله بعدی خودش را پایه ریزی می کند.



DNS Proxy

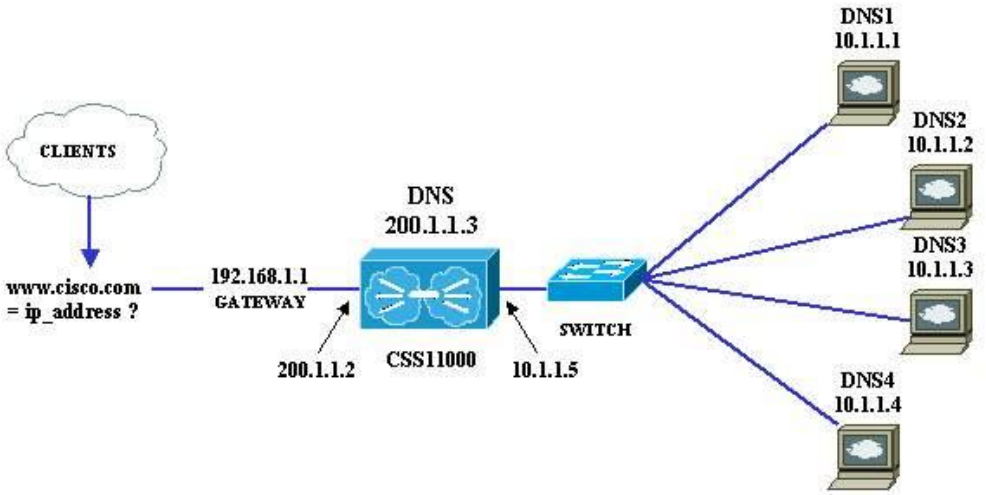
DNS (Domain Name Server) شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانند

http://www.irib.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.

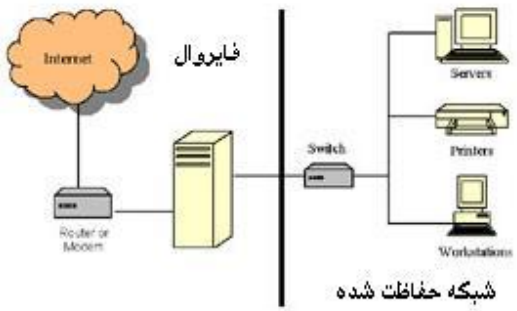


نتیجه گیری

با مطالعه این قسمت ها، 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.

فایروال (قسمت اول)

در صورتی که تاکنون مدت زمان کوتاهی از اینترنت استفاده کرده باشید و یا در یک اداره مشغول بکار هستید که بستر لازم برای دستیابی به اینترنت فراهم شده باشد، احتمالا" واژه " **فایروال** " را شنیده اید. مثلا" اغلب گفته می شود که: " در اداره ما امکان استفاده از این سایت وجود ندارد، چون سایت فوق را از طریق فایروال بسته اند". در صورتیکه از طریق خط تلفن به مرکز ارائه دهنده خدمات اینترنت (ISP) متصل و از اینترنت استفاده می نمائید، امکان استفاده فایروال توسط ISP مربوطه نیز وجود دارد. امروزه در کشورهائی که دارای خطوط ارتباطی با سرعت بالا نظیر DSL و یا مودم های کابلی می باشند، به کاربران خانگی توصیه می گردد که هر یک از فایروال استفاده نموده و با استقرار لایه فوق بین شبکه داخلی در منزل و اینترنت، مسائل ایمنی را رعایت نمایند. بدین ترتیب با استفاده از یک فایروال می توان یک شبکه را در مقابل عملیات غیر مجاز توسط افراد مجاز و عملیات مجاز توسط افراد غیرمجاز حفاظت کرد.



فایروال چیست ؟

فایروال نرم افزار و یا سخت افزاری است که اطلاعات ارسالی از طریق اینترنت به شبکه خصوصی و یا کامپیوتر شخصی را فیلتر می نماید. اطلاعات فیلترشده، فرصت توزیع در شبکه را بدست نخواهند آورد.

فرض کنید، سازمانی دارای ۵۰۰ کارمند باشد. سازمان فوق دارای ده ها کامپیوتر بوده که بر روی هر کدام یک کارت شبکه نصب شده و یک شبکه درون سازمانی (خصوصی) ایجاد شده است. سازمان فوق دارای یک یا چند خط اختصاصی (T۱ و یا T3) برای استفاده از اینترنت است. بدون استفاده از فایروال تمام کامپیوترهای موجود در شبکه داخلی، قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت می باشند. کاربران مربوطه قادر به استفاده از برنامه هائی همچون FTP و یا Telnet بمنظور ارتباط مستقیم با افراد حقوقی و یا حقیقی موجود بر روی اینترنت می باشند. عدم رعایت مسائل ایمنی توسط پرسنل سازمان، می تواند زمینه دستیابی به اطلاعات موجود در شبکه داخلی را برای سارقین و متجاوزان اطلاعاتی اینترنت فراهم نماید.

زمانیکه در سازمان فوق از فایروال استفاده گردد، وضعیت کاملا" تغییر خواهد کرد. سازمان مربوطه می تواند برروی هر یک از خطوط ارتباطی اینترنت یک فایروال نصب نماید.فایروال مجموعه سیاست های امنیتی را پیاده سازی می نماید. مثلا" یکی از قوانین فوق می تواند بصورت زیر باشد:

تمام کامپیوترهای موجود در شبکه مجاز به استفاده از اینترنت می باشند ، فقط یک فرد مجاز به استفاده از سرویس FTP است و سایر پرسنل مجاز به استفاده از سرویس فوق نخواهند بود.

یک سازمان می تواند برای هر یک از سرویس دهندگان خود (وب ، FTP، Telnet و ...) قوانین مشابه تعریف نماید. سازمان قادر به کنترل پرسنل بهمراه لیست سایت های مشاهده خواهد بود. با استفاده از فایروال یک سازمان قادر به کنترل کاربران شبکه خواهد بود.

فایروال ها بمنظور کنترل ترافیک یک شبکه از روش های زیر استفاده می نمایند:

- **فیلتر نمودن بسته های اطلاعاتی** . بسته های اطلاعاتی با استفاده ازتعدادی فیلتر، آنالیز خواهند شد. بسته هائی که از آنالیز فوق سربلند بیرون آیند از فایروال عبور داده شده و بسته ها ئی که شرایط لازم را برای عبور از فایروال را نداشته باشند دور انداخته شده و از فایروال عبور نخواهند کرد.
- **سرویس Proxy** . اطلاعات درخواستی از طریق اینترنت توسط فایروال بازیابی و در ادامه در اختیار درخواست کننده گذاشته خواهد شد. وضعیت فوق در مواردیکه کامپیوتر موجود در شبکه داخلی، قصد ارسال اطلاعاتی را برای خارج از شبکه خصوصی داشته باشند، نیز صدق می کند.

بهینه سازی استفاده از فایروال

فایروال ها را می توان با توجه به اهداف سازمانی بصورت کاملا" سفارشی نصب و پیکربندی کرد. در این راستا امکان اضافه و یا حذف فیلترهای متعدد بر اساس شرایط متفاوت وجود خواهد داشت:

- **آدرس های IP** . هر ماشین بر روی اینترنت دارای یک آدرس منحصر بفرد با نام IP است . IP یک عدد ۳۲ بیتی بوده که بصورت چهار عدد دهدهی که توسط نقطه از هم جدا می گردند نمایش داده می شود (Octet) . در صورتیکه یک آدرس IP خارج از شبکه، فایل های زیادی را از سرویس دهنده می خواند (ترافیک و حجم عملیات سرویس دهنده را افزایش خواهد داد) فایروال می تواند ترافیک از مبداء آدرس فوق و یا به مقصد آدرس فوق را بلاک نماید.
- **اسامی دامنه ها (حوزه)**. تمام سرویس دهندگان بر روی اینترنت دارای اسامی منحصر بفرد با نام " اسامی حوزه" می باشند. یک سازمان می تواند با استفاده از فایروال، دستیابی به سایت هائی را غیرممکن و یا صرفا" امکان استفاده از یک سایت خاص را برای پرسنل خود فراهم نماید.

- **پروتکل ها** . پروتکل نحوه گفتگوی بین سرویس دهنده و سرویس گیرنده را مشخص می نماید . پروتکل های متعدد با توجه به اهداف گوناگون در اینترنت استفاده می گردد. مثلا" http پروتکل وب و Ftp پروتکل مربوط به دریافت و یا ارسال فایل ها است. با استفاده از فایروال می توان، میدان فیلتر نمودن را بر روی پروتکل ها متمرکز کرد. برخی از پروتکل های رایج که می توان بر روی آنها فیلتر اعمال نمود بشرح زیر می باشند:

- Internet Protocol(IP). پروتکل اصلی برای عرضه اطلاعات بر روی اینترنت است.
- Transport Control Protocol (TCP). مسئولیت تقسیم یک بسته اطلاعاتی به بخش های کوچکتر را دارد.
- Hyper Text Transfer Protocol (HTTP). پروتکل فوق برای عرضه اطلاعات در وب است.
- File Transfer Protocol (FTP). پروتکل فوق برای دریافت و ارسال فایل ها استفاده می گردد.
- Protocol User Datagram(UDP) . از پروتکل فوق برای اطلاعاتی که به پاسخ نیاز ندارند استفاده می شود(پخش صوت و تصویر)
- Internet control Message Protocol (ICMP). پروتکل فوق توسط روترها و بمنظور تبادل اطلاعات فی المابین استفاده می شود.
- Simple Mail Transfer Protocol(SMTP). از پروتکل فوق برای ارسال e-mail استفاده می گردد.
- Simple Network Management Protocol (SNMP).از پروتکل فوق بمنظور اخذ اطلاعات از یک کامپیوتر راه دور استفاده میشود

- Telnet . برای اجرای دستورات بر روی یک کامپیوتر از راه دور استفاده می گردد.

- **پورت ها** . هر سرویس دهنده ، خدمات مورد نظر خود را با استفاده از پورت های شماره گذاری شده بر روی اینترنت ارائه می دهد. مثلا" سرویس دهنده وب اغلب از پورت ۸۰ و سرویس دهنده Ftp از پورت ۲۱ استفاده می نماید. یک سازمان ممکن است با استفاده از فایروال امکان دستیابی به پورت ۲۱ را بلاک نماید.

- **کلمات و عبارات خاص** . می توان با استفاده از فایروال کلمات و یا عباراتی را مشخص نمود تا امکان کنترل بسته های اطلاعاتی حاوی کلمات و عبارات فراهم گردد. هر بسته اطلاعاتی که حاوی کلمات مشخص شده باشد توسط فایروال بلاک خواهد شد.

همانگونه که اشاره شد فایروال ها به دو صورت نرم افزاری وسخت افزاری استفاده می گردند.فایروال های نرم افزاری بر روی کامپیوتری نصب می گردند که خط اینترنت به آنها متصل است. کامپیوتر فوق بمنزله یک Gateway رفتار می نماید چون تنها نقطه قابل تماس، بمنظور ارتباط کامپیوتر و اینترنت است. زمانیکه فایروال بصورت سخت افزاری در نظر گرفته شود، تمام بخش فوق بصورت Gateway خواهد بود. امنیت فایروال های سخت افزاری بمراتب بیشتر از فایروال های نرم افزاری است.

تهدیدات

حمله کنندگان به شبکه های کامپیوتری از روش های متعددی استفاده می نمایند.

- **Remote Login** . امکان برقراری ارتباط با کامپیوتر و کنترل آن توسط فرد غیرمجاز است . دامنه عملیات فوق می تواند از مشاهده و دستیابی به برخی از فایل ها تا اجرای برخی برنامه ها بر روی کامپیوتر باشد.

- **Backdoors Application** . برخی از برنامه ها دارای امکانات ویژه ای برای دستیابی از راه دور می باشند. برخی دیگر از برنامه ها دارای اشکالاتی بوده بگونه ای که یک Backdoor را ایجاد و یا امکان دستیابی مخفی را ارائه می دهند. در هر حالت امکان کنترل برنامه فراهم خواهد گردید.
- **hijacking SMTP session** . پروتکل SMTP رایج ترین روش برای ارسال e-mail است. با دستیابی به لیستی از آدرس های e-mail ، یک شخص قادر به ارسال e-mail به هزاران کاربر دیگر خواهد شد.
- **اشکالات سیستم های عامل** . سیستم های عامل نظیر سایر برنامه های کاربردی ممکن است دارای Backdoors باشند.
- **انفجار E-mail** . یک شخص قادر به ارسال صدها و هزاران e-mail مشابه در مقاطع زمانی متفاوت است. با توجه به وضعیت فوق سیستم پست الکترونیکی قادر به دریافت تمام نامه های ارسالی نخواهد بود.
- **ماکرو**. اغلب برنامه های کاربردی این امکان را برای کاربران خود فراهم می نمایند که مجموعه ای از اسکریپت ها را بمنظور انجام عملیات خاصی نوشته و نرم افزار مربوطه آنها را اجراء نماید. اسکریپت های فوق " ماکرو " نامیده می شوند. حمله کنندگان به شبکه های کامپیوتری با آگاهی از واقعیت فوق، اقدام به ایجاد اسکریپت های خاص خود نموده که با توجه به نوع برنامه ممکن است داده ها را حذف و یا باعث از کار افتادن کامپیوتر گردند.

سرویس دهنده Proxy

سرویس دهنده Proxy اغلب با یک فایروال ترکیب می گردد. سرویس دهنده Proxy بمنظور دستیابی به صفحات وب توسط سایر کامپیوترها استفاده می گردد. زمانیکه کامپیوتری درخواست یک صفحه وب را می نماید، صفحه مورد نظر توسط سرویس

دهنده Proxy بازیابی و در ادامه برای کامپیوتر متقاضی ارسال خواهد شد. بدین ترتیب تمام ترافیک (درخواست و پاسخ) بین درخواست کننده یک صفحه وب و پاسخ دهنده از طریق سرویس دهنده Proxy انجام می گیرد.

سرویس دهنده Proxy می تواند کارائی استفاده از اینترنت را افزایش دهد. پس از دستیابی به یک صفحه وب، صفحه فوق بر روی سرویس دهنده Proxy نیز ذخیره (Cache) می گردد. در صورتیکه در آینده قصد استفاده از صفحه فوق را داشته باشید صفحه مورد نظر از روی سرویس دهنده Proxy در اختیار شما گذاشته می شود (الزامی به برقراری ارتباط مجدد و درخواست صفحه مورد نظر نخواهد بود)

فایروال (قسمت دوم)

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند.علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۱- توانایی ثبت و اخطار: ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می شود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲- بازدید حجم بالایی از بسته های اطلاعات: یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر

کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۳- سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه های می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

٤- امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال: اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی: یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

تفاوت در کارایی انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم، انجام می دهند، اما روش انجام کار توسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود. بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

۱- فایروالهای سطح مدار (Circuit-Level): این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲- فایروالهای پروکسی سرور: فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۳- فیلترهای Nosstateful packet : این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد

با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

٤- فیلترهای Stateful Packet : این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانندداعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

٥- فایروالهای شخصی : فایروالهای شخصی، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند. آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات

ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از:

- موقعیت و محل نصب از لحاظ توپولوژیکی : معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.
- قابلیت دسترسی و نواحی امنیتی: اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی وتنظیم فایروال جهت صدور اجازه به کاربران

خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

ü مسیریابی نامتقارن : بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.

ü فایروالهای لایه ای : در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد.معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

Tools security

Ethereal

قسمت اول

Ethereal ابزاری کد-باز و رایگان است، که آن‌را می‌توان در دسته‌ی Snifferها جای داد. این نرم‌افزار با توجه به ویژگی‌هایش، یکی از متداول‌ترین ابزارهای آنالیز ترافیک شبکه است، هرچند که در حال حاضر، با وجود گذشت زمان نسبتاً زیادی از معرفی آن، هنوز در مرحله‌ی تست قرار داشته و در زمان نگارش این مطلب آخرین نگارش آن نگارش 0.10.4 است که از پایگاه www.ethereal.com قابل دریافت است. لازم به ذکر است که سورس این نرم‌افزار را نیز می‌توانید از همین آدرس دریافت کنید.

این نرم‌افزار نیز مانند WinDump، پس از نصب، از کتابخانه‌ی Winpcap برای دریافت اطلاعات بسته‌ها استفاده می‌کند، لذا پیش از نصب Ethereal، آخرین نسخه‌ی نرم‌افزار Winpcap را نصب کنید. همان‌طور که گفته شد این بسته امکان دریافت بسته‌ها و استخراج اطلاعات از آن‌ها را، تحت سیستم‌عامل Windows، فراهم می‌کند.

اگر برای اولین بار است که قصد نصب و کار با این دسته از نرم‌افزارها (Snifferها) را دارید، پیش‌نهاد می‌کنیم ابتدا قسمت اول مقاله‌ی مربوط به WinDump را، که به مقدمه‌یی در باب Snifferها پرداخته است، مطالعه کنید.

Ethereal، به عنوان نمونه‌یی از یک Sniffer، وظیفه‌ی ثبت رخدادها، اطلاعات و بسته‌های رد و بدل شده بر روی لایه‌های شبکه را بر عهده دارد. با ثبت داده‌های در حال انتقال بر روی شبکه و تجزیه‌ی آنها، می‌توان بسته‌های اطلاعاتی مربوط به پروتکل‌های

متفاوت را از یکدیگر تفکیک نمود و ارتباطات مجزا را شناسایی نمود. همان‌گونه که در معرفی این دسته از نرم‌افزارها گفته شد، این قبیل تحلیل‌ها، می‌توانند به شناسایی ارتباطات خطرناک، تلاش‌های پیاپی برای دست‌یابی به منابع شبکه و نفوذ به آن و یا از کار انداختن نرم‌افزارها و سخت‌افزارها فعال بر روی شبکه، بیانجامد. با این وجود از آنجاکه خروجی این دسته از نرم‌افزارها به حدی پیچیده‌اند که کاربران عادی قادر به تحلیل آنها نیستند، لذا این‌گونه نتیجه‌گیری‌ها و تحلیل‌ها عموماً توسط متخصصین شبکه انجام می‌پذیرد.

نرم‌افزار Ethereal بر روی سه بستر اصلی Windows، Linux و Solrais ارایه می‌شود که نسخه‌یی که ما بررسی می‌کنیم، نسخه‌ی تحت Windows آن است.

توانایی‌های این دسته از ابزارها را عموماً می‌توان به بخش‌های زیر تقسیم کرد:

– انواع پروتکل‌ها و انواع رابط‌های شبکه‌یی که توسط ابزار شناسایی شده و تفکیک می‌گردند.

– روش‌ها و قالب‌های ذخیره‌سازی خروجی برداشت و تحلیل اطلاعات شبکه

– امکان بازخوانی اطلاعات ذخیره شده توسط نرم‌افزارهای Sniffer مشابه دیگر

– امکان استفاده از فلیتر برای پروتکل‌های مختلف

– قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متنوع

البته ساده‌گی کار با نرم‌افزار، به عنوان قابلیت‌های ویژه‌ی رابط کاربری، نیز یکی دیگر از قابلیت‌هایی است که اغلب برای کاربران نیمه‌حرفه‌یی و مبتدی اهمیت ویژه‌یی دارد.

قابلیت‌های خاص Ethereal را، با توجه به تقسیم‌بندی فوق، می‌توان به شرح دسته‌بندی نمود :

- شناسایی پروتکل‌ها و رابط‌های شبکه‌ی متنوع

این نرم‌افزار قابلیت شناسایی حدود ۵۰۰ نوع پروتکل مجزا را دارد. تنوع این پروتکل‌ها به این نرم‌افزار قدرتی ویژه بخشیده است.

از باب ارتباطات نیز این نرم‌افزار قابلیت دریافت اطلاعات بسته‌های فعال ارتباطات Ethernet، FDDI، Token-Ring، IEEE 802.11، IP over ATM و رابط‌های loopback را دارد.

- ذخیره‌سازی اطلاعات

Ethereal با ایجاد فایل‌های خروجی قابل ویرایش در قالب‌های lippcap(tcpdump)، Sun snoop، Microsoft Network Monitor و Network Associate Sniffer از نظر ذخیره‌سازی اطلاعات نیز ابزاری قدرت‌مند محسوب می‌شود.

- سازگاری با خروجی نرم‌افزارها و سیستم‌های دیگر

Ethereal قابلیت بازخوانی پرونده‌های اطلاعاتی نرم‌افزارهای مشابه دیگری همچون TCPDump، NAI's Sniffer & Sniffer Pro، NetXray، MS Network Monitor، Novell LANanalyser، Cisco Secure IDS iplog و غیره را دارد.

- فیلترها

این ابزار، با محدود سازی روش دریافت و تحلیل اطلاعات جمع‌آوری شده از بسته‌ها، در بسیاری از حالات امکان استفاده از فیلترهای پرقدرتی را به کاربر

می‌دهد. در عین حال با استفاده از این فیلترهای می‌توان به جست‌وجوی بسته‌ها در میان اطلاعات ذخیره شده نیز پرداخت.

- قابلیت‌ها رابط کاربری

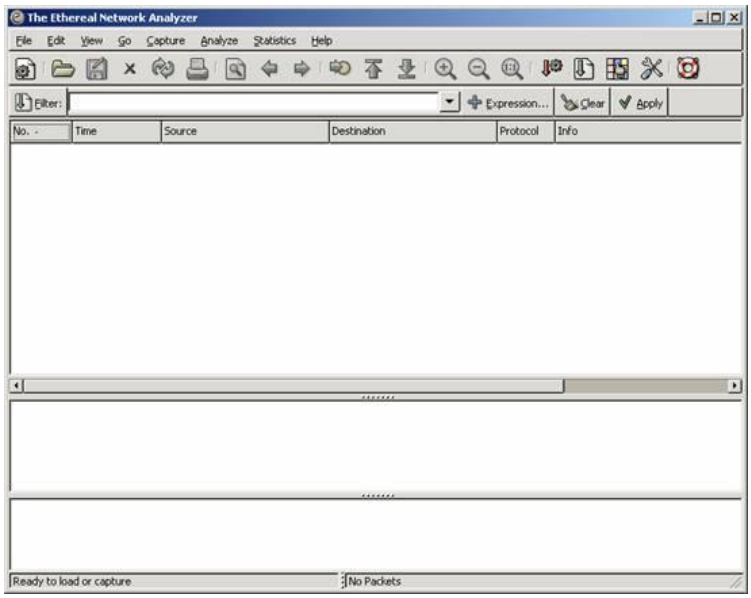
رنگ‌های متنوع برای تغییر روش نمایش اطلاعات بسته به فیلتر انتخاب شده، منوهای متنوع و دیگر امکانات رابط کاربری، که بیشتر در بخش‌ها آتی در حین معرفی چگونگی استفاده از این نرم‌افزار به آنها اشاره خواهیم کرد، به تحلیل و شناسایی بسته‌ها کمک شایانی می‌کند. همان‌طور که ذکر شد، این قابلیت جذابیت ویژه‌یی برای کاربران مبتدی و نیمه‌حرفه‌یی دارد.

در قسمت بعد به بررسی مقدماتی روش‌های استفاده از این نرم‌افزار و ارایه‌ی مثال‌هایی در این باب خواهیم پرداخت

Ethereal قسمت دوم

در قسمت اول، ضمن ارایه‌ی جمع‌بندی در مورد Snifferها، که Ethereal یکی از معروف‌ترین و قدرتمندترین نرم‌افزارهای این دسته از ابزارهاست، به ویژگی‌های برجسته‌ی این نرم‌افزار اشاره کردیم. بررسی قابلیت‌های این نرم‌افزار بر اساس جنبه‌های مختلف و متنوعی صورت گرفت که در مورد این دسته از ابزارها مد نظر قرار می‌گیرد.

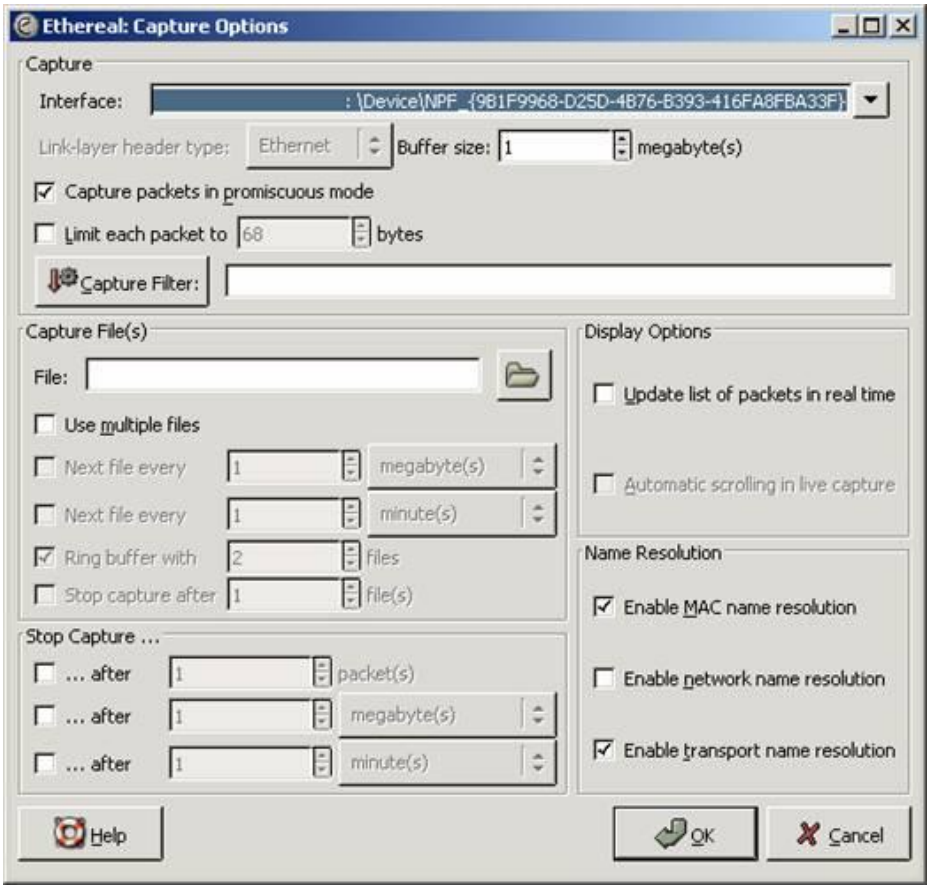
شکل زیر، رابط کاربری این نرم‌افزار پیش از شروع عملیات را نشان می‌دهد:



همان‌گونه که مشاهده می‌کنید، رابط کاربری این نرم‌افزار بسیار شبیه به رابط‌های گرافیکی متداول سیستم‌های عامل Linux است، محیط‌هایی همچون KDE و GNOME.

در منوی فایل، می‌توان خروجی عملیات انجام شده را در قالب‌های مختلف درون فایل ذخیره کرد یا فایل‌های ذخیره شده در قالب‌های مختلف، ایجاد شده توسط نرم‌افزارهای گوناگون، را باز کرد و تحلیل نمود.

شروع عمکرد این نرم‌افزار با استفاده از منوی Capture صورت می‌گیرد. شکل زیر صفحه‌ی مربوط به این منو را نشان می‌دهد:



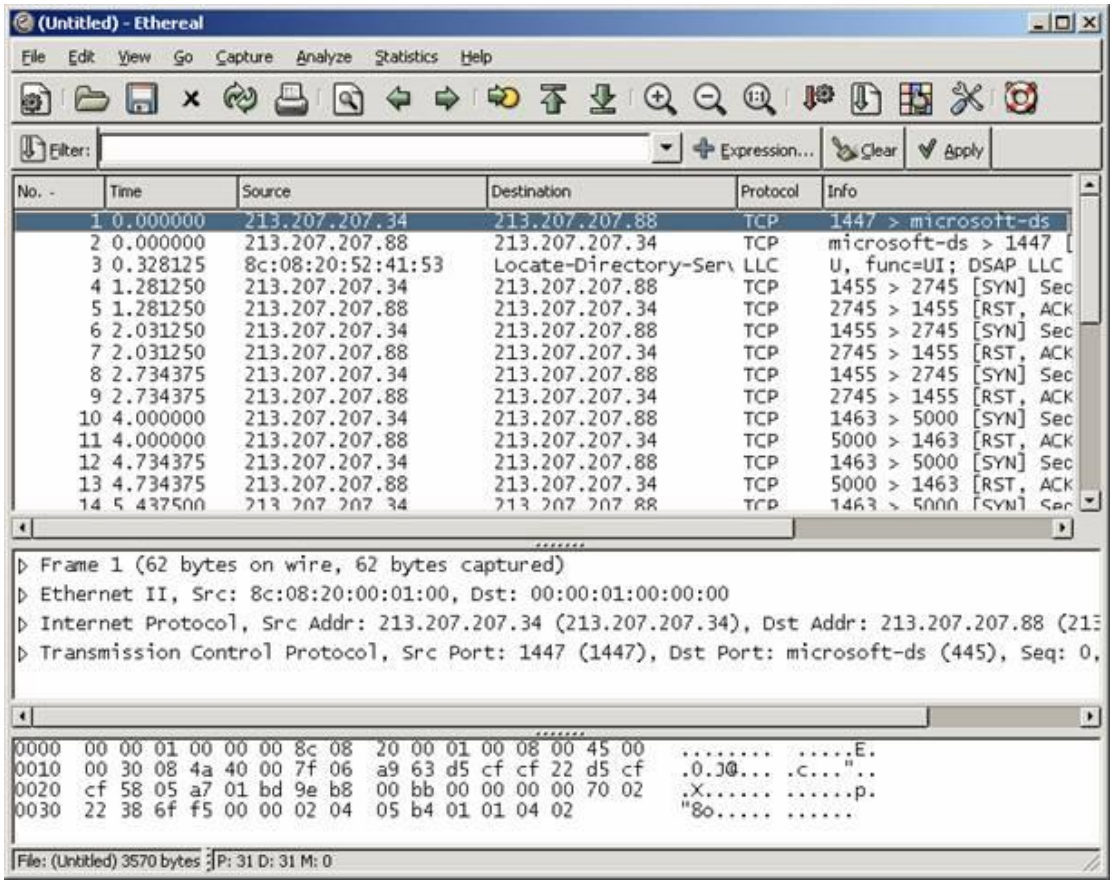
در قسمت بالا، رابط شبکه‌یی که عملیات دریافت بسته‌ها بر روی آن انجام می‌گیرد مشخص می‌شود. این رابط شبکه می‌تواند به ارتباط مودم ما با اینترنت نیز اشاره کند. به عبارت دیگر توسط چنین نرم‌افزارهایی، می‌توان به بررسی وضعیت ارسال و دریافت بسته‌ها و تحلیل آن‌ها در ارتباطات میان مودم‌ها و ارایه‌کننده‌گان سرویس اینترنت نیز پرداخت. خروجی این عملیات می‌تواند اطلاعات مفیدی از حملات احتمالی در حال انجام به سیستم ما را نشان دهد.

قسمت‌های دیگر این صفحه شامل تعیین نام فایلی که بسته‌های دریافت شده در آن‌ها قرار می‌گیرد و همچنین شرایط که در صورت حصول آن‌ها عمل Capture خاتمه می‌پذیرد. سمت راست این صفحه نیز یکی از ویژه‌گی‌های مهم عمل Capture را تعیین می‌کند که تعیین نام مترادف آدرس‌ها در شبکه است. این عمل، ضمن آن‌که اطلاعات جامع و مفیدی را در اختیار ما قرار می‌دهد، عمل دریافت و جمع‌آوری بسته‌ها را کند می‌کند.

شکل زیر، وضعیت پس از آغاز عملیات Capture را نشان می‌دهد. رابط شبکه‌ی مورد استفاده، ارتباط PPP برقرار شده است :

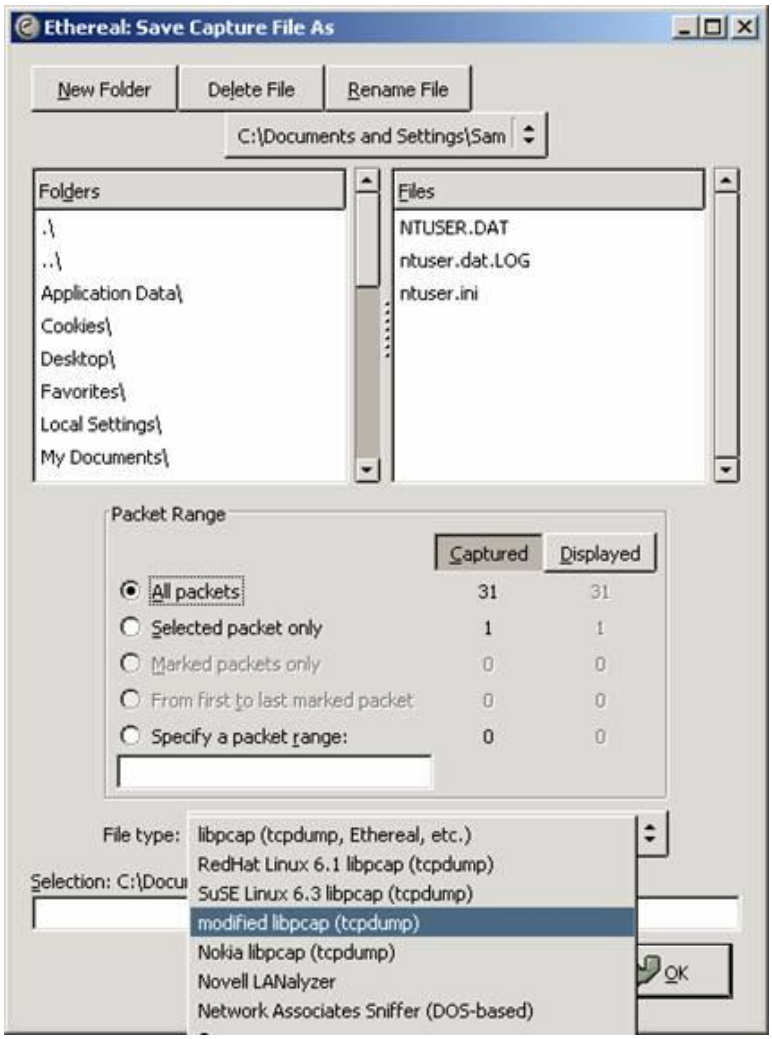
همان‌گونه که در شکل نیز مشخص است، انواع پروتکل‌ها در خروجی مورد نظر دسته‌بندی شده‌اند و در مقابل نام آنها تعداد دریافت شده از آن پروتکل درج می‌شود.

پس از قطع عمل Capture، فهرستی از بسته‌های دریافت شده در پنجره‌ی اصلی نمایش داده می‌شود :



بسته‌های دریافت شده، به ترتیب و بر اساس زمان دریافت مرتب شده‌اند. این فهرست شامل شماره‌ی بسته، زمان دریافت/ارسال آن، آدرس‌های مبدأ و مقصد و نوع بسته نمایش داده شده است. در قسمت پایین‌تر، نوع بسته و اطلاعاتی که از ابتدای بسته استخراج شده‌اند، مانند مبدأ و مقصد، پورت و دیگر اطلاعات درج می‌شود و در قسمت پایین پنجره‌ی اصلی محتوای خام بسته نمایش داده شده است.

خروجی به دست آمده را می‌توان با تعیین قالب مورد نظر برای دسترسی‌های آتی ذخیره نمود. شکل زیر صفحه‌یی که در آن امکان ذخیره سازی پرونده با تعیین قالب مورد نظر وجود دارد را نشان می‌دهد :



شکل بالا، تعدادی از قالب‌های قابل استفاده برای ذخیره‌ی پرونده توسط این نرم‌افزار را نشان می‌دهد. انواع این قالب‌ها در قسمت اول از بررسی این نرم‌افزار معرفی شده‌اند.

در قسمت بعدی از بررسی این نرم‌افزار به روش تعریف فیلترها و چگونه‌گی جستجو و تحلیل در بسته‌های دریافت/ارسال شده، با استفاده از فایل‌های پیشین ذخیره شده، خواهیم پرداخت.

Ethereal

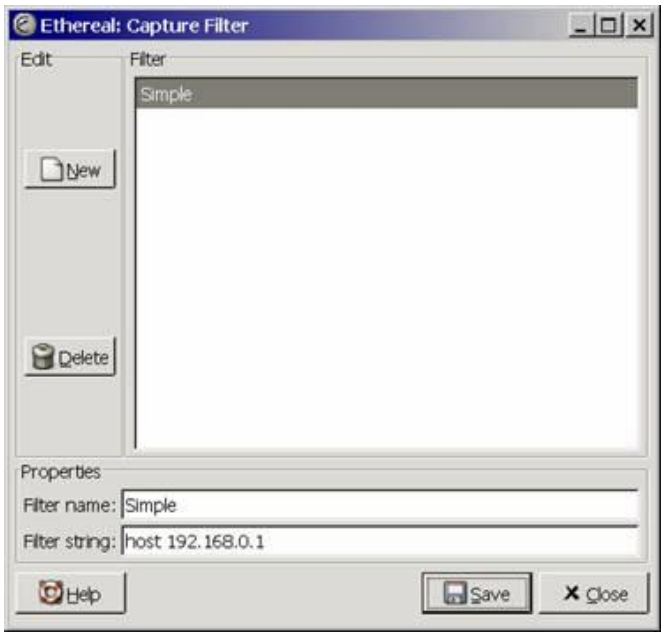
قسمت سوم

در دو قسمت پیشین، ضمن تعریف ابزارهای Sniffer، به معرفی یکی از متداول‌ترین آن‌ها، یعنی Ethereal پرداختیم. در این قسمت، به معرفی امکان استفاده از Filterهای این نرم‌افزار، و چگونه‌گی انجام تحلیل بر اساس خروجی‌های به‌دست آمده می‌پردازیم.

در این نرم‌افزار، عملاً سه نوع فیلتر قابل تعریف است:

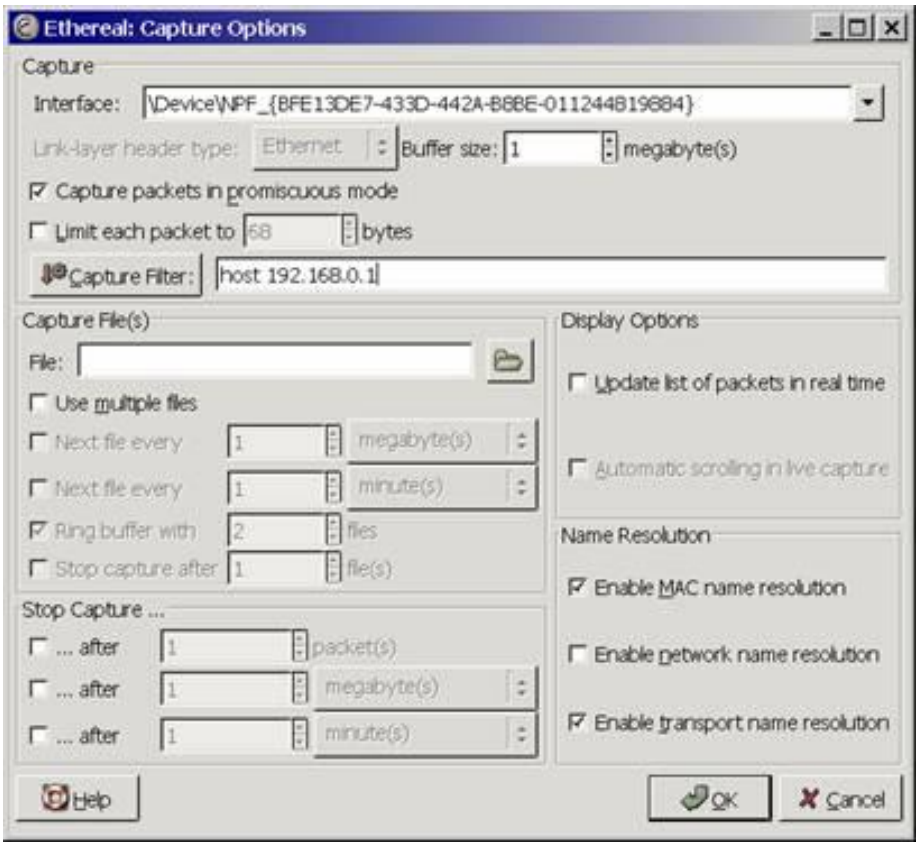
- فیلترهای Capture
- فیلترهای نمایش
- فیلترهای رنگی

برای استفاده از فیلترهای Capture، در منوی Capture، گزینه‌ی Capture Filters را انتخاب می‌کنیم. پنجره‌یی به شکل زیر باز می‌شود:



با انتخاب گزینه‌ی New، فیلتر جدیدی تعریف می‌کنیم.

این نرم‌افزار برای تعریف فیلتر رابط کاربری به‌صورت گرافیکی ندارد، لذا با استفاده از گزینه‌ی Help در پایین همین پنجره، می‌توان از روش تعریف فیلترها به‌صورت متنی آگاه شد. در این مثال، فیلتری به نام Simple تعریف می‌کنیم که توسط آن، Ethereal تنها به دریافت بسته‌هایی مبادرت می‌کند که آدرس فرستنده آن 192.168.0.1 باشد. فیلتر را ذخیره می‌کنیم پنجره را می‌بندیم. اکنون عمل Capture را آغاز می‌کنیم:



همان‌گونه در شکل بالا مشخص است، در قسمت Capture Filters می‌توان فیلتری را تعریف کرد و یا از فیلترهای تعریف شده‌ی پیشین استفاده کرد. پس از انجام عمل Capture، Ethereal تنها بسته‌هایی را دریافت خواهد کرد که آدرس مبدأ آنها 192.168.0.1 باشد.