معرفی نرم‌افزار Snort

قسمت اول : ویژگی‌های Snort

شهریور ۱۳۹۲

www.nsec.ir

۱- ۱ مقدمه

امنیت سیستم‌های کامپیوتری شامل محرمانگی، صحت اطلاعات و کنترل دسترسی است. تشخیص نفوذ عبارت است از کارهایی که برای شناخت و پاسخگویی به فعالیت‌های غیر مجاز، رفتارها و فعالیت‌هایی که منجر به خطر افتادن سه پارامتر اصلی ذکرشده در امنیت می‌شود.

سیستم تشخیص تهاجم[1] وقوع حملات کامپیوتری را گزارش می‌دهد. بنابراین هدف از تشخیص تهاجم این است که استفاده غیرمجاز، سوء استفاده و آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری توسط هر دو دسته‌ی کاربران داخلی و مهاجمان خارجی شناسایی شود. در یک سیستم کامل امنیتی در کنار استفاده از حفاظ‌ها، روش‌های مخفی‌سازی اطلاعات و هویت‌شناسی، که سعی می‌کنند از تهاجم جلوگیری کنند، از تشخیص تهاجم به عنوان دیواری برای محافظت از سیستم‌های کامپیوتری استفاده می‌شود.

IDSها عملاً سه وظیفه‌ی کلی را برعهده دارند : پویش، تشخیص، واکنش. هرچند که واکنش در موردIDS ها عموماً به ایجاد اخطار، در قالب‌های مختلف، محدود می‌گردد .هرچند دسته‌ای مشابه از ابزارهای امنیتی به نام Intrusion Prevention System (IPS) وجود دارند که پس از پویش و تشخیص، بسته[2]های حمله‌های احتمالی را حذف می‌کنند.

سیستم‌های تشخیص تهاجم را می‌توان در سه دسته مبتنی بر میزبان[3]، مبتنی بر شبکه[4] و مبتنی بر منابع ناهمگون[5] دسته‌بندی کرد.

در نوع مبتنی بر میزبان برای تحلیل از داده‌های جمع‌آوری شده در سطح سیستم‌عامل استفاده می‌کنند.این نوع IDS وظیفه تشخیص نفوذ و حملات به یک ماشین خاص را دارد .

نوع مبتنی بر شبکه شامل سیستم‌هایی است که ترافیک شبکه را به عنوان منبع اطلاعاتی مورد استفاده قرار داده‌اند.NIDSها در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌پذیرد می‌باشند. از آنجایی‌که NIDS ها تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گستردگی بیش‌تری داشته و فرایند تشخیص را به صورت توزیع‌شده انجام می‌دهند. با این وجود این سیستم‌ها در رویایی با بسته‌های رمزشده و یا شبکه‌هایی با سرعت و ترافیک بالا کارایی خود را از دست می‌دهند.

ناکافی بودن یک نوع منبع اطلاعاتی برای تشخیص تهاجم، سیستم‌های تشخیص تهاجم را به سمت استفاده از منابع اطلاعاتی ناهمگون سوق داد. این سیستم‌ها اطلاعات را هم از میزبان و هم از شبکه جمع آوری می‌کنند. سیستم‌های نسل سوم به سمت معماری توزیع شده پیش رفته‌اند(هم از حیث جمع آوری داده ها و هم از نظر تحلیل آنها). این سیستم‌ها را مبتنی بر عامل گویند.

Snort یک نرم‌افزار امنیتی پیشرفته است که توسط sourcefire توسعه داده می‌شود. این نرم‌افزار در سه حالت قابل برنامه‌ریزی می‌باشد، می‌تواند به عنوان یک sniffer برای بسته‌های شبکه، ثبت‌کننده بسته‌ها یا یک سیستم تشخیص نفوذ کامل مبتنی بر شبکه مورداستفاده قرار گیرد. در حالت اول این نرم‌افزار تنها محتوای بسته‌های ردوبدل شده بر روی شبکه را بر روی کنسول نمایش می‌دهد. در حالت ثبت‌کننده‌ی بسته‌ها، Snort اطلاعات بسته‌های شبکه را در پرونده‌ای که مشخص می‌شود ذخیره می‌کند.در نهایت در حالت سیستم تشخیص نفوذ، بر اساس دو قابلیت پیشین و با استفاده از قابلیت

[1] IDS
[2] Packet
3 HIDS: Host based IDS
[4] NIDS: Network based IDS
[5] DIDS: Distributed IDS

تحلیل بسته‌ها و قوانینی که تعیین می‌گردد، Snort امکان پویش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را بروز می‌دهد.

۲-۱ Snort چیست؟

امنیت سیستم‌های کامپیوتری شامل محرمانگی، صحت اطلاعات و کنترل دسترسی است. تشخیص نفوذ عبارت است از کارهایی که برای شناخت و پاسخگویی به فعالیت‌های غیر مجاز، رفتارها و فعالیت‌هایی که منجر به خطر افتادن سه پارامتر اصلی ذکرشده در امنیت می‌شود.

سیستم تشخیص تهاجم[6] وقوع حملات کامپیوتری را گزارش می‌دهد. بنابراین هدف از تشخیص تهاجم این است که استفاده غیرمجاز، سوء استفاده و آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری توسط هر دو دسته‌ی کاربران داخلی و مهاجمان خارجی شناسایی شود. در یک سیستم کامل امنیتی در کنار استفاده از حفاظ‌ها، روش‌های مخفی‌سازی اطلاعات و هویت‌شناسی، که سعی می‌کنند از تهاجم جلوگیری کنند به مانند نرم‌افزارهای معرفی شده در بخش‌های قبل، از تشخیص تهاجم به عنوان دیواری برای محافظت از سیستم‌های کامپیوتری استفاده می‌شود.

Snort یک سامانه کشف مزاحمت بازمتن[7] می باشد. علت محبوبیت Snort بازمتن بودن آن و قابل نصب بودن آن روی بسیاری از سیستم عامل ها می‌باشد. به‌راحتی می‌توان نسخه‌های متفاوتی از Snort را برای سیستم عامل‌های مختلف پیدا کرد و یا حتی ساخت. این سامانه توسط آقای Marty Roesch نوشته شده است.

بصورت خلاصه می‌توان گفت Snort یک packet sniffer[8] ، packet logger[9] و network IDS[10] می‌باشد. کار اصلی آن خواندن محتوای داخل هر بسته می‌باشد. با خواندن محتوای هر بسته‌ای که در شبکه ردوبدل می‌شود این سامانه می‌تواند محتویات بسته‌ها را با بانک قوانین حملات مطابقت دهد و در صورت مطابقت داشتن محتوای یک بسته با یک حمله اخطار دهد.

Snort یک نرم‌افزار امنیتی پیشرفته است که توسط sourcefire توسعه داده می‌شود.همانطورکه گفته شد این نرم‌افزار در سه حالت قابل برنامه‌ریزی می‌باشد، می‌تواند به عنوان یک شنودگر[8]برای بسته‌های شبکه، ثبت‌کننده بسته‌ها[9] یا یک سیستم تشخیص نفوذ[10] کامل مبتنی بر شبکه مورداستفاده قرار گیرد.

- در حالت اول این نرم‌افزار تنها محتوای بسته‌های ردوبدل شده بر روی شبکه را بر روی محیط کنسول نمایش می‌دهد.

- در حالت ثبت‌کننده‌ی بسته‌ها، Snort اطلاعات بسته‌های شبکه را در پرونده‌ای که مشخص می‌شود ذخیره می‌کند.

- در نهایت در حالت سیستم تشخیص نفوذ، بر اساس دو قابلیت پیشین و با استفاده از قابلیت تحلیل بسته‌ها و قوانینی که تعیین می‌گردد، Snort امکان پویش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را بروز می‌دهد.

---

[6] IDS (**Intrusion detection system**)
[7] Open Source
[8] Sniffer
[9] packet logger
[10] IDS (**Intrusion detection system**)

۳-۱ امکانات Snort

Snort از چهار مؤلفه اصلی زیر تشکیل شده است:

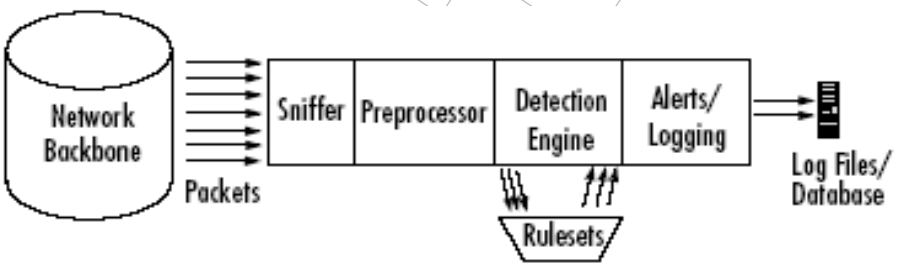
Sniffer

Preprocessor

Detection engine

Output

بسته‌ها از طریق Sniffer گرفته می شود به بخش Preprocessor ارسال می شوند. در بخش Preprocessor به ماهیت و محتوای هر بسته رسیدگی می‌شود. سپس در بخش Detection engine محتوای هر بسته با قوانین مطابقت داده می‌شود و بنا به نتیجه حاصل خروجی در بخش output به بیرون از سامانه ارسال می گردد. شکل ۱-۱ یک ساختار ساده از Snort که بیانگر این چهار مؤلفه می‌باشد را نشان می‌دهد.



شکل ۱-۱ ساختار ساده‌ای از Snort

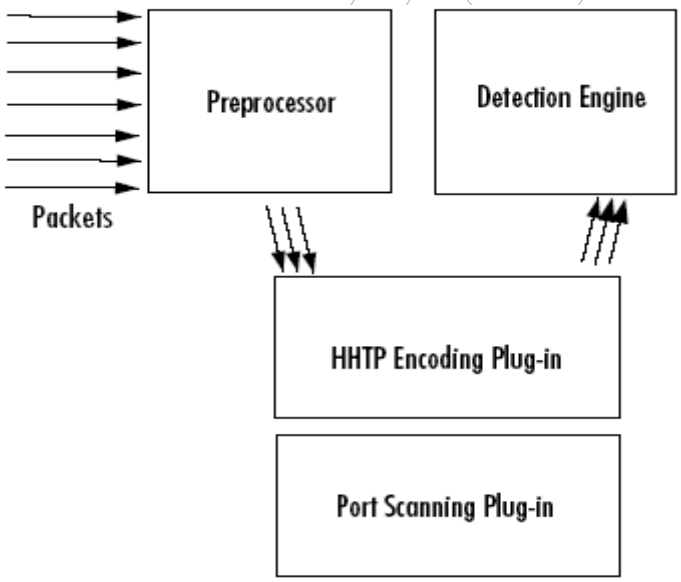
سه بخش Preprocessor , Detection engine و output دارای قابلیت plug-ins می باشد. Plug ها برنامه‌های کوچکی هستند که بخش های از کد هسته Snort را تشکیل می‌دهند به‌راحتی قابل تغییر، حذف و یا اضافه کردن هستند. این قابلیت Snort انعطاف‌پذیری فوق العاده‌ای به آن داده است.

Packet Sniffer ۱-۳-۱

Packet Sniffer یک وسیله سخت افزاری یا نرم‌افزاری می باشد که روی خطوط شبکه استراق سمع می‌کند و بسته‌ها را می‌خواند. از آنجایی که بسته ها با پروتکل‌های مختلفی روی خطوط شبکه درحال نقل و انتقال می‌باشد این وسیله توانایی تحلیل بسته‌هایی باتوجه به پروتکل خاص آن را داراست. این وسایل برای تحلیل شبکه و مشکل زدای آن، محک زدن شبکه و حتی بدست آوردن کلمات عبور رمزنگاری نشده مورد استفاده قرار می‌گیرند.

Preprocessor ۲-۳-۱

Preprocessor بسته‌های خام را از قسمت Sniffer دریافت می‌کند و آنها را توسط چند Plug-in مطابقت می‌دهد. این Plug-in ها رفتارهای خاصی از بسته‌ها را مورد آزمایش قرار می‌دهند. اگر یک بسته رفتار خاصی را داشت به قسمت بعدی یعنی Detection Engine ارسال می‌شود.



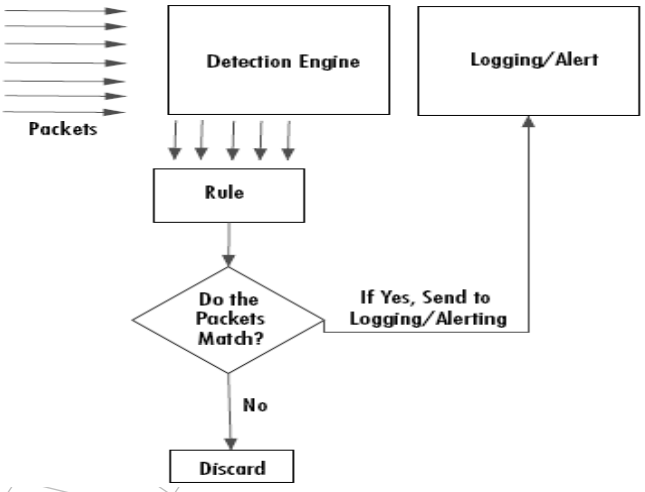
شکل ۱-۲ Preprocessor در Snort

Detection Engine ۳-۳-۱

این قسمت بسته‌های رسیده از مرحله قبل را دریافت و پس از مطابقت دادن آن‌ها با قوانیین موجود در صورتی که بسته‌ای با قانونی مطابقت داشت قسمت اخطاردهنده را آگاه می‌سازد. نوشتن قوانین مناسب برای Snort یکی از مهم‌ترین بخش‌های تنظیم کردن این سامانه است. این قوانین شکل خاص خود را دارند.

اخطار دهنده ۴-۳-۱

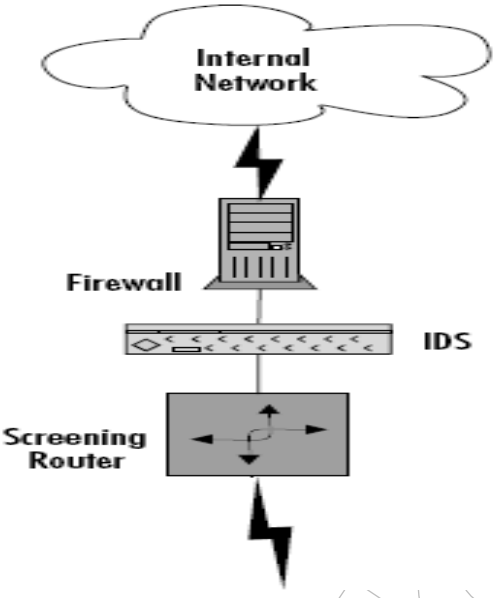
اگر بسته‌ای از بخش قبل با یکی از قوانین همخوانی داشت این بخش فراخوانده می‌شود تا زنگ اخطار را فعال کند. این اخطار شامل ذخیره اطلاعات در فایل Log یا بانک اطلاعاتی، فرستادن پیغام از طریق شبکه باشد.



شکل ۱-۳ قسمت اخطار دهنده در Snort

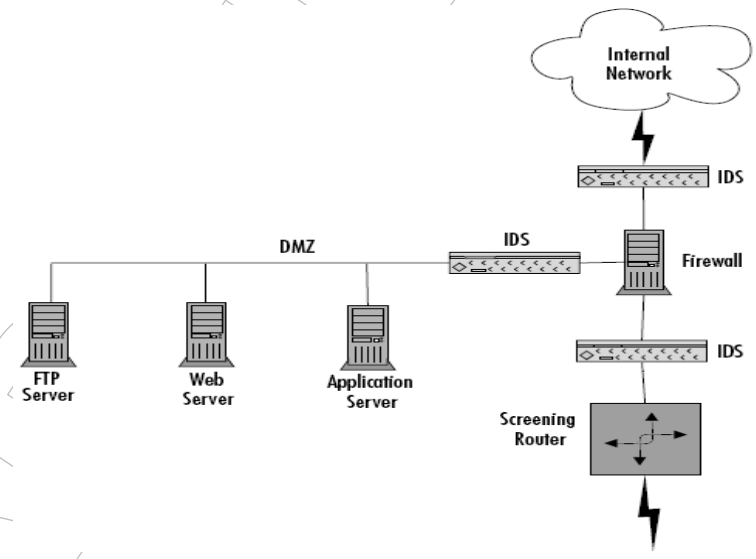
Snort ۴-۱ و ساختار شبکه

این سوال پیش می آید که محل قرار گیری سامانه کشف مزاحمت در کجای شبکه است؟ بهترین جای قرار گیری این سامانه ها بین دیواره آتش و مسیر یاب شبکه می باشد. اگر IDS در محل بین دیواره آتش و شبکه بیرونی (اینترنت) قرار بگیرد ممکن است خطاهای بسیاری را شامل شود و حجم کار بسیار زیادی روی سامانه IDS وارد نماید. شکل۱-۴ نمونه محل مناسبی از قرار گیری سامانه IDS می باشد.



شکل ۱-۴ محل مناسب قرار گیری سامانه کشف مزاحمت در شبکه

برای شبکه های DMZ که از یک extranet برای سرویس دهنده‌هایی چون Web, FTP, Application استفاده می‌کنند بهترین ساختار پیاده سازی سامانه کشف مزاحمت در شکل۱-۵ به نمایش گذاشته شده است.



شکل ۱-۵ پیاده سازی سامانه کشف مزاحمت در DMZ

بصورت کلی برای یک شبکه دلخواه محل قرار گیری این سامانه‌ها باید بصورت زیر باشد:

یکی در داخل مسیر یاب

برای هر زیر شبکه یک سامانه کشف مزاحمت قرار بگیرد.

۱-۵ ضعف های Snort

Snort یک ابزار بسیار قوی می‌باشد اما همانند ابزار های دیگر با مشکلاتی روبروست این مشکلات عبارتند از:

- جمع آوری نکردن کلیه بسته‌ها :

این ایراد بیشتر زمانی اتفاق می‌افتد که سرعت شبکه با سامانه‌ای که Snort روی آن قرار دارد یکی نباشد.

- اخطار درست ندادن :

بسیاری از اوقات وقتی این سامانه با تنظیمات پیش فرض نصب می شود این ایراد اتفاق می افتد. در این حالت حمله ای روی شبکه اتفاق می افتد در صورتی که Snort از آن بی اطلاع است.

- اخطار غلط دادن :

بسیاری از اوقات وقتی این سامانه با تنظیمات پیش فرض نصب می شود این ایراد اتفاق می افتد. در این حالت بدون ایجاد حمله ای Snort اخطار می دهد.