



دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

مقطع: کارشناسی

گرایش: نرم افزار

راهنمای راه اندازی و نصب Snort

فروردین ۱۳۹۹

صفحه

فهرست مطالب

بخش اول آشنایی با IDS ها.....	۳
بخش اول دریافت و نصب Snort.....	۵
بخش سوم پیکره‌بندی.....	۸
بخش چهارم تست و اجرا.....	۱۳
بخش پنجم استفاده از Snort به عنوان IPS.....	۱۷

بخش اول

آشنایی با IDS ها

IDS^۱ دستگاه‌ها یا ابزارهای نرم‌افزاری هستند که یک شبکه یا یک سیستم را به منظور تشخیص فعالیت‌های مخرب و یا نقض کننده پالیسی‌ها، مانیتور می‌کنند. یکی از قدرتمندترین IDS ها Snort می‌باشد. در این گزارش سعی در نصب و راه‌اندازی این IDS داریم. این ابزار هم می‌تواند به عنوان یک IPS^۲ (در حالت اجرای inline) و هم به عنوان یک IDS مورد استفاده قرارگیرد. این ابزار از ruleهای زیادی بهره‌مند می‌باشد و همچنین این قابلیت وجود دارد که به صورت دستی برای آن Rule تعیین کرد. توضیحات بیشتر درمورد انواع Rule ها و ساختار آن‌ها در ادامه توضیح داده خواهد شد.

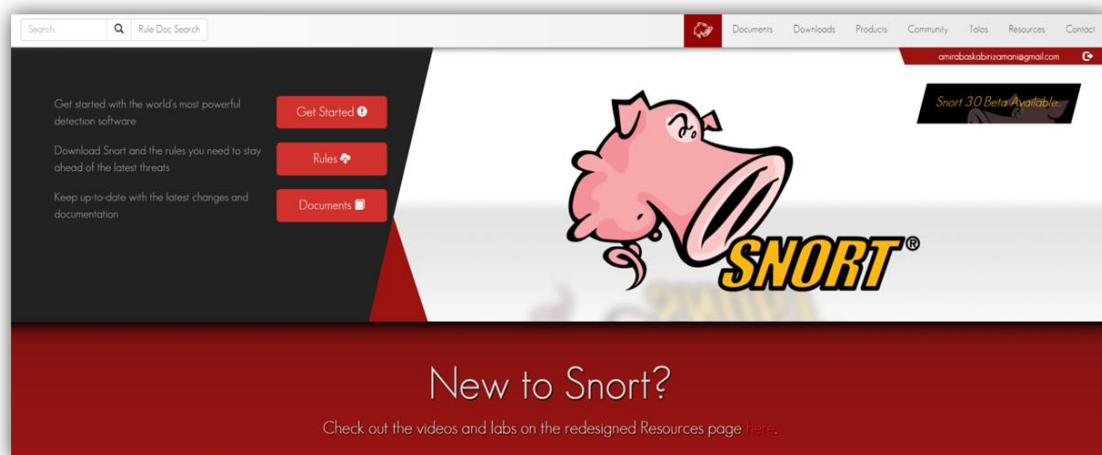
^۱ Intrusion Detection Systems

^۲ Intrusion Prevention System

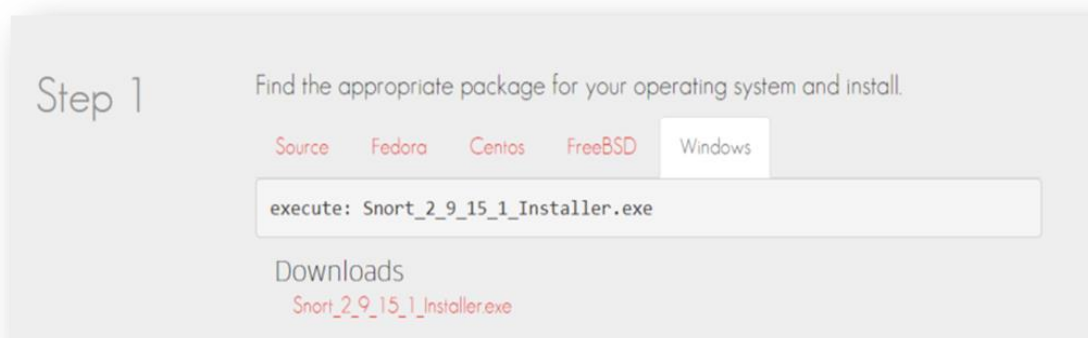
بخش اول

دریافت و نصب Snort

برای استفاده از Snort، ابتدا فایل نصب آن را از وب سایت snort.org دریافت می کنیم. بدین منظور از طریق مرورگر وارد سایت اصلی Snort می شویم:



وب سایت دارای رابط کاربری ساده ای می باشد، لذا برای استفاده از آن کافیسست به بخش Get Started! بروید. پس از بارگزاری صفحه مورد نظر، از قسمت Step 1 نسخه مرتبط با سیستم عامل خود را دریافت کنید.



همانطور که قابل مشاهده است، Snort برای سیستم عامل های مختلف موجود می باشد، در اینجا ما نسخه ویندوز را انتخاب و دریافت می کنیم.

پس از دریافت فایل نصب Snort، نیاز به دریافت فایل مربوط به Rule ها داریم. Rule ها متدولوژی های متفاوتی هستند که برای اجرای Snort به کار گرفته می شوند.

به طور کلی ۳ نوع Rule برای Snort قابل دریافت است، که همگی آن ها از صفحه اصلی وب سایت قابل دریافت می باشند. بدین منظور از طریق صفحه اصلی وب سایت وارد بخش Rules می شویم. دسته بندی Rule ها به صورت زیر می باشد:

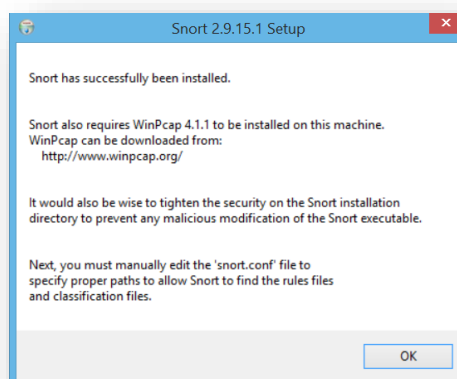
نسخه Community: این نسخه نیاز به ثبت نام در سایت و ساختن حساب کاربری ندارد.

نسخه Registered: این نسخه نیاز به ثبت نام در وب سایت دارد. ساخت حساب در وب سایت Snort رایگان می باشد.

نسخه Subscriber: این نسخه از دیگر نسخه ها کامل تر بوده و نیاز به ثبت نام و هم چنین پرداخت هزینه دارد.

تفاوت نسخه Subscriber و Registered در دریافت بروزرسانی ها می باشد. بدین صورت که نسخه Subscriber بر خلاف نسخه Registered بلافاصله بروزرسانی ها را دریافت می کند. توجه داشته باشید که ساختار هر دو نسخه یکسان می باشد و تنها تفاوت در زمان دریافت بروزرسانی ها می باشد.

پس از دریافت نسخه مورد نظر، نوبت به نصب Snort و تعریف Rule ها برای آن می باشد. فایل Snort_۲_۹_۱۵_۱_Installer را باز و نصب می کنیم. در انتها با پیامی مواجه می شویم که از ما می خواهد برای اجرای Snort، WinPcap که یک ابزار استراق سمع شبکه می باشد، را نیز نصب کنیم. بدین منظور WinPcap را از اینترنت دریافت و نصب کنید.



بخش سوم

پیکره بندی

برای پیکره‌بندی و راه‌اندازی Snort ابتدا Rule‌های دریافت شده از وب سایت را در مسیر زیر که فولدر rules در محل نصب Snort می‌باشد، قرار دهید:

~\Snort\rules

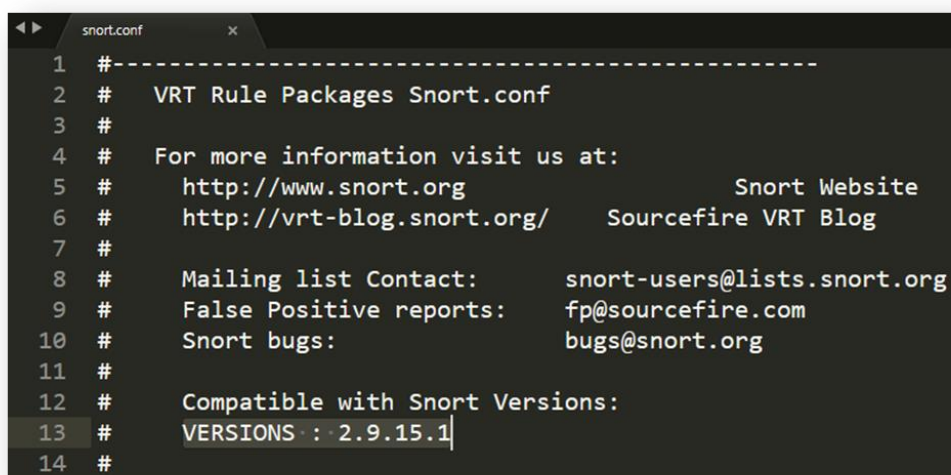
برای اینکار فایل snortrules-snapshot-xxxxx.tar را از حالت فشرده خارج و کپی کنید. حال شما تعدادی Rule در اختیار دارید که می‌توانید از آن‌ها برای اجرای Snort استفاده کنید. برای مثال local.rules یک Rule می‌باشد که می‌توانید درون آن یک Rule جدید و شخصی بنویسید. سپس به مسیر زیر رفته و محتویات preproc_rules را در آن کپی و جایگزین^۳ کنید:

~\Snort\preproc_rules

فایل‌ها میبایست جایگزین شوند چرا که باید از بروز بودن آن‌ها اطمینان داشته باشیم.

در مرحله بعد میبایست مسیر Rule‌ها را برای Snort تعریف کنیم تا بتواند از آن مسیر Rule‌ها و PreprocRule‌ها را بخواند. بدین منظور در مسیر نصب Snort به پوشه etc رفته و فایل snort.conf را به وسیله یک ویرایشگر متن باز می‌کنیم. در این مرحله می‌بایست تغییراتی در این فایل پیکره‌بندی انجام دهیم تا Snort بدون خطا اجرا شود.

در قسمت ابتدایی این فایل اطلاعاتی کلی نظیر نسخه فعلی Snort قابل مشاهده است:



```
1 #-----
2 #   VRT Rule Packages Snort.conf
3 #
4 #   For more information visit us at:
5 #       http://www.snort.org           Snort Website
6 #       http://vrt-blog.snort.org/     Sourcefire VRT Blog
7 #
8 #   Mailing list Contact:      snort-users@lists.snort.org
9 #   False Positive reports:   fp@sourcefire.com
10 #   Snort bugs:              bugs@snort.org
11 #
12 #   Compatible with Snort Versions:
13 #   VERSIONS : 2.9.15.1
14 #
```

در ادامه می‌بایست متغیر HOME_NET را می‌توانیم با متغیر any رها کنیم و یا مطابق با محدوده IP شبکه فعلی تغییر دهیم، برای مثال:

```
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 192.168.1.0/24
```

اکثر مسیرهایی که به‌صورت پیش‌فرض در Snort وجود دارد طبق دیرکتوری‌های Linux/UNIX نوشته شده‌است، لذا در صورت نصب Snort بروی ویندوز، می‌بایست این مسیرها را اصلاح کنیم. اولین مسیر که می‌بایست اصلاح شود، مسیر Rule ها و PreprocRule ها می‌باشد:

```
104 var RULE_PATH C:\Snort\rules
105 #var SO_RULE_PATH ../so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

مسیرها را مطابق با شکل بالا تغییر می‌دهیم، به این صورت که مسیر دقیق^۴ و نه نسبی^۵ را تعریف می‌کنیم. در صورت استفاده از ویندوز باید قبل از متغیر SO_RULE_PATH یک # به معنی کامنت بودن این خط قرار دهیم چرا که این آپشن در ویندوز فعال نیست.

برای اجرای صحیح Snort و مواجهه نشدن با ارور در هنگام تست و اجرا، به متغیرهای BLACK_LIST_PATH و WHITE_LIST_PATH مقدار c:\snort\rules را بدهید. در آینده می‌توانید به صورت واقعی برای Snort لیست تهیه کنید. در حال حاضر، دو فایل white.list و black.list را درون مسیر مذکور ایجاد کنید. در حال حاضر این فایل‌ها را بدون محتوا رها کنید.

بعد از تعریف مسیر Rule ها نوبت به تعریف کتابخانه‌های مورد نیاز می‌باشد. با توجه به شکل زیر مسیرها را تعریف کنید:

^۴ Absolute Path

^۵ Relative

```

246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/
248
249 # path to base preprocessor engine
250 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
251
252 # path to dynamic rules libraries
253 #dynamicdetection directory C:\Snort\lib\snort_dynamicpreprocessor

```

از آنجا که اجرای inline در نسخه ویندوزی Snort موجود نمی‌باشد، برای جلوگیری از بروز مشکل خطوط زیر را به وسیله # کامنت می‌کنیم:

```

263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 #preprocessor normalize_ip4
266 #preprocessor normalize_tcp: ips ecn stream
267 #preprocessor normalize_icmp4
268 #preprocessor normalize_ip6
269 #preprocessor normalize_icmp6

```

دو فایل white.list و black.list را که پیش‌تر ایجاد کردیم در قسمت زیر مشخص می‌کنیم:

```

511 whitelist $WHITE_LIST_PATH/white.list, \
512 blacklist $BLACK_LIST_PATH/black.list

```

در قسمت زیر می‌توانید Rule‌هایی را مشاهده کنید که برای Snort تعریف شده‌اند، بنابراین اگر قصد اضافه کردن Rule جدیدی را دارید، می‌بایست در این قسمت include کنید. هم‌چنین در صورتی که از ویندوز استفاده می‌کنید، می‌بایست backslash‌ها را با slash‌ها جابجا کنید تا مسیرها به مسیرهای معتبر برای ویندوز تبدیل شوند:

```

545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/app-detect.rules
549 include $RULE_PATH/attack-responses.rules
550 include $RULE_PATH/backdoor.rules
551 include $RULE_PATH/bad-traffic.rules
552 include $RULE_PATH/blacklist.rules
553 include $RULE_PATH/botnet-cnc.rules

```

```

223 include $RULE_PATH/rofu-cnc.rules
225 include $RULE_PATH/rtack.rules

```

در نهایت، در بخش زیر، ruleهای preprocessor را از حالت کامنت خارج کنید:

```

658 # decoder and preprocessor event rules
659 include $PREPROC_RULE_PATH/preprocessor.rules
660 include $PREPROC_RULE_PATH/decoder.rules
661 include $PREPROC_RULE_PATH/sensitive-data.rules

```

بخش چهارم

تست و اجرا

در این قسمت تلاش خواهیم کرد با اجرای Snort به وسیله فلگ T، پیکره‌بندی را مورد آزمون قرار داده و از عملکرد صحیح آن مطلع شویم. بدین منظور ابتدا یک صفحه CMD را در حالت Run as administrator باز کرده و پس از وارد مسیر C:\Snort\bin~ می‌شویم. ابتدا با زدن دستور زیر لیست آداپتورهای موجود در سیستم را دریافت می‌کنیم:

```
C:\Snort\bin>snort -W

-~> Snort! <~-
o"~)~
....

Version 2.9.15.1-WIN32 GRE (Build 15104)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

-----
Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:6196:bc5d \Device\NPF_{0D822072-6911-4B95-976F-78FAD317A0F2}
2      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:a5af:a5cf \Device\NPF_{5E42335B-2B33-48BD-A81F-0648131FCD98}
3      00:FF:02:3E:6F:FD      0000:0000:fe80:0000:0000:0000:34c3:3263 \Device\NPF_{023E6FFD-E7DF-4D0F-B8DE-C1170978D98C}
4      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:fc9f:9cf8 \Device\NPF_{FD36BD5B-F846-4BA4-B7C1-7A795986190C}
5      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:4d71:1ef6 \Device\NPF_{93E7206A-8565-40BD-A6FC-E8DF6C523A8D}
6      00:FF:34:5B:89:F4      0000:0000:fe80:0000:0000:0000:191e:fab4 \Device\NPF_{345B89F4-55B3-4921-B45A-01B32825D53}
7      78:24:AF:C9:03:12      0000:0000:fe80:0000:0000:0000:fda0:eb0a \Device\NPF_{3129AE43-0FFD-42F3-B6C9-3C7BF3DF928E}
8      44:45:53:54:4F:53      0000:0000:fe80:0000:0000:0000:6d04:fb48 \Device\NPF_{4431C003-F7F9-4B1B-8FE4-8FB5C7607C7D}
9      00:FF:E1:56:63:D6      0000:0000:fe80:0000:0000:0000:b082:686a \Device\NPF_{E15663D6-324F-450A-9CD9-7A465A1FF27C}
10     00:FF:36:21:1D:AB      0000:0000:fe80:0000:0000:0000:4171:4e96 \Device\NPF_{36211DAB-A9E3-4F91-97A6-743AA3FBD958}
```

برای مثال در سیستم شکل بالا، ۱۰ آداپتور موجود می‌باشد. حال نوبت به تست فایل پیکره‌بندی می‌باشد. با زدن دستور زیر فایل پیکره‌بندی را بر روی Interface انتخابی تست می‌کنیم:

```
C:\Snort\bin>snort -i 7 -c c:\Snort\etc\snort.conf -T
```

که در اینجا، فلگ i برای انتخاب Interface موردنظر است. عدد روبروی فلگ i شماره Index آداپتوری است که می‌خواهیم تست بر روی آن انجام شود. این شماره از خروجی دستور قبلی قابل مشاهده است. نکته مهمی که می‌بایست به آن توجه کنید، انتخاب صحیح شماره ایندکس مربوطه می‌باشد. در صورت نیاز می‌توانید از تنظیمات سیستم خود، Interface‌های دیگر را غیرفعال و دستور Snort -W را بار دیگر اجرا کنید. در نهایت، اگر پس از اجرای دستور بالا با پیام زیر روبرو شدید، تنظیمات با موفقیت انجام شده است.

```
Snort successfully validated the configuration!
Snort exiting
```

حال، به عنوان مثال می‌خواهیم یک Rule برای Snort بنویسیم و از آن استفاده کنیم. فایل local.rules را از مسیر \Snort\rules~ باز کرده و خط زیر را در آن اضافه کنید:

```
alert icmp any any -> $HOME_NET any (msg:"An attempt for ping"; sid:۱۰۰۰۰۰۱;  
rev:۱; classtype:icmp-event;)
```

این Rule در صورت Ping شدن سیستم توسط دیگران، به ما هشدار می‌دهد. این Rule از اجزای زیر تشکیل شده:

Alert: به معنای این است که سیستم در صورت اتفاق افتادن رویدادی که تعریف می‌کنیم هشدار بدهد.
Icmp: پروتکلی است که به هنگام ping کردن از آن استفاده می‌شود.

Arrow: در سمت چپ فلش IP و پورت مبدا و در سمت راست آن IP و پورت مقصد انتخاب می‌شود.
در اینجا ما IP و پورت مبدا را any و IP مقصد را از متغیر HOME_NET انتخاب کرده‌ایم.

Msg: پیامی است که به هنگام به وقوع پیوستن رخداد موردنظر، بر روی سیستم نمایش داده می‌شود.

Sid: مخفف Snort Rule ID می‌باشد که تا عدد ۱۰۰۰۰۰۰ آن رزرو شده است به همین دلیل است که ما عددی بزرگتر از آن را انتخاب کرده‌ایم.

Rev: یک آپشن است که برای نگهداری و استفاده از rule کاربرد دارد. به وسیله این شماره می‌توانید Rule را در دیگر بخش‌ها راحت‌تر فراخوانی کنید.

Classtype: اتفاقی است که می‌خواهید سیستم در صورت وقوع آن واکنش نشان بدهد.

حال یک دستور زیر را در CMD که در حالت Run as Administrator باز شده و در مسیر \snort\bin قرار دارد بزنید:

```
C:\Snort\bin>snort.exe -i 1 -c c:\Snort\etc\snort.conf -q -A console
```


به وسیله دستور snort -help می‌توانید راهنمای فلگ‌های Snort و مقادیر ممکن برای آن‌ها را مشاهده کنید. در اینجا فلگ -A به معنای Alarm Mode و فلگ -q برای نشان ندادن گزارشات می‌باشد. بعد از اجرای دستور بالا سیستم فعال می‌شود. (برنامه بدون دادن ارور، در حالت Listen قرار می‌گیرد.) حال می‌بایست از طریق یک سیستم داخل شبکه، سیستم خود را Ping کنیم. این سیستم می‌تواند یک کامپیوتر، تلفن همراه و یا یک ماشین مجازی باشد. در اینجا از ماشین مجازی استفاده می‌کنیم:

```
root@kali:~# ping 192.168.1.36
PING 192.168.1.36 (192.168.1.36) 56(84) bytes of data.
64 bytes from 192.168.1.36: icmp_seq=1 ttl=128 time=0.467 ms
64 bytes from 192.168.1.36: icmp_seq=2 ttl=128 time=0.748 ms
64 bytes from 192.168.1.36: icmp_seq=3 ttl=128 time=0.693 ms
64 bytes from 192.168.1.36: icmp_seq=4 ttl=128 time=0.529 ms
64 bytes from 192.168.1.36: icmp_seq=5 ttl=128 time=0.730 ms
64 bytes from 192.168.1.36: icmp_seq=6 ttl=128 time=0.839 ms
64 bytes from 192.168.1.36: icmp_seq=7 ttl=128 time=0.699 ms
64 bytes from 192.168.1.36: icmp_seq=8 ttl=128 time=0.793 ms
64 bytes from 192.168.1.36: icmp_seq=9 ttl=128 time=0.809 ms
64 bytes from 192.168.1.36: icmp_seq=10 ttl=128 time=0.783 ms
```

سپس به سیستم خود رفته و شاهد هشدار سیستم ما به دلیل Ping شدن از سمت دیگران هستیم:

```
C:\Snort\bin>snort.exe -i 1 -c c:\Snort\etc\snort.conf -q -A console
03/31-20:12:14.385247 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:15.416004 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:16.418182 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:17.424059 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:18.448948 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:19.472586 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:20.473681 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:21.487762 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:22.512381 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
03/31-20:12:23.512606 ** [1:1000001:1] An attempt for ping ** [Classification: Generic ICMP event] [Priority: 3] (ICMP) 192.168.1.37 -> 192.168.1.36
```


بخش پنجم

استفاده از Snort به عنوان IPS

در این بخش می‌خواهیم به بحث IPS بپردازیم. اسنورت می‌تواند علاوه بر IDS، به عنوان یک IPS^۶ نیز عمل کند. به بیان ساده، اسنورت در این حالت علاوه بر اینکه ما را از رویدادهایی که برای آن تعریف کرده‌ایم با خبر می‌سازد، می‌تواند جلوی آن‌ها را نیز بگیرد. برای مثال، می‌توانیم از اسنورت بخواهیم که در صورت وارد شدن پکت ICMP به سیستم، علاوه بر اینکه ما را از آن با خبر می‌کند، جلوی آن را نیز بگیرد و اصطلاحاً پکت‌ها را Drop کند. در این صورت گوییم اسنورت در حالت Inline کار می‌کند.

همانطور که پیش‌تر گفتیم، مود Inline در نسخه ویندوزی اسنورت موجود نمی‌باشد. بنابراین پس از نصب اسنور بر روی یک سیستم لینوکسی و پیکره‌بندی آن (پیکره‌بندی مطابق با محتویات گزارش) نیاز به نصب چند Dependency داریم. لیست پکیج‌های این Dependency‌ها می‌توانید از طریق `apt-get install` آن‌ها را نصب کنید، به صورت زیر می‌باشد:

Libdnet

Build-essential

Bison flex

Libpcap-dev

Libpcap3-dev

Libnet1-dev

Zlib1g-dev

Libnetfilter-queue-dev

Libmnl-dev

Libnfnetlink-dev

بنابراین تمامی این پکیج‌ها را نصب می‌کنیم:

```
debian@debian10: ~
File Edit View Search Terminal Help
debian@debian10:~$ sudo su -
root@debian10:~# apt-get install libdnet && apt-get install build-essential && apt-get install bison flex && apt-get install libpcap-dev && apt-get install libpcap-dev && apt-get install libnet1-dev && apt-get install zlib1g-dev && apt-get install libnetfilter-queue-dev # daq: nfq && apt-get install libmnl-dev && apt-get install libnfnetlink-dev && apt-get install libnetfilter_queue-dev
```

توجه کنید که ابتدا باید در مود سوپریوزر از لینوکس قرار داشته باشید.

بعد از اتمام نصب پیش‌نیازها آخرین نسخه DAQ و Libdnet را از سایت مرجع دانلود کنید:

DAQ: snort.org → Downloads → Sources → daq-xxx.tar.gz

Libdnet → <http://libdnet.sourceforge.net>

سپس وارد فایل پیکره‌بندی اسنورت یعنی snort.conf شده (در لینوکس: /etc/snort/snort.conf) و بخش مربوط به daq را جست‌وجو کنید:

```
# Configure DAQ related options for inline operation. For more information, see README.daq
#
# config daq: <type>
# config daq_dir: <dir>
# config daq_mode: <mode>
# config daq_var: <var>
#
# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ>
```

همانطور که مشاهده می‌کنید، این تنظیمات کامنت بوده و غیرفعال می‌باشد. خطوط زیر را به منظور فعال‌سازی و تنظیم daq وارد می‌کنیم:

```
# Configure DAQ related options for inline operation. For more information, see README.daq
#
config daq_dir: /home/debian/Downloads/daq-2.0.7
config daq:afpacket
config daq_mode:inline
```

در اینجا daq یک لایه بر روی libpcap ایجاد می‌کند کار کردن و عملیات بر روی تعداد زیادی اینترفیس مجازی یا فیزیکی را راحت می‌کند. Libpcap نیز عملیات شبکه‌ای پکت‌ها را انجام می‌دهد.

پس از کانفیگ daq، حال نوبت به استفاده از این قابلیت می‌رسد. برای مثال، نمونه Rule که پیش‌تر در این گزارش برای هشدار دادن به هنگام فرارسیدن پکت ICMP نوشتیم را به صورت زیر تغییر می‌دهیم:

```
debian@debian10: ~  
File Edit View Search Terminal Help  
GNU nano 3.2 /etc/snort/rules/local.rules  
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
# -----  
# LOCAL RULES  
# -----  
# This file intentionally does not come with signatures. Put your local  
# additions here.  
drop icmp any any -> $HOME_NET any (msg:"An attempt for ping"; sid:1000001; rev:1; classtype:icmp-event;)
```

تنها دستور alert به drop تغییر پیدا کرده است. زین پس، بسته‌های ورودی ICMP، نه تنها توسط اسنورت شناسایی می‌شوند بلکه از ورود آن‌ها جلوگیری نیز می‌شود.