✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

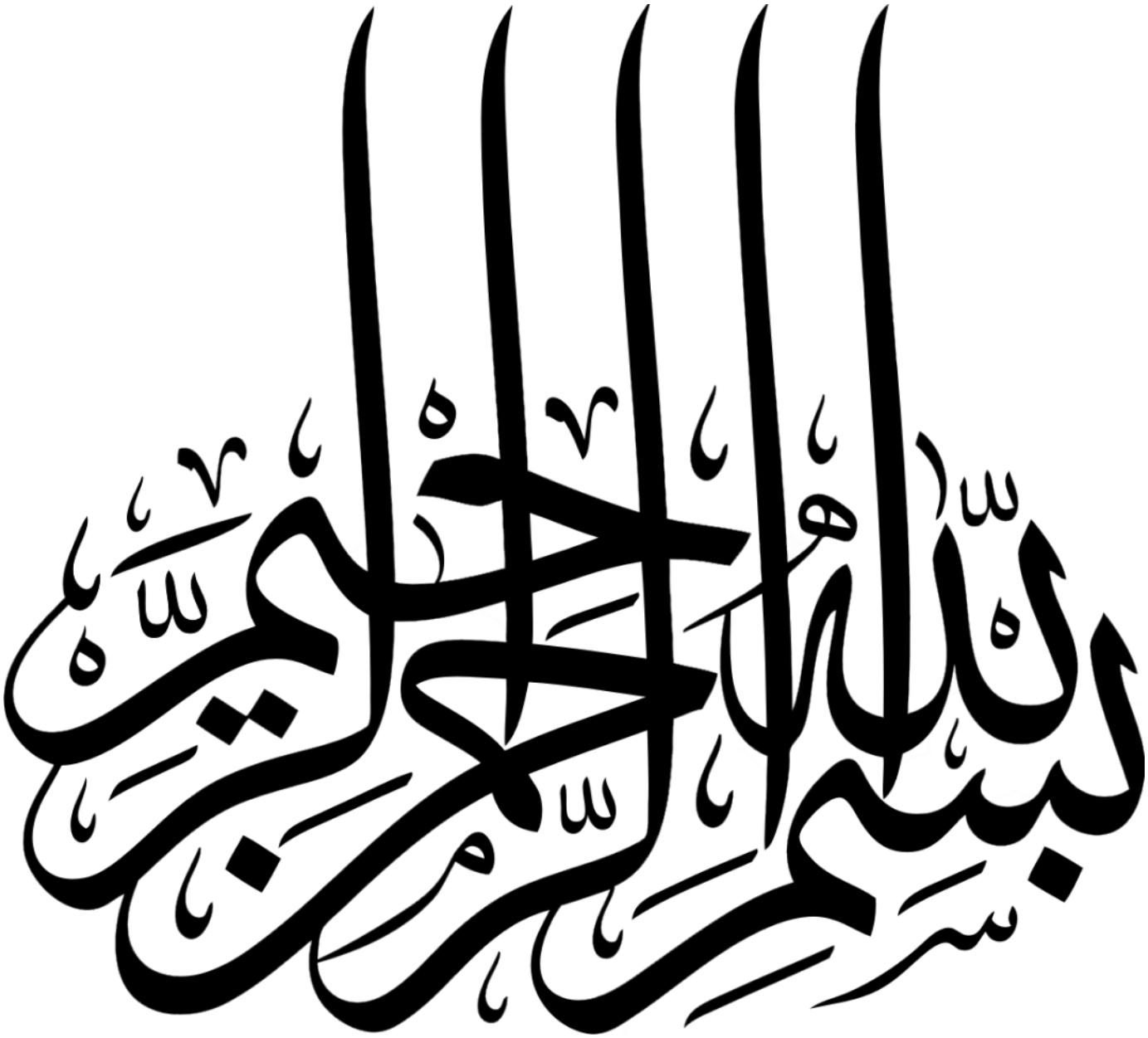
۱۳۹۳

آشنایی با فایروال، سیستم های تشخیص نفوذ و Honey Pot

گروه امنیتی امپراطور

نویسنده

احسان نیک آور



فهرست مطالب

مقدمه

امروزه فناوری اطلاعات در تمامی سازمان ها و شرکت ها رشد چشمگیری را به خود دیده است. استفاده از این فناوری و استفاده از شبکه های رایانه ای در بخش های مختلف سازمان موجب پیشرفت قابل توجه سازمان در نحوه ارائه خدمات و همچنین افزایش کارایی سازمان گردیده است. حال استفاده این امکانات بدون رعایت نکات امنیتی و استفاده مناسب از ابزارهای موجود، همواره با مخاطرات بسیاری همراه می باشد. امنیت یکی از مهمترین اجزای مرتبط با فناوری اطلاعات می باشد و عدم رعایت موارد امنیت می تواند صدمات جبران ناپذیری را به سازمان مطبوع شما وارد نماید.

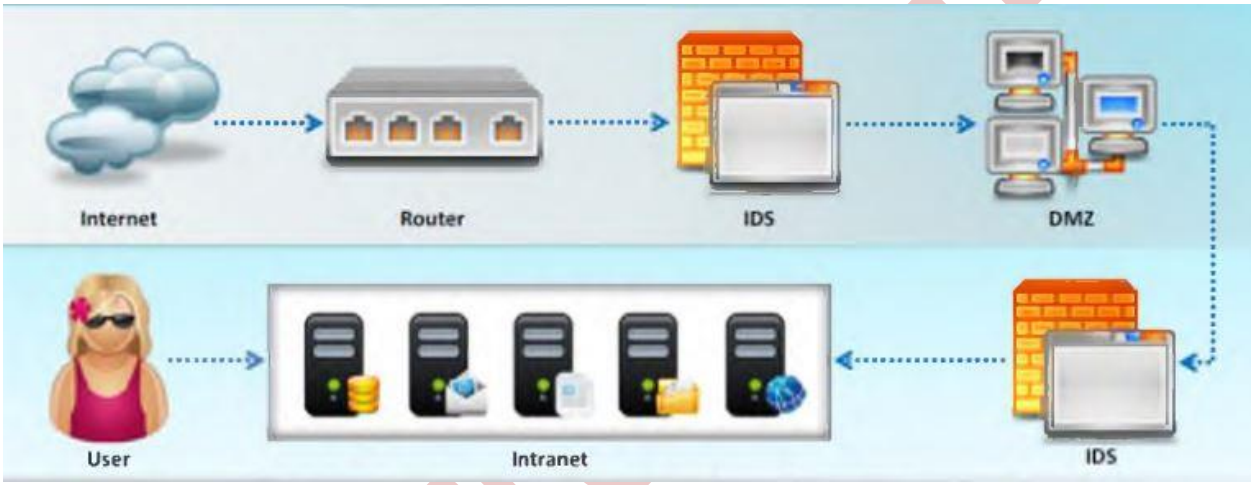
در این کتاب قصد دارم تا شما را سه ابزار امنیتی که استفاده از آنها تا حدودی شما را از آسیب های موجود در فضای شبکه های رایانه ای در امان می دارد، آشنا سازم. در ابتدای هر فصل ابتدا به معرفی ابزار و نحوه عملکرد آن پرداخته شده و در انتها ابزارهای مرتبط با فصل معرفی می گردند. البته لازم به ذکر استفاده ابزار های مذکور در این کتاب به تنهایی امنیت شما را فراهم نمی کند. همانطور که می دانید امنیت یک فرآیند است و با رعایت یک سلسله از این فرآیند ها شما قادر به برقرار امنیت در سازمان خود خواهید بود.

مطالب مطرح شده در کتاب بر گرفته از فصل هفدهم از دوره امنیتی CEH نسخه هشت با نام Evading IDS, Firewalls, and Honeypots می باشد. البته در این کتاب به جنبه معرفی ابزار و ارائه توضیحات در آن پرداخته شده است.

از تمامی دوستان و همکاران گرامی صمیمانه تقاضا دارم در صورت هرگونه انتقاد و پیشنهاد در مورد کتاب و برای هر چه بهتر شدن آن، نظرات خود را به آدرس پست الکترونیکی azamanian۸@yahoo.com ارسال نمایید.

IDS و محل قرارگیری آن

یک سیستم تشخیص نفوذ یا IDS اطلاعات را از یک کامپیوترها و یا یک شبکه به منظور شناسایی امکان نقض سیاست های امنیتی شامل دسترسی غیر مجاز و سوء استفاده های مختلف، جمع آوری نموده و مورد تجزیه و تحلیل قرار می دهد. یک سیستم تشخیص نفوذ همچنین به عنوان یک Packet Sniffer مورد استفاده قرار گرفته و در این مد نیز کار می کند و قادر به رهگیری بسته در امتداد رسانه های ارتباطی مختلف و پروتکل ها در ساختار TCP/IP می باشد. بسته ها در سیستم تشخیص نفوذ پس از مانیتور شدن مورد تجزیه و تحلیل قرار می گیرند. یک IDS همچنین هنگام شناسایی یک نفوذ و رخداد های مشکوک، یک پیام هشدار صادر می کند.



سیستم تشخیص نفوذ چگونه کار می کند؟

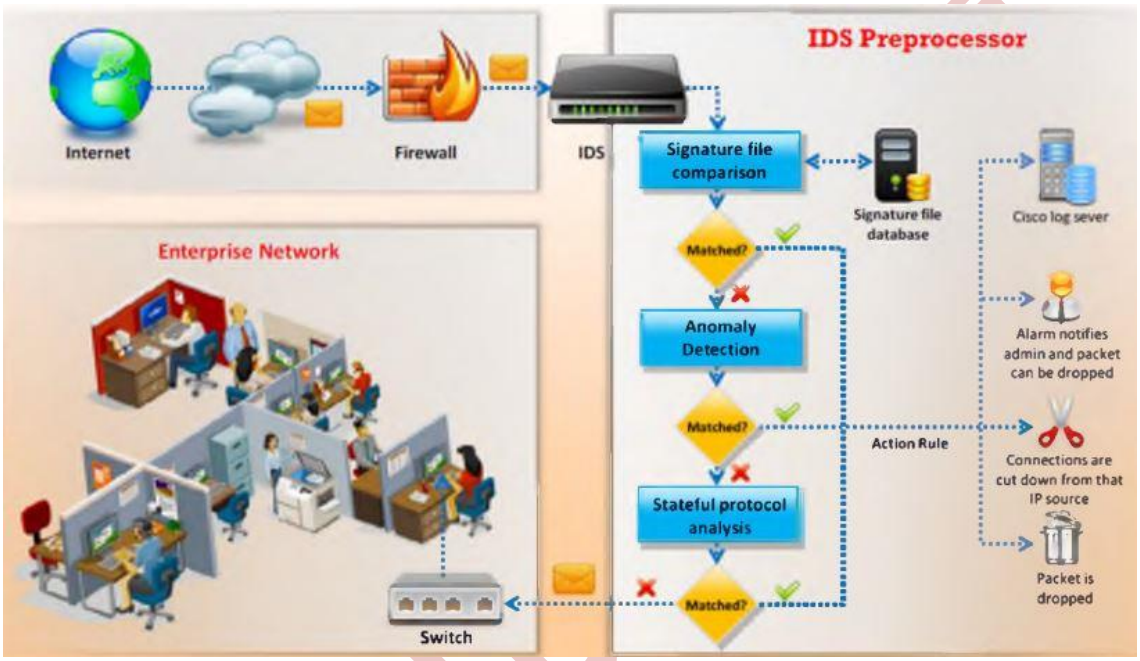
هدف اصلی استفاده از یک IDS نه تنها جلوگیری از نفوذ غیر مجاز بوده بلکه بلافاصله در هنگامی که حمله جریان دارد به مدیر هشدار می دهد. یک مدیر می تواند روش ها و تکنیک هایی که توسط نفوذگر استفاده شده را شناسایی نماید.

IDS ها دارای سنسور هایی به منظور تشخیص امضاء (signature) و برخی IDS های پیشرفته دارای سیستم تشخیص فعالیت های رفتاری مخرب می باشند. آنها حتی اگر امضاء مطابقت نداشته باشد، سیستم تشخیص نفوذ می تواند احتمال وقوع حمله را در موارد خاص به مدیر شبکه گزارش نماید.

اگر امضاء مطابقت داشت، سپس آن را به مرحله بعد حرکت داده یا اتصالات مربوطه را از آدرس IP منبع قطع نموده، بسته حذف شده و یک پیام هشدار به مدیر شبکه ارسال می نماید.

پس از انطباق امضاء، سنسورها بسته را جهت تشخیص ناهنجاری به مرحله بعد هدایت می کنند که آیا بسته دریافتی یا درخواست مورد نظر با آن منطبق هست یا خیر

اگر بسته از مرحله تشخیص ناهنجاری عبور کرد، به مرحله تحلیل پروتکل Stateful می رسد. اگر در این مرحله ساختار پروتکل در تجزیه و تحلیل دچار مشکلی نبود، سپس بسته از طریق سوییچ به شبکه منتقل خواهد شد. در این مرحله نیز در صورت بروز هر گونه مشکل، اتصالات از آدرس IP منبع قطع شده و بسته حذف می گردد و یک هشدار به مدیر ارسال خواهد شد.



راه های شناسایی یک نفوذ

راه های شناسایی نفوذ از طریقه IDS به سه دسته تقسیم می شود.

شناسایی امضاء Signature Detection : این روش به عنوان تشخیص سوء استفاده هم شناخته می شود. این روش تلاش می کند تا با استفاده از امضاء هایی که برای هر نفوذ وجود دارد، رویدادهایی که از قصد سوء استفاده از یک سیستم را دارند، شناسایی نماید.

تشخیص ناهنجاری یا Signature Detection : این روش، نفوذ را بر اساس ویژگی های رفتاری ثابت کاربر تشخیص می دهد.

Protocol Anomaly Detection: این روش به ناهنجاری های خاص مربوط به یک پروتکل اشاره دارد. این مدل به تازگی با مدل IDS یکپارچه شده است. در این روش معایب خاص پروتکل های مدل TCP/IP در شبکه شناسایی می شوند.

پروتکل ها همراه با مشخصات خاص که در ساختار RFC ها موجود است، به منظور استفاده در ارتباطات شبکه، مورد استفاده قرار می گیرند. حال با ردیابی پروتکل های متفرقه و تغییر یافته، حملات جدید قابل شناسایی خواهند بود.

انواع سیستم های تشخیص نفوذ

Network Based IDS

NIDS هر بسته ورودی به شبکه را برای حضور ناهنجاری و اطلاعات نادرست، کنترل می نماید. بر خلاف فایروال ها که نسبت به فیلتر نمودن بسته ها داده با محتوای آسیب رسان محدود می باشند، NIDS ها هر بسته را به صورت کامل کنترل می نمایند. یک NIDS صرف نظر اینکه ترافیک مجاز باشد، همه ترافیک ها را مانیتور نموده و مورد بررسی قرار می دهد. بر اساس محتوا، در هر IP یا سطح برنامه یک هشدار تولید می شود. یک NIDS اساسا برای شناسایی ناهنجاری های سطح روتر طراحی شده است و به ممیزی اطلاعات موجود در بسته های داده و ورود اطلاعات مخرب به شبکه می پردازد.

Host-based Intrusion Detection

یک سیستم تشخیص نفوذ مبتنی بر میزبان رفتارهای مربوط به هر سیستم را مورد تجزیه و تحلیل قرار می دهد. HIDS را می توان بر روی هر سیستم اعم از PC یا یک سرور نصب کرد. NIDS ها معمولا دارای امکانات بیشتری نسبت به HIDS های می باشند. یکی از NIDS برنامه ای است که بر روی یک سیستم اجرا شده و رخدادهای مربوط به برنامه ها و سیستم عامل را دریافت می کند. این برنامه ها برای تشخیص سوء استفاده داخل سیستم بسیار موثر می باشند. اگر یکی از کاربران سعی در فعالیت های غیر مجاز داشته باشد،HIDS معمولا آن را در اسرع وقت شناسایی می کند. علاوه بر تشخیص فعالیت های داخلی غیر مجاز، HIDS ها همچنین در تشخیص تغییر فایل ها به صورت غیر مجاز نیز موثر هستند. HIDS پلت فرم محور بوده و تمرکز بیشتری بر روی سیستم عامل ویندوز دارد. اما HIDS های دیگری برای سیستم عامل های Unix هم وجود دارد. این مکانیسم معمولا شامل حسابرسی برای اتفاقاتی است که در یک میزبان خاص رخ می دهد.

Log File Monitoring

LFM لاگ های ایجاد شده توسط سرویس های شبکه را مانیتور می کند. این IDS ها به منظور شناسایی رویدادهای مخرب، در میان فایل های رخداد به جستجو می پردازند. در شیوه ای مشابه به NIDS ها، این سیستم ها اقدام به جستجوی الگوهای خاص در فایل های رخداد که نشانه های یک نفوذ را دارد، می نمایند.

File Integrity Checking

این مکانیزم ها تروجان ها یا فایل هایی که تغییر یافته اند را کنترل می نماید. از نمونه ای از این برنامه ها می توان به Trip wire اشاره نمود.

Trip wire یک System Integrity Verifier می باشد که ساختار فایل های سیستم را مانیتور نموده و هر گونه تغییر در آن را شناسایی می نماید.

general indications of intrusions (نشانه های کلی نفوذ)

File System Intrusions

با مشاهده فایل های سیستم شما قادر به تشخیص وجود یک مزاحم خواهید بود. فایل سیستم ها، فعالیت های سیستم را ضبط می کنند. هر گونه تغییر یا حذف در خصوصیات فایل به منزله مورد هدف قرار گرفتن سیستم است.

اگر شما به تازگی یک فایل یا برنامه ناشناخته را روی سیستم خود مشاهده می کنید، ممکن است سیستم شما مورد نفوذ قرار گرفته باشد. این سیستم در معرض خطر است و می تواند به سیستم های دیگر در شبکه نیز آسیب وارد کند.

زمانی که یک دسترسی اولیه به یک سیستم ایجاد شد، فرد مورد نظر می تواند این دسترسی را افزایش دهد. پس از آن نفوذگر اقدام به تغییر مجوزهای دسترسی می نماید. به طور مثال دسترسی ها را از فقط خواندنی به دسترسی نوشتن ارتقاء می دهد.

تغییرات غیر قابل توضیح در اندازه یک فایل نیز نشانه ای از یک حمله است. شما باید از تجزیه و تحلیل فایل سیستم اطمینان حاصل کنید.

شما می توانید نام فایل های ناآشنا در دایرکتوری ها را شناسایی کنید که شامل فایل های اجرایی با پسوند های عجیب و با پسوند های دوگانه می باشد.

گمشدن فایل های نیز از نفوذ احتمالی به سیستم خبر می دهند.

Network Intrusions

افزایش ناگهانی در مصرف پهنای باند می تواند نشانه ای از یک نفوذ باشد.

درخواست های اتصال از IP های دیگر از کسانی که در محدوده شبکه می باشند، نشان می دهد که یک کاربر غیر مجاز قصد تلاش برای اتصال به شبکه شما را داشته است.

شما می توانید تلاش های مکرر برای ورود از ماشین های از را ه دور را تشخیص دهید.

داده های بسیار زیاد وارد شده در فایل های ثبت رخداد نشان دهنده تلاش برای حملاتی مانند انکار سرویس، مصرف پهنای باند و انکار سرویس توزیع شده می باشد.

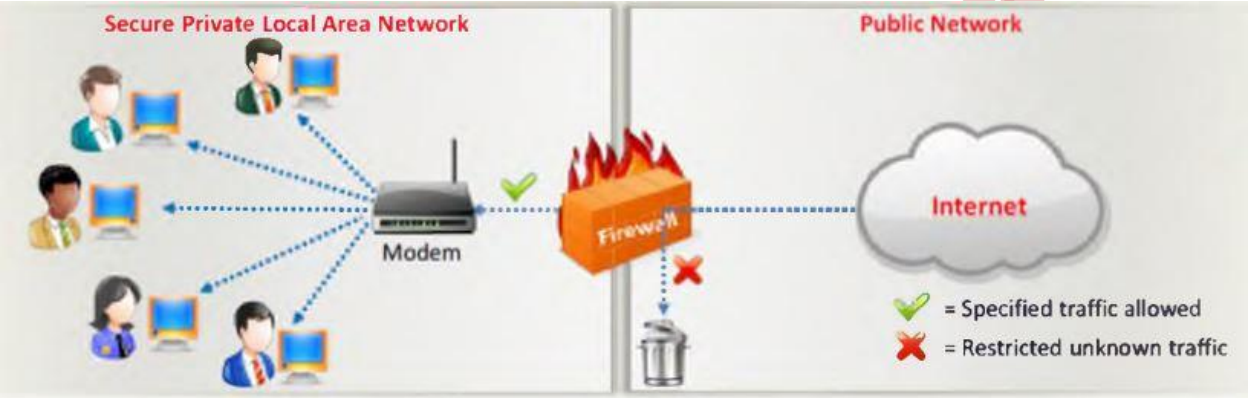
برای بررسی اینکه آیا سیستم مورد حمله قرار گرفته است یا خیر شما نیاز به بررسی پارامتر های خاصی که به وضوح نشان می دهد که یک مزاحم در سیستم شما وارد شده است. هنگامی که یک مزاحم تلاش می کند تا به یک سیستم نفوذ کند، به این موضوع توجه دارد که با تغییرات خاص در سیستم و پیکر بندی های خاص، نشانه های نفوذ خود را مخفی سازد.

نشانه های خاص نفوذ به شرح زیر است:

- سیستم قادر به شناسایی کاربر معتبر نمی باشد.
- ورود به سیستم در ساعات غیر کاری
- تغیرات در نرم افزارهای سیستم و فایل های پیکربندی با استفاده از دسترسی مدیر و وجود فایر های مخفی
- شکاف در فایل های لاگ و بازبینی که نشان می دهد سیستم برای آن زمان خاص بیکار بوده است. این شکاف در واقع نشان می دهد که تلاشی برای نفوذ صورت گرفته و رخداد های مربوط به آن حذف شده است.
- عملکرد سیستم به شدت کاهش می یابد
- سیستم به صورت ناگهانی قفل شده و بدون دخالت کاربر ریبوت می شود.
- دسترسی فعال بدون استفاده از ورود
- رخداد های سیستم بسیار کوتاه و ناقص هستند.
- برچسب های زمانی رخدادها تغییر یافته است که شامل ورودی های عجیب و غریب است.
- مجوز دسترسی روی رخداد ها تغییر یافته، از جمله مالکیت مربوط به رخدادها
- رخدادهای سیستم حذف شده اند
- عملکرد سیستم غیر طبیعی بوده و به روش های نا آشنا پاسخ می دهد.
- پروسه های ناشناس بر روی سیستم شناسایی می شوند.
- صفحه نمایش به صورت غیرمعمول کار کرده و پیام های متنی و پاپ آپ های نا متعارف در سیستم مشاهده می گردند.

Firewall

فایروال سیستمی است که به منظور حفاظت از شبکه خصوصی و کاربران آن در برابر شبکه های دیگر مورد استفاده قرار می گیرد و هم به صورت سخت افزاری و هم به صورت نرم افزاری مورد استفاده قرار می گیرد. فایروال ترافیک های ورودی و خروجی به شبکه را کنترل می کند. یک فایروال در سطح شبکه در نزدیکی مسیریاب قرار گرفته و تمام بسته های شبکه را فیلتر می نماید تا تعیین کند مقصد مورد نظر کجا می باشد. فایروال معمولا به دور از اچزای دیگر شبکه نصب شده به شکلی که هیچ درخواستی به صورت مستقیم نمی تواند توسط منابع خصوصی دریافت گردد. اگر فایروال به درستی پیکربندی گردد، سیستمی که در یک طرف فایروال قرار دارد، از سمت دیگر محافظت خواهد شد.



فایروال یک مکانیزم تشخیص نفوذ است. این سیستم به صورت خاص به عنوان یک سیاست امنیت شناخته می شود. تنظیمات فایروال را می توان برای ایجاد بهترین عملکرد تغییر داد.

فایروال ها می توانند برای محدود کردن ترافیک هایی مانند POP، SNMP و فعال کردن دسترسی ایمیل، تنظیم گردد. همچنین فایروال قادر به مسدود نمودن سرویس ایمیل برای امنیت در برابر هرزنامه ها نیز می باشد.

فایروال می تواند به منظور کنترل ترافیک ورودی در یک نقطه پیکربندی گردد که اصطلاحا آن را choke point می نامند. فایروال همچنین می تواند فعالیت یک برنامه تلفن را که قصد تلاش و ایجاد مزاحمت جهت شماره گیری مودم را در شبکه دارد، شناسایی نماید.

فایروال ترافیک ورودی و خروجی را به وسیله قوانین خود بازبینی نموده و همچنین به مانند یک روتر قادر به انتقال داده بین شبکه ها می باشد. فایروال مدیریت دسترسی به شبکه های خصوصی با برنامه های میزبان را مدیریت می کند.

تمامی تلاش ها در شبکه از جمله تلاش های غیر مجاز مانند تلاش برای ورود به یک حساب برای رسیدگی ثبت می شوند. فایروال می تواند بسته ها را بر اساس آدرس و نوع ترافیک مسدود نماید. آدرس و پورت مربوط به مبدا و مقصد در فایروال

قابل شناسایی هستند، این در حالی است که مسدود سازی آدرس اعمال شده باشد. زمانی که مسدود سازی پروتکل در نظر گرفته شده باشد، نوع ترافیک شبکه و پروتکل ها نیز قابل شناسایی می باشند. هچنین فایروال قادر به شناسایی وضعیت و خواص مربوط به بسته های داده نیز می باشد.

معماری فایروال

نحوه قرارگیری فایروال در ساختار شبکه به سه صورت می باشد که در ادامه به آنها خواهیم پرداخت.

Bastion Host

این نوع ساختار به منظور مقابله در برابر حملات طراحی شده است. در واقع در این حالت فایروال به عنوان یک واسط بین داخل و خارج شبکه می باشد. یک Bastion Host یک سیستم کامپیوتری است که برای محافظت از منابع شبکه در برابر حملات طراحی و پیکربندی شده است.

ترافیک ورودی یا خروجی شبکه از میان فایروال عبود داده می شود. این فایروال دارای دو اینترفیس است.

- اینترفیس عمومی که به صورت مستقیم به اینترنت متصل شده است.
- اینترفیس خصوصی که به شبکه داخلی یا اینترانت متصل شده است.

Screened subnet

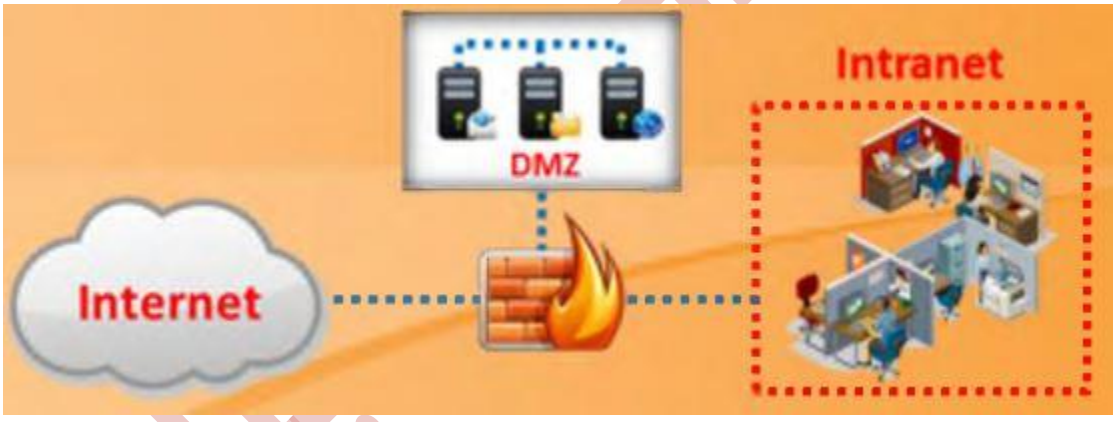
در این نوع طراحی از سه اینترفیس استفاده می شود. اینترفیس اول برای اتصال به اینترنت، اینترفیس دوم برای اتصال به DMZ و اینترفیس سوم برای اتصال به اینترانت یا شبکه داخلی می باشد.

مهمترین مزیت این ساختار جداسازی اینترنت، DMZ از شبکه داخلی است. چنانچه زمانی فایروال به خطر افتاد، دسترسی به شبکه داخلی امکان پذیر نباشد.

DMZ شامل میزبان هایی است که سرویس های عمومی را ارائه می دهند.

محیط عمومی به صورت مستقیم به اینترنت متصل شده است و هیچ میزبان کنترل شده ای توسط سازمان در آن وجود ندارد.

محیط خصوصی سیستمی است که کاربران اینترنت به آن دسترسی ندارند.



Multi-homed firewall

این نوع ساختار معمولا برای دو شبکه و یا بیشتر از آن ارائه می گردد. هر اینترفیس به صورت منتطقی و فیزیکی به شبکه های جداگانه متصل می شود. این نوع از فایروال به منظور بهبود کارایی و قابلیت اطمینان شبکه مورد استفاده قرار می گیرد. در این مورد بیشتر از سه اینترفیس قرار دارد که تقسیم بندی سیستم را به قسمت های کوچک بر اساس اهداف امنیتی خاص سازمان فراهم می نماید.

DeMilitarized Zone (DMZ)

DMZ یک کامپیوتر میزبان یا یک شبکه است که بین محیط داخی یا خصوصی شبکه و محیط خارجی و عمومی قرار می گیرد و به منظور جلوگیری از دسترسی کاربران خارجی به داده های خصوصی شرکت مورد نظر استفاده می شود. DMZ به مانند یک حائل میان شبکه امن داخلی و قسمت نا امن که همان اینترنت است، قرار می گیرد.

انواع فایروال

فایروال ها هم به صورت سخت افزاری و هم به صورت نرم افزاری ارائه می شوند و در یک سیستم برای کنترل ترافیک و تعیین دسترسی ها مورد استفاده قرار می گیرند. فایروال ها به چهار دسته اصلی تقسیم بندی می شوند.

- Packet filters
- Circuit-level gateway
- Application-level gateway
- Stateful multilayer inspection firewalls

Packet filters

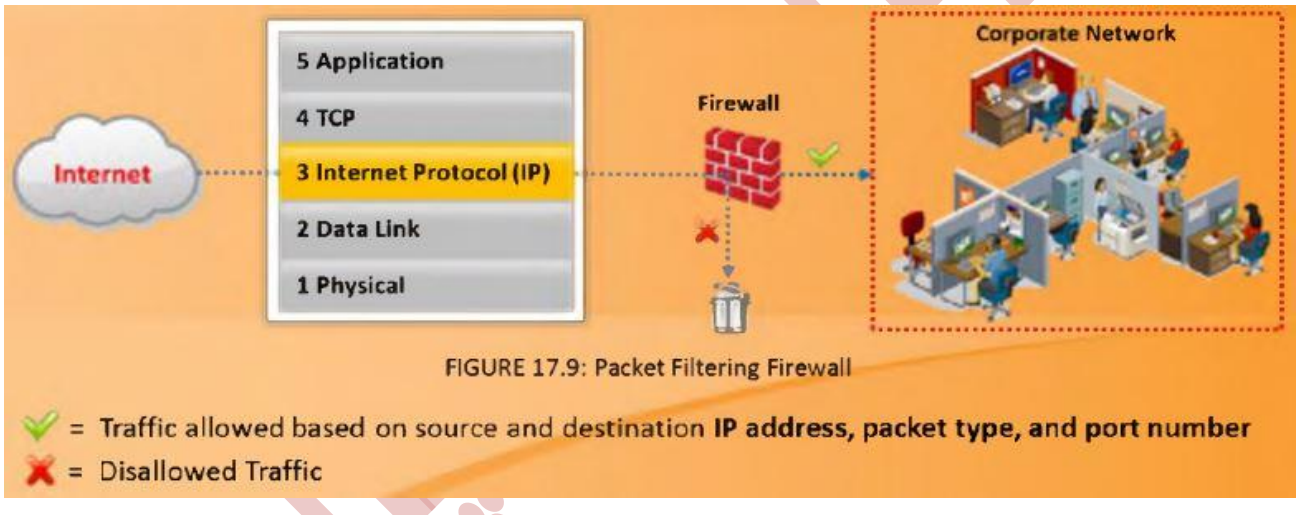


FIGURE 17.9: Packet Filtering Firewall

این نوع فایروال هر یک از بسته هایی که قصد عبور از آن را دارند مورد بازرسی و آنالیز قرار داده و تصمیم می گیرد که آیا این بسته عبور داده شده یا از بین برود. این فایروال بر اساس اطلاعات زیر در مورد بسته ها تصمیم گیری می کند.

آدرس IP مبدا: این مورد به منظور کنترل منبع معتبر استفاده می شود. اطلاعات در مورد آدرس IP مبدا می تواند از سرآیند IP بسته مورد نظر کشف شود که نمایانگر آدرس سیستم مبدا می باشد.

آدرس IP مقصد: از این مورد به منظور کنترل اینکه بسته به مقصد درست فرستاده شده و نوع بسته ارسالی توسط مقصد تایید شود. این اطلاعات نیز از سرآیند IP بسته قابل شناسایی می باشد.

پورت: آدرس پورت TCP/UDPمبدا و مقصد که به منظور شناسایی سرویس مورد نظر استفاده می شود.

بیت های کد TCP: مربوط به Flag های تنظیم شده در بسته مانند SYN، ACK و دیگر بیت ها می باشد.

پروتکل مورد استفاده: به منظور کنترل اینکه آیا به پروتکل مورد نظر اجازه داده شده یا خیر. این مورد بدین منظور است که در برخی از شبکه ها اجازه استفاده از پروتکل های UDP داده نمی شود.

جهت: برای کنترل اینکه آیا بسته در حال وارد شدن و یا خارج شدن است، استفاده می شود.

اینترفیس: برای کنترل اینکه آیا بسته از یک سایت غیرقابل اطمینان آمده یا خیر.

Circuit-Level Gateway Firewall

این نوع فایروال در لایه Session از مدل OSI و یا در لایه Transport در مدل TCP/IP کار می کند. این فایروال داده را بین شبکه ها بدون تایید آن هدایت می کند. بسته های ورودی به میزبان را مسدود می کند اما اجازه می دهد ترافیک از خودش عبور کند. هنگامی که اطلاعات از میان یک فایروال Circuit-Level Gateway عبور داده شده و به یک کامپیوتر راه دور می رسد، به نظر می رسد که منبع اصلی بسته ها Gateway می باشد.

برای شناسایی اینکه آیا نشست های درخواست شده معتبر هست یا خیر، این فایروال دست تکانی TCP را بین بسته ها کنترل می کند. Circuit-Level Gateway بسته منحصر به فردی را فیلتر نمی کند . این نوع فایروال ها نسبتا ارزان بوده و اطلاعات مربوط به شبکه خصوصی را مخفی نگه می دارند.

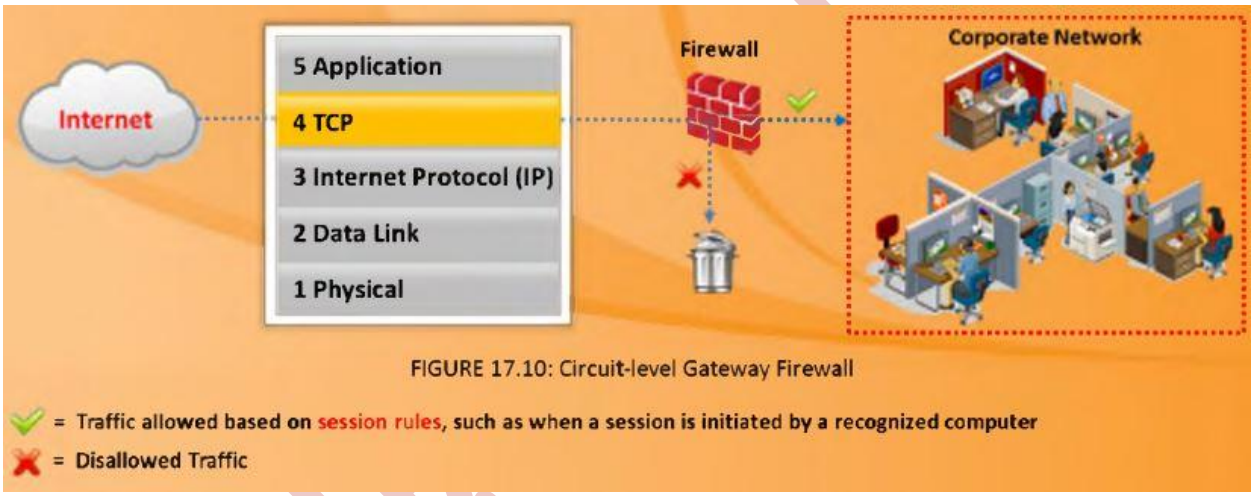


FIGURE 17.10: Circuit-level Gateway Firewall

Application-Level Firewall

فایروال Application-Level در لایه Application از مدل OSI تمرکز دارد. این فایروال اطلاعات برنامه ها را تجزیه و تحلیل می نماید تا در مورد انتقال بسته تصمیم گیرد. در این ساختار تمام ترافیک ورودی و خروجی به خدمات ارائه شده توسط فایروال محدود شده و تمامی درخواست سرویس های دیگر محدود شده اند. شما با استفاده از این فایروال قادر خواهید بود تا ترافیک های مربوط به سرویس های لایه کاربرد مانن FTP، Telnet و دیگر سرویس های این لایه را محدود و یا مسدود نمایید. علاوه بر موارد مذکور انتقال اطلاعاتی که از طریق پروتکل HTTP و با متدها POST و GET ارسال می شوند، توسط این فایروال قابل کنترل و اعمال محدودیت می باشند. لازم به ذکر است به این نوع فایروال ها پروکسی فایروال نیز گفته می شود.

Stateful Multilayer Inspection Firewall

فایروال Stateful همه جنبه های سه نوع دیگر را دارا می باشد. این فایروال ها قادر به مسدود نمودن بسته ها در لایه شبکه، تصمیم گیری در مورد نشست های قانونی و ارزیابی محتوای بسته ها در لایه کاربرد می باشند. لازم به ذکر است که ناتوانی فایروال های Packet Filter در کنترل سرآیند بسته ها و اجازه عبور بسته، توسط فایروال های Stateful حل گردیده است.

این نوع فایروال ها می تواند سابقه بسته های انتقال یافته را در خود ذخیره کنند و در مورد بسته هایی که به آن ها در آینده پاسخ داده خواهد شد تصمیم گیری کنند. با توجه به موضوعات مطرح شده فایروال های Stateful نسبت به دو نوع Packet Filter و Application Firewall عملکرد بهتری از خود نشان می دهند.

لازم به ذکر است که فایروال PIX شرکت سیسکو از نوع Stateful می باشد.

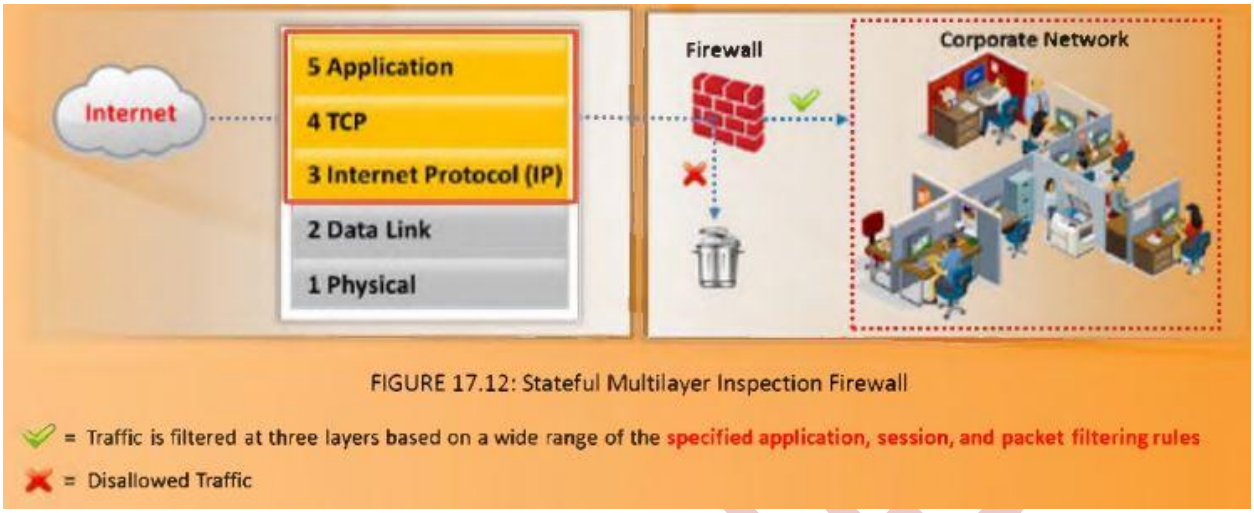


FIGURE 17.12: Stateful Multilayer Inspection Firewall

شناسایی فایروال به وسیله اسکن پورت

به طور سیستماتیک اسکن پورت های یک کامپیوتر، به عنوان عملیات پورت اسکن شناخته می شود. نفوذگران با استفاده از چنین روش هایی سعی در شناسایی آسیب پذیری های مختلف به منظور به خطر انداختن یک شبکه را دارند. این یکی از روش های رایجی است که نفوذگر با استفاده از آن به جستجوی پورت های استفاده شده توسط قربانی مبادرت می ورزد. یکی از بهترین ابزارها بدین منظور نرم افزار Nmap می باشد.

یک پورت اسکن به نفوذگر کمک می کند تا پورت های در دسترس و سرویس های فعال در این پورت ها را شناسایی نماید. این روش شامل ارسال یک پیغام به هر پورت در یک بازه زمانی مشخص است. نوع پاسخ دریافتی، وضعیت پورت موجود را به شما نشان خواهد داد.

حال برخی از فایروال ها به وسیله پورت اسکن شناسایی می شوند. دلیل شناسایی این فایروال ها، پورت هایی است که در آن ها به حالت گوش کردن یا Listen وجود دارد. به طور مثال در Check Point's FireWall-۱ پورت های ۲۵۶، ۲۵۷ و ۲۵۸ از نوع TCP به گوش می باشد و یا پروکسی سرور های مایکروسافت معمولا بر روی پورت های ۱۰۸۰ و ۱۷۴۵ به گوش هستند.

شناسایی فایروال به وسیله Firewalking

Firewalking روشی است که برای جمع آوری اطلاعات در مورد شبکه ها از راه دور که در پشت فایروال قرار دارند، استفاده می شود. در این حالت شما قادر خواهید بود تا لیست های کنترل دسترسی یا ACL را بر روی فایروال ها و روترهای Packet Filter ، شناسایی نمایید. در این ساختار از همان تکنیک های مربوط به Tracerouting استفاده می شود و با استفاده از ارسال یک بسته ICMP با یک TTL اقدام به شناسایی اولین روتر و به همین ترتیب به تعداد TTL ها اضافه می گردد تا به فایروال برسیم.

نرم افزار Firewalk شناخته شده ترین ابزار به منظور انجام عملیات firewalking می باشد. این عملیات شامل دو مرحله است که یکی مرحله شناسایی و دیگری مرحله اسکن بوده و نیازمند سه نوع میزبان است که به شرح زیر می باشند.

Firewalking host: میزبان Firewalking سیستمی است خارج از شبکه هدف که بسته های داده به منظور به دست آوردن اطلاعات بیشتر در مورد شبکه هدف، از آن به میزبان مقصد ارسال می شود.

Gateway host: میزبان Gateway سیستمی است داخل شبکه که به اینترنت متصل شده و از طریق آن بسته های داده به مقصد مورد نظر هدایت می شوند.

Destination host: میزبان مقصد سیستم هدف در شبکه مورد نظر است که بسته های داده خطاب به آن ارسال می شود.

شناسایی فایروال به وسیله Banner Grabbing

بنرها پیام هایی هستند که توسط سرویس های شبکه در مدت اتصال به سرویس مورد نظر، فرستاده می شوند. بنرها در واقع اعلام می کنند که سرویس روی سیستم مورد نظر در حال اجرا می باشد. Banner Grabbing روش عمومی است که به منظور شناسایی سیستم عامل و سرویس های سیستم هدف مورد استفاده قرار می گیرد. سرویس های FTP، Telnet و وب سرور، سه سرویس اصلی هستند که بنرهای خود را ارسال می کنند.

پورت های مربوط به سه سرویس ذکر شده نباید باز قرار داده شوند، به این دلیل که در برابر Banner Grabbing آسیب پذیر می باشند. یک فایروال نمی تواند Banner Grabbing را مسدود سازد زیرا ارتباط بین سیستم نفوذگر و سیستم هدف مشروع به نظر می رسد.

به طور مثال Banner Grabbing سرویس STMP به صورت زیر است:

Telnet mail.targetcompany.org ۲۵

Banner Grabbing مکانیزمی است برای مشخص نمودن آگهی ها و اطلاعات مربوط به برنامه هاست. برای مثال هنگامی که کاربر یک ارتباط از نوع Telnet با یک پورت شناخته شده در سرور هدف برقرار می کند(دستور بالا را وارد کرده و کلید Enter را می زند) پس از مدت زمانی نتایج زیر نمایش داده می شود.

C:\>telnet www.corleone.com ۸۰

HTTP/۱,۰ ۴۰۰ Bad Request

Server: Netscape - Commerce/۱,۱۲

اطلاعات بدست آمده در این روش می تواند کمک بسیار زیادی به نفوذگر برای ادامه حمله خود نماید.

Honey pot

یک Honey pot سیستمی است که برای جلب توجه و گمراه کردن افرادی که قصد تلاش برای دسترسی غیر به شبکه را دارند، بکار می رود. Honey pot به معنای ظرف عسل است. البته نام گذاری این سیستم با این نام اشاره به محرک بودن آن برای نفوذگر ها می باشد که در ادامه به ویژگی های این سیستم امنیتی اشاره خواهیم کرد. هر زمان که تعاملی با یک Honey pot برقرار شود، به احتمال زیاد یک فعالیت مخرب می باشد. Honey pot منحصر به فرد هستند و مشکل خاصی را حل نمی کنند، در عوض آنها یک ابزار بسیار انعطاف پذیر با بسیاری از برنامه های امنیتی متفاوت هستند. برخی از Honey pot ها می توانند از حملات جلوگیری نمایند و برخی دیگر حملات را تشخیص می دهند در حالی که تعداد کمی از آنها می توانند برای جمع آوری اطلاعات مورد استفاده قرار گیرند.

به مثال های زیر توجه نمایید.

نصب یک سیستم در شبکه با هیچ هدف خاصی به غیر از ثبت تمامی رخدادهای مربوط به تلاش برای دسترسی به سیستم

نصب یک سیستم عامل قدیمی با آسیب پذیری های اصلاح نشده در شبکه. به طور مثال نصب یک سیستم عامل ویندوز NT ۴ با IIS نسخه ۴ که می تواند با روش های مختلفی هک شود. حال می توان از یک سیستم تشخیص نفوذ استاندار برای شناسایی نفوذ به این سیستم و تلاش برای حمله به آن، استفاده کرد. زمانی که نفوذگر سیستمی با مشخصات آسیب پذیر در شبکه برخورد می نماید، قصد حمله به آن را دارد که تلاش های وی برای این کار توسط ساختار پیاده سازی شده تشخیص داده شده و اطلاعات مربوط در سیستم مورد نظر ذخیره می گردد. بدین صورت از ورود فرد با مشخصات ثبت شده جلوگیری می گردد و شبکه اصلی شما از دسترس این فرد در امان خواهد بود.

هر سیستمی می تواند یک Honey pot باشد. برای مثال شما می توانید روی یک ویندوز NT نام حساب مدیر یا administrator را تغییر داده و یک حساب جعلی با همین نام ایجاد کنید به طوری که فاقد کلمه عبور باشد. ویندوز NT اجازه ثبت فعالیت کاربر را فراهم می کند. بنابر این Honey pot تلاش برای دسترسی به حساب مدیر و بدست آوردن دسترسی آن را ردیابی می کند.

انواع Honey pot

Honey pot ها اساسا به دو دسته تقسیم می شوند.

Low-interaction Honeypot

این نوع از Honey pot ها توسط شبیه سازی سرویس ها و برنامه هایی که می خواهید پیدا شوند بر روی یک سیستم کار می کنند. اگر نفوذگر کاری انجام دهد که خارج از ساختار شبیه سازی شده باشد، Honey pot پیغام خطا خواهد داد. آنها مقدار محدودی از اطلاعات و برخی از فعالیت ها را مانیتور می کند. نرم افزارهایی مانند Spector، Honeyd و KFSensor نمونه ای از این نوع Honey pot می باشند.

ابزار Honeyd متن باز می باشد و برای اجرا در سیستم های یونیکسی طراحی شده است. این نرم افزار براساس مفهوم مانیتورینگ فضای IP استفاده نشده کار می کند بدین صورت که اگر مشاهده نماید تلاشی برای اتصال به یک IP استفاده نشده در حال صورت گرفتن می باشد، اتصال را قطع نموده و سپس اقدام به تعامل با نفوذگر می نماید و تظاهر می کند که هدف یا همان قربانی است.

به صورت پیش فرض Honeyd، ارتباطات روی هر پورت TCP و UDP را شناسایی و ثبت می نماید.علاوه بر این کاربر می تواند تنظیمات مربوط به پورت خاصی را شبیه سازی نماید. هنگامی که نفوذگر به سرویس شبیه سازی شده متصل می

گردد، نه تنها Honey pot فعالیت های وی را شناسایی و ثبت می نماید همچنین تمامی فعالیت های نفوذگر را با سرویس مورد نظر مانیتور می نماید.

High-interaction Honeypot

Honey net ها نمونه ای از این Honey pot ها می باشند. Honey net ها، نه یک محصول بوده و نه یک راه حل نرم افزاری هستند که کاربر آنها را نصب نماید. در واقع آن یک معماری است که در آن تمام کامپیوترهای شبکه برای حمله طراحی شده اند. این ایده بدین منظور است که تمامی فعالیت های در سطح شبکه جمع آوری شده و مانیتور شوند. در این شبکه قربانیان در نظر گرفته شده قرار می گیرند و شبکه اصلی در حال اجرای برنامه های کاربردی واقعی می باشد.

نفوذگر این سیستم های در نظر گرفته شده پیدا کرده و به آن ها نفوذ می کنند. هنگامی که در حال انجام این کار ها هستند، تشخیص نمی دهند که با یک Honey net در ارتباط هستند. تمام فعالیت های آن ها در این ارتباط بدون اینکه متوجه شوند، مانیتور شده و ثبت می گردد.

در این زمان Honey net فعالیت های نفوذگر را کنترل می کند. Honey net این کار را توسط Honey wall Gateway انجام می دهد. این Gateway اجازه می دهد تا ترافیک ورودی به سیستم های قربانی در نظر گرفته شده وارد شود، ولی ترافیک خروجی را با استفاده از تکنولوژی های پیشگیری از نفوذ کنترل می کند. با این روش، انعطاف پذیری لازم را در اختیار نفوذگر قرار داده می شود تا تنها با سیستم های در نظرگرفته تعامل برقرار نماید و از نفوذ وی به سیستم های دیگر غیر از Honey net جلوگیری به عمل می آید.

آشنایی با برخی از سیستم های IDS، Firewall و Honey pot

در این قسمت با برخی از ابزارهای مورد استفاده در شبکه ها که تحت عنوان سیستم های تشخیص نفوذ، فایروال و Honey pot می باشند آشنا می خواهیم شد.

ابزارهای تشخیص نفوذ Snort

Snort یک سیستم تشخیص و جلوگیری از نفوذ متن باز است که توانایی انجام تجزیه و تحلیل آنلاین ترافیک شبکه و ثبت بسته ها رو شبکه های مبتنی بر IP را داراست. این نرم افزار قادر به تجزیه تحلیل پروتکل، جستجو و تطبیق محتوا نیز می باشد. از این ابزار همچنین می توانید برای شناسایی انواع حملات در سطح شبکه مانند سر ریز بافر، اسکن پورت، حملات CGI، حملات مربوط به شناسایی سیستم عامل و غیره استفاده نمایید.

Snort از یکسری قوانین انعطاف پذیر برای توصیف ترافیک استفاده می کند که باید جمع آوری شده و مصوب شوند. همچنین به عنوان یک موتور شناسایی با بهره گیری از پلاگین های خود و ساختار معماری ماژولار فعالیت می کند. Snort

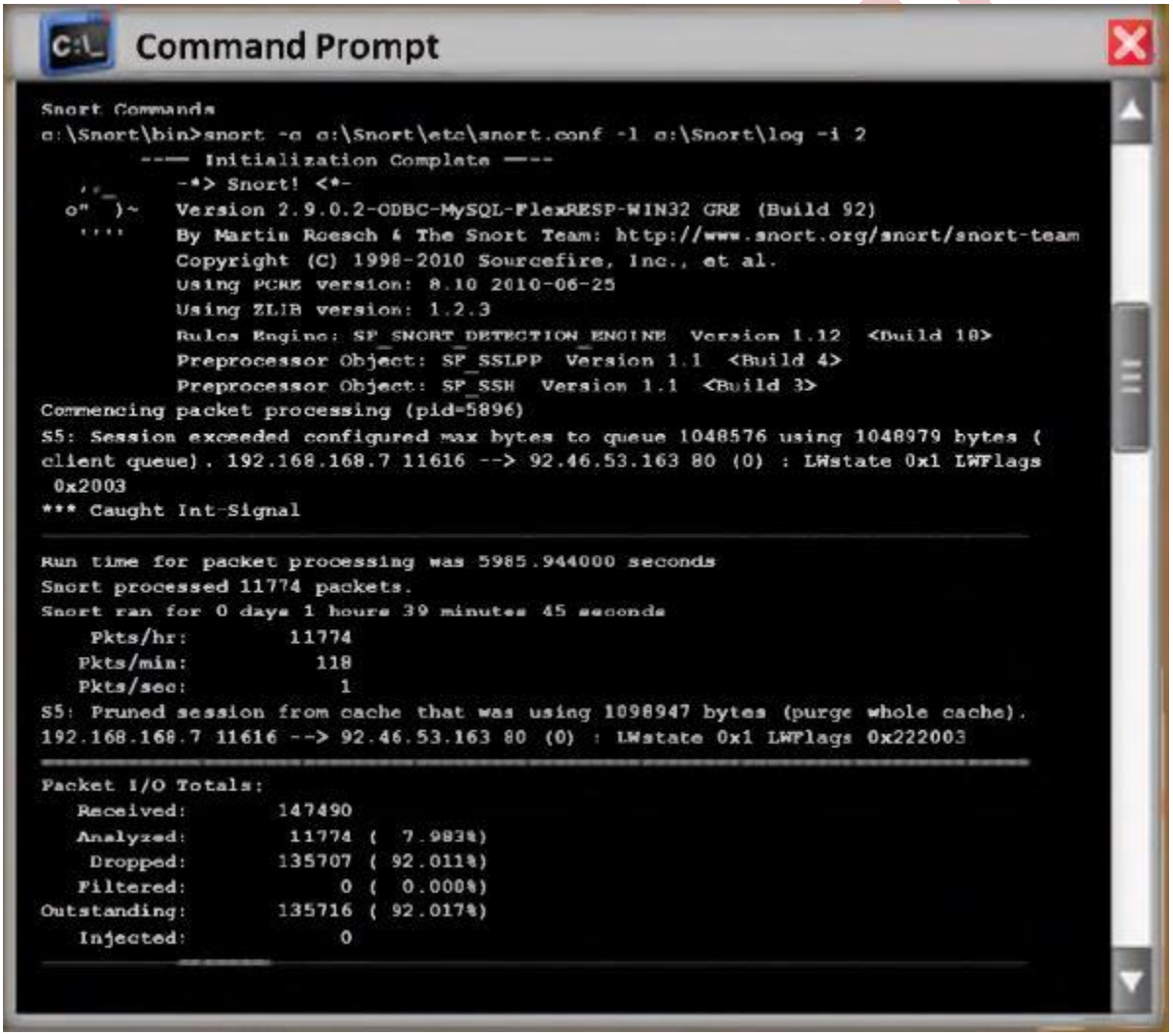
دارای یک سیستم هشدار Real Time بوده و قادر است هشدار های ایجاد شده را برای ساختارهای Syslog، فایل خاص، سوکت مربوط به Unix و یا یک پیغام برای کلاینت ویندوز، ارسال نماید.

Snort در سه مد قابل استفاده می باشد. این مد ها شامل:

به عنوان یک شنود بسته یا Packet Snifer مانند Tcpdump

به عنوان یک ثبت کننده بسته یا Packet Logger که برای اشکال زدایی و غیره مفید می باشد.

به عنوان یک سیستم تشخیص و جلوگیری از نفوذ تمام عیار



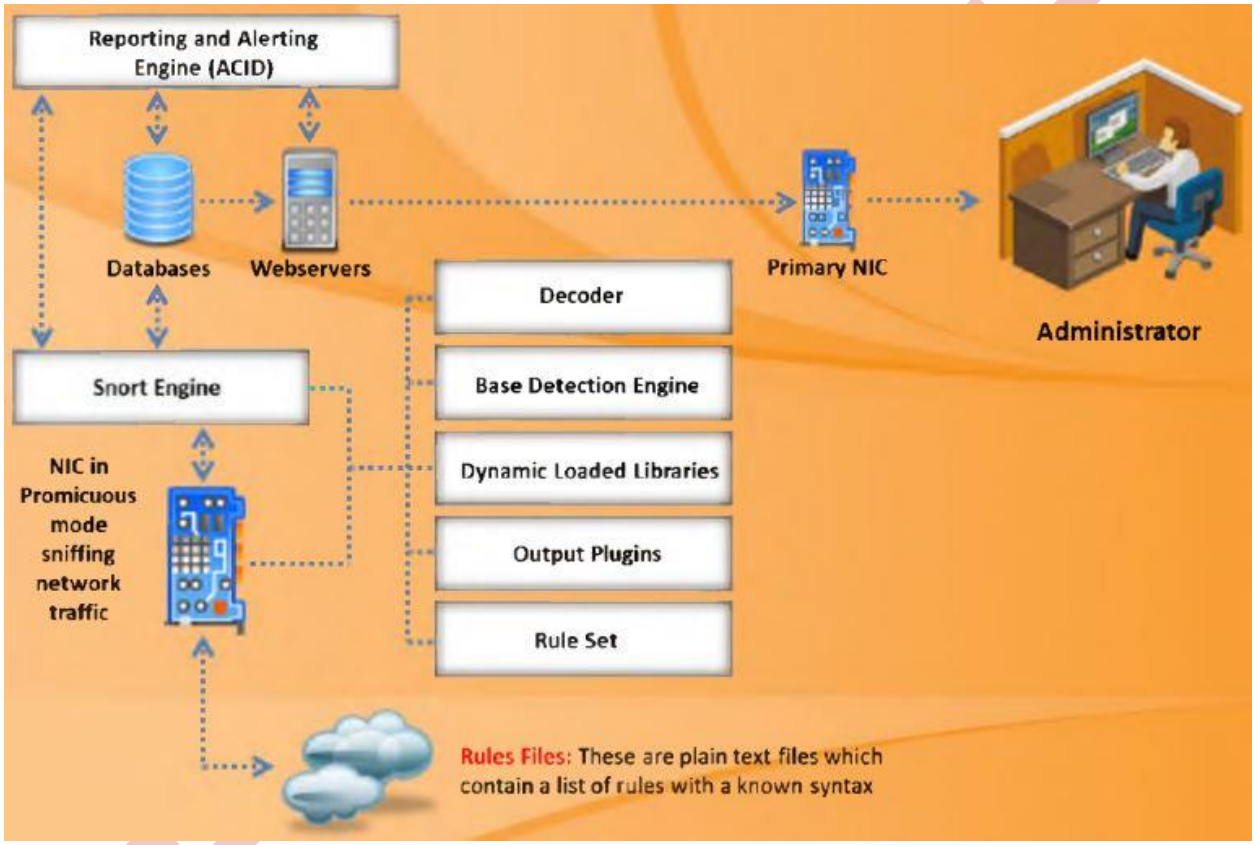
Snort چگونه کار می کند؟

سه عنصر اساسی در این ابزار به شرح زیر است.

Decoder: ذخیره بسته های مانیتور شده در پشته، شناسایی پروتکل های سطح پیوند و رمزگشایی IP

Detection Engine: تطبیق بسته ها با قوانین از قبل تعریف شده و راه اندازی اولیه Snort

Output Plug-ins: این ماژول مربوط به فرمت اطلاعیه برای کاربر جهت دسترسی آنها با روش های مختلف



قوانین Snort

Snort از توابع کتابخانه ای معروف Libpcap برای لینوکس و یونیکس یا Winpcap برای ویندوز استفاده می کند. این در واقع همان کتابخانه ای است که Tcpdump برای انجام عملیات شنود بسته از آن استفاده می کند. Snort می تواند تمام ترافیک عبوری از میان رسانه شبکه را رمزگشایی نموده و آنالیز نماید. البته نکته ای که باید به آن توجه کرد این است که Snort باید به پورتی وصل شود که قابلیت کار در مد بی قاعده را داشته باشد. در ساختار سوییچ های سیسکو، سیستمی

که Snort در آن اجرا شده است را به پورتی متصل می کنند که خاصیت Span در آن فعال شده باشد. این قابلیت باعث می شود تا یک نسخه از تمام ترافیکی عبوری در شبکه، به سمت پورت Span شده که Snort به آن متصل است هدایت شود. بر اساس محتوای بسته های ارسالی و قوانین تعریف شده در Snort که در فایل پیکربندی قرار دارد، هشدار مورد نظر تولید می گردد.

در Snort اجازه نوشتن برخی قوانین برای کاربران فراهم شده است که این قوانین باید موارد زیر را توصیف کنند:

هرگونه تخلف از سیاست های امنیت شرکت که ممکن است تهدیدی برای امنیت شبکه و دیگر اطلاعات با ارزش آن شرکت باشد.

شناسایی تمام تلاش های شناخته شده و مشترک برای بهره برداری از آسیب پذیری ها

شرایطی که کاربر فکر می کند یک بسته شبکه غیر معمولی می باشد به عنوان مثال زمانی که هویت بسته ناشناخته و نا معتبر است.

قوانین Snort نوشته شده برای تجزیه و تحلیل هر دو پروتکل بوده و قادر به جستجو و تطبیق باشد. ویژگی دیگری که در این مورد باید به آن توجه کرد، مقاوم و انعطاف پذیر بودن این قوانین است. زمانی که صحبت از مقاومت یا همان robust به میان می آید، این بدان معنی است که سیستم باید به صورت کامل فعالیت های صورت گرفته بر روی شبکه را کنترل نماید و مدیر را از هر گونه تلاش بالقوه نفوذ با خبر سازد. حال زمانی که سخن از انعطاف پذیری یا flexible بودن به میان می آید، بدان معنی است که سیستم باید سازگاری کافی به منظور اقدامات سریع و همچنین اقدامات مربوط به اصلاح و چاره جویی برای مشکل بوجود آمده را داشته باشد.

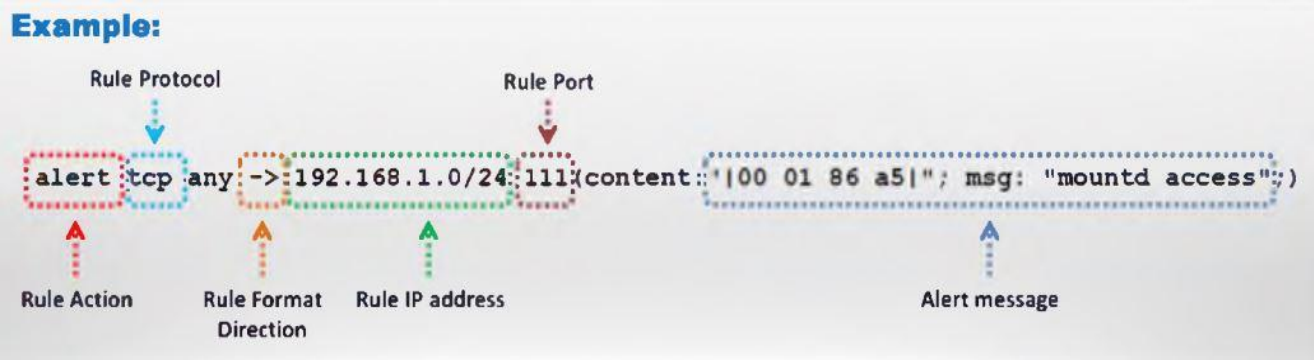
هر دو محبث مربوط به استحکام و انعطاف پذیری از طریق یک راهکار ساده و آسان قابل دستیبابی است و آن استفاده زبان مربوط به قوانینی است که در snort وجود دارد. دو اصل اساسی وجود دارد که برای نوشتن قوانین snort باید آنها را به یاد داشته باشید. آنها به شرح زیر می باشند:

سعی کنید قوانین را کوتاه، دقیق و قابل درک نوشته که از یک خط تجاوز ننماید.

هر قانون باید به دو بخش منطقی تقسیم گردد که یکی سرآیند قانون بوده و دیگری گزینه ها یا Option های آن می باشد.

سرآیند یک قانون شامل Action های آن قانون به همراه نوع پروتکل، آدرس IP مبدا و مقصد، پورت های مبدا و مقصد و بازه شبکه ای که این قانون باید روی آن اجرا شود(CIDR) ، می باشد.

قسمت Option در قوانین Snort در واقع همان پیام های هشداری می باشد که برای اطلاعات بیشتر در مورد آن قانون است. در زیر شما نمونه ای از یک قانون در Snort را می بینید.



Action های قوانین و پروتکل های IP

سرآیند قوانین شامل اطلاعاتی است که تعریف می کند که چه کسی، کجا و چه بسته ای ارسال نموده است. این باعث می شود که تمام خصوصیات مربوط به بسته نمایش داده شود. اولین گزینه در قوانین، مربوط به Action آن می باشد. Action مربوط به قوانین می گوید Snort زمانی که بسته ای را که با قوانین مطابقت دارند پیدا کرد، چه واکنشی را از خود نشان دهد. پنج action پیش فرض در Snort قابل تعریف است که به صورت زیر می باشند.

Alert: یک هشدار را با استفاده از روش هشدار انتخاب شده تولید می کند و سپس بسته مورد نظر را ثبت می کند.

Log: بسته هار را ثبت می کند.

Pass: از بسته ها صرفنظر می کند.

Active: هشدار داده و سپس قانون دیگری را فعال می کند.

Dynamic: منتظر می ماند تا توسط یک قانون فعال دیگر فراخوانی شده و سپس به مانند قوانین عمل می کند.

علاوه بر موارد فوق اگر شما Snort را در وضعیت inline قرار دهید شما قادر به drop، Sdrop و reject کردن نیز می باشد.

Drop : مسدود نمودن و ثبت بسته ها

Reject : مسدود نمودن، ثبت بسته و ارسال یک TCP reset اگر از پروتکل TCP استفاده کرده باشد و ارسال پیام ICMP port unreachable در صورتی که از پروتکل UDP استفاده کرده باشد.

Sdrop : مسدود نمودن بسته بدون ثبت آن

پروتکل های IP

پروتکل IP به منظور ارسال داده از یک سیستم به سیستم دیگر در اینترنت مورد استفاده قرار می گیرد. IP از آدرس دهی یکتا برای هر کامپیوتر درون یک شبکه پشتیبانی می نماید. داده ها در ساختار IP داخل بسته (Packet) سازماندهی می شوند. هر بسته شامل آدرس مبدا، مقصد و موارد دیگر است. Snort از سه نوع پروتکل مربوط به IP جهت شناسایی رفتار های مشکوک پشتیبانی می نماید.

TCP: پروتکل TCP یا (Transmission Control Protocol) به منظور اتصال دو میزبان مختلف به یکدیگر و تبادل اطلاعات بین آنها مورد استفاده قرار می گیرد.

UDP: پروتکل UDP یا (User Datagram Protocol) به منظور ارسال پیام های همگانی در یک شبکه مورد استفاده قرار می گیرد.

ICMP: پروتکل ICMP یا (Internet Control Message protocol) توسط سیستم عامل به منظور ارسال پیام های خطا و غیره مورد استفاده قرار می گیرد.

البته لازم به ذکر است موارد ذکر شده در مورد پروتکل های TCP، UDP و ICMP فقط توضیح بسیار کوتاه بوده و هر کدام از آنها وظایف بسیار بیشتری در شبکه دارند که توضیح کامل آنها در این مطلب شایسته نمی باشد. برای اطلاع هر چه بهتر در این زمینه به کتاب های مربوط به شبکه مراجعه فرمایید.

عملگر مسیر و آدرس های IP

عملگر مسیر ($<>$-) نشان دهنده مسیر و جهت ترافیک می باشد که قوانین آنها را وضع و تایید می نمایند. آدرس IP و شماره پورت که در سمت چپ عملگر مسیر هستند به این مطلب اشاره دارند که ترافیک از سمت میزبان مبدا می آید و اطلاعات مربوط به آدرس IP و پورت که در سمت راست عملگر قرار دارند به این مطلب اشاره دارند که ترافیک به سمت میزبان مقصد در حال حرکت است. البته عملگر مسیر دو طرفه نیز وجود دارد که با علامت $<>$ نشان داده می شود. این عملگر به Snort می گوید که هر دو آدرس و پورت را در مبدا و مقصد در نظر بگیرد. این موارد به ضبط و تحلیل مکالمات دو طرفه مانند Telnet و جلسات POP۳ کمک می کند.

همچنین به این نکته توجه داشته باشید که هیچ عملگرد مانند $<$- وجود ندارد.

بخش بعدی در قوانین مربوط به Snort، استفاده از آدرس IP و پورت مبداء و مقصد می باشد. لازم به ذکر است که مسیر و جهت آن نیز باید مشخص گردد. Snort می تواند یک آدرس IP و یا لیستی از آدرس ها را قبول نماید. هنگامی که لیستی از آدرس های IP را در نظر دارید باید به وسیله یک کاما همانند مثال زیر آنها را از هم جدا نمایید.

۱۹۲,۱۶۸,۱,۱،۱۹۲,۱۶۸,۱,۴۵،۱۰,۱,۱,۲۴

باید مراقب باشید که فضای خالی بین آدرس ها وجود نداشته باشد.

همچنین شما می توانید رنج خاصی از آدرس ها را نیز انتخاب نمایید. برای این کار از نماد های CIDR استفاده نمایید. همچنین شما می توانید از عملگر منطقی Not با نماد (!) به منظور جدا سازی یک رنج یا آدرس خاص از قوانین مربوطه، استفاده نمایید.

شماره پورت

شما می توانید شماره پورت را به روش های مختلفی مانند any یا همه، static یا دستی، range یا گروهی و به صورت negation یا نقیض تعریف نمایید. مثال زیر نمونه از یک قانون است که نشان می دهد action از نوع log بوده و نوع پروتکل آن tcp است. مسیر آن نیز از هر پورت و هر آدرس IP به رنج آدرس ۱۹۲,۱۶۸,۱,۰ به غیر از پورت های ۶۰۰۰ تا ۶۰۱۰ می باشد.

log tcp any any -> ۱۹۲,۱۶۸,۱,۰/۲۴ !۶۰۰۰:۶۰۱۰

به جدول زیر توجه نمایید.

Protocols	IP address	Action
Log UDP any any ->	92.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from privileged ports less than or equal to 1024 going to ports greater than or equal to 400

دیگر سیتسم های تشخیص نفوذ

علاوه بر Snort سیستم های تشخیص نفوذ ذیگری نیز موجود است که اسامی برخی از آنها همراه با آدرس سایت ارائه دهنده به شرح زیر است:

Tipping Point

http://hl۰۱۶۳.wwwl.hp.com

IBM Security Network IDS

http://www-۰۱.ibm.com

Peek & Spy

http://networkingdvnamics.com

INTOUCH INSA-Network Security Agent

http://www.ttinet.com

Strata Guard

http://www.stillsecure.com

IDP۸۲۰۰ Intrusion Detection and Prevention Appliances

https://www.juniper.net

OSSEC

http://www.ossec.net

Cisco Intrusion Prevention Systems

http://www.cisco.com

AIDE (Advanced Intrusion Detection Environment)

http://aide.sourceforge.net

SNARE (System iNtrusion Analysis & Reporting Environment)

http://www.intersectalliance.com

Vanguard Enforcer

http://www.go۲vanguard.com

Check Point Threat Prevention Appliance

http://www.checkpoint.com

Fragroute

http://www.monkey.org

Next-Generation Intrusion Prevention System (NGIPS)

http://www.sourcefire.com

Outpost Network Security

http://www.agnitum.com

Check Point IPS-۱

http://www.checkpoint.com

FortiGate

http://www.fortinet.com

Enterasys® Intrusion Prevention System

http://www.enterasys.com

StoneGate Virtual IPS Appliance

http://www.stonesoft.com

Cyberoam Intrusion Prevention System

http://www.cyberoam.com

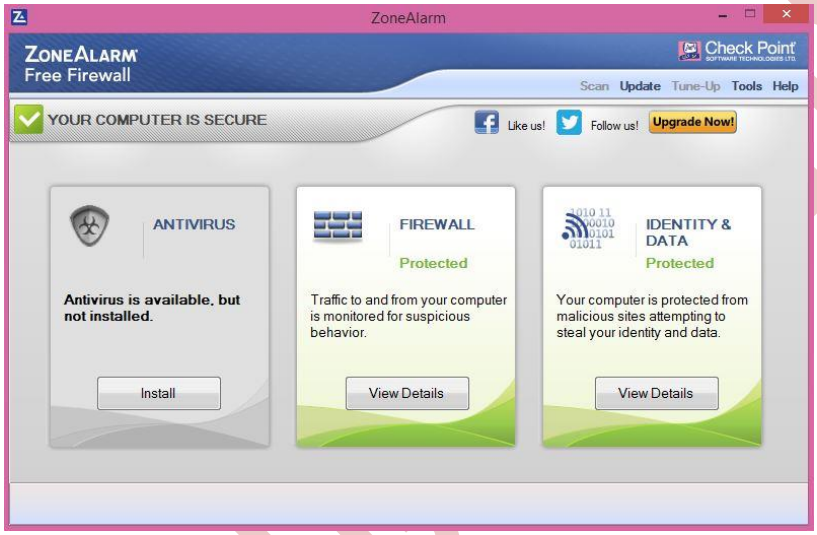
McAfee Host Intrusion Prevention for Desktops

http://www.mcafee.com

پس از معرفی ابزارهای مربوط به تشخیص نفوذ حال به ابزارهای فایروال و Honey pot می پردازیم.

فایروال Zone Alarm

این فایروال هم به صورت رایگان و هم به صورت پولی قابل بهره برداری است. شما می توانید این فایروال را به همراه آنتی ویروسی با همین نام نیز نصب نمایید. این نرم افزار از بروز برخی حملات جلوگیری نموده و ترافیک ها و رفتارهای مشکوک در سیستم شما را گزارش می دهد.



دیگر فایروال ها

اسامی ابزارهای کاربردی دیگر به عنوان فایروال را در زیر مشاهده نمایید.

Check Point Firewall Software Blade

http://www.checkpoint.com

eScan Enterprise

http://www.escanav.com

Jetico Personal Firewall

http://www.ietico.com

Outpost Security Suite

http://free.agnitum.com

Novell BorderManage

http://www.novell.com

Firewall UTM

http://www.esoft.com

Sonicwall

http://www.tribecaexpress.com

Comodo Firewall

http://personalfirewall.comodo.com

Online Armor

http://www.online-armor.com

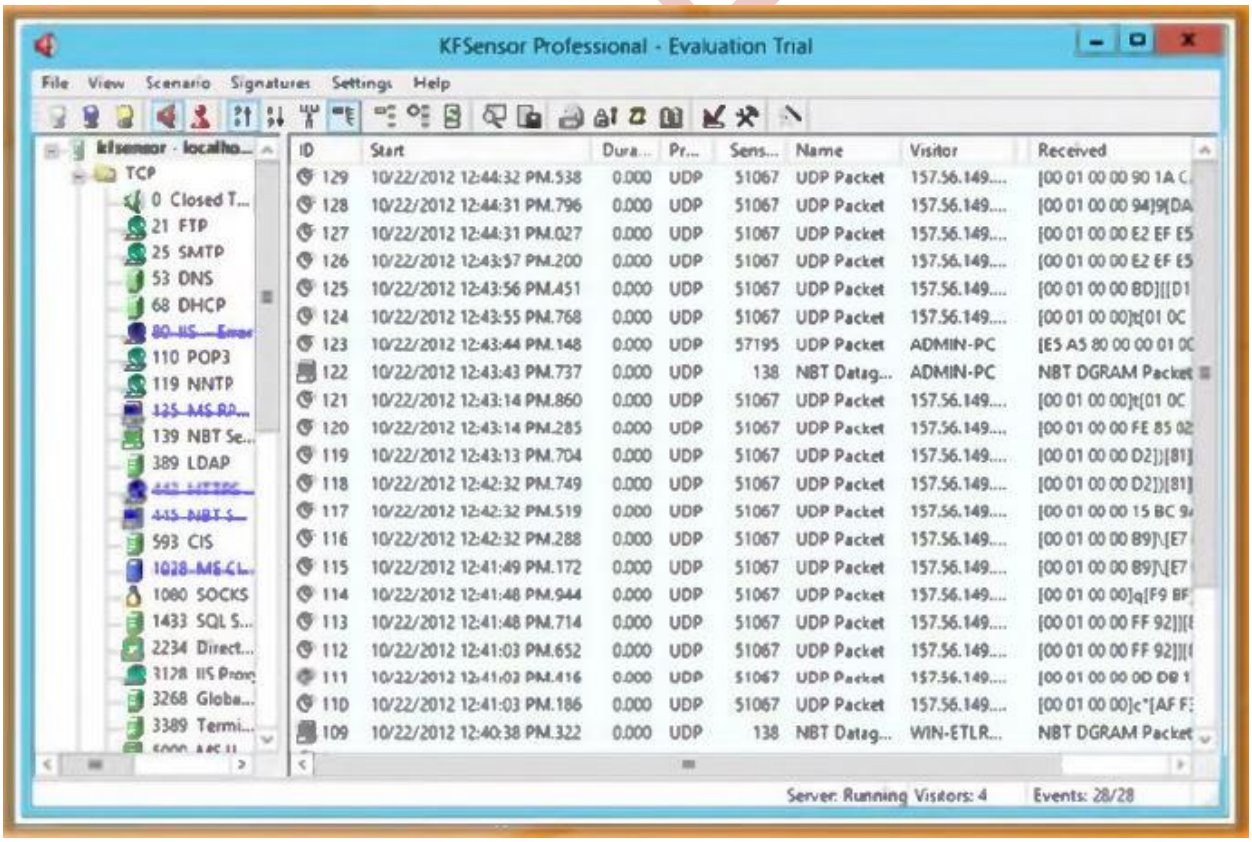
FortiGate-۵۱۰۱C

http://www.fortinet.com

ابزار KfSensor

این ابزار در واقع یک سیستم تشخیص نفوذ و Honey pot بوده که برای محیط های ویندوز طراحی شده است. این ابزار محیط آسیب پذیری را شبیه سازی نموده و به وسیله آن نفوذگر را به سمت خود هدایت نموده و مشخصات وی را ثبت می نماید. همچنین این ابزار دارای ویژگی های زیر می باشد.

- محیط گرافیکی
- مدیریت از راه دور
- سازگاری با امضا های Snort
- شبیه سازی پروتکل های شبکه ویندوزی
- خروجی رخداد ها در چندین فرمت مختلف



ابزار های دیگر Honey Pot

اسامی دیگر ابزارهای Honey pot به همراه سایت ارائه دهنده را در زیر مشاهده می نمایید.

specter

http://www.specter.com

LaBrea Tarpit

http://labrea.sourceforge.net

PatriotBox

http://www.alkasis.com

Koionev

http://koioney.sourceforge.net

HoneyBOT

http://www.atomicsoftwaresolutions.com

Google Hack Honeypot

http://ghh.sourceforge.net

WinHoneyd

http://www٢.netvigilance.com

HIHAT

http://hihat.sourceforge.net

Argos

http://www.few.vu.nl

Glastopf

http://glastopf.org

Send-Safe Honeypot Hunter

http://www.send-safe.com