

Deteksi dan mencegah intrusi pada jaringan dengan Suricata

Oleh:

Henry Saptono <boypyt@gmail.com>

Intrusion detection system bukanlah hal yang baru, banyak yang telah melakukannya. Mobil dengan alarm pencurian, gedung gedung dengan pendeteksi kebakaran, rangkaian listrik dengan pendeteksi hubungan singkat dan lain lain. Tujuan dari *intrusion detection system* adalah melakukan upaya pendeteksian adanya gangguan atau ancaman terhadap suatu system sehingga diharapkan kemungkinan terjadinya kegagalan fungsi system tersebut dapat sedini mungkin dicegah.

Dalam tulisan ini penulis akan menjelaskan instalasi dan penerapan sederhana perangkat lunak pendeteksian gangguan atau yang lebih dikenal dengan istilah *intrusion detection system* terhadap komputer dan jaringan menggunakan perangkat lunak free dan open source yang berjalan pada sistem operasi linux ubuntu 10.04. Salah satu perangkat lunak *intrusion detection system* yang dapat digunakan pada sistem linux secara bebas adalah perangkat lunak Suricata (<http://www.openinfosecfoundation.org>)

Suricata

Suricata adalah perangkat lunak pendeteksi dan pencegah intrusi (*Intrusion Detection and Prevention System*) open source yang merupakan generasi berikutnya dari perangkat perangkat IDS/IPS yang ada saat ini yang tidak sekedar dimaksudkan untuk hanya menggantikan atau meniru perangkat perangkat yang ada di industri, tetapi akan membawa ide-ide dan teknologi baru. Suricata dirilis oleh OISF (<http://openinfosecfoundation.org/>). Dan suricata dapat Anda unduh dari link ini <http://openinfosecfoundation.org/download/suricata-1.0.1.tar.gz>.

Suricata dapat menggunakan rule rule yang biasa digunakan oleh perangkat lunak snort IDS. Jadi jika Anda sebelumnya menggunakan Snort dan untuk beralih menggunakan Suricata tidak perlu susah payah membuat atau mencari rule baru cukup menggunakan rule yang telah ada.

Instalasi Suricata

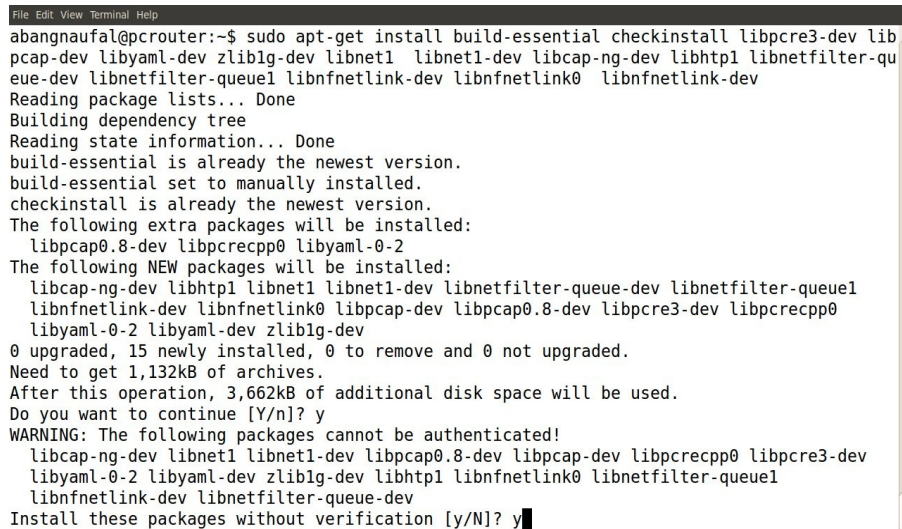
Setelah Anda mengunduh suricata versi terbaru saat ini (sampai penulis menulis artikel ini suricata versi terbaru adalah [suricata-1.0.1.tar.gz](http://openinfosecfoundation.org/download/suricata-1.0.1.tar.gz)). Maka langkah berikutnya adalah menginstal suricata. Dalam proses instalasi ini penulis akan menggunakan tools checkinstall (*installation tracker*) sebagai upaya untuk menghasilkan paket binary debian (.deb) dari perangkat lunak suricata agar proses instal dan uninstal suricata nantinya cukup mudah.

Sebelum melakukan instalasi suricata ada beberapa paket perangkat lunak dan pustaka yang semestinya

sudah terinstal pada sistem linux. Jika paket perangkat lunak dan pustaka tersebut belum terinstall maka lakukan instalasi dengan perintah berikut:

```
abangnaufal@pcrouter:~$ sudo apt-get install build-essential checkinstall libpcre3-dev libpcre3-dev libpcap-dev libyaml-dev zlib1g-dev libnet1 libnet1-dev libcap-ng-dev libhtp1 libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0
```

Ilustrasi perintah diatas dapat juga Anda lihat pada gambar berikut:



```
File Edit View Terminal Help
abangnaufal@pcrouter:~$ sudo apt-get install build-essential checkinstall libpcre3-dev lib
pcap-dev libyaml-dev zlib1g-dev libnet1 libnet1-dev libcap-ng-dev libhtp1 libnetfilter-qu
eue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0 libnfnetlink-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version.
build-essential set to manually installed.
checkinstall is already the newest version.
The following extra packages will be installed:
  libpcap0.8-dev libpcrecpp0 libyaml-0-2
The following NEW packages will be installed:
  libcap-ng-dev libhtp1 libnet1 libnet1-dev libnetfilter-queue-dev libnetfilter-queue1
  libnfnetlink-dev libnfnetlink0 libpcap-dev libpcap0.8-dev libpcre3-dev libpcrecpp0
  libyaml-0-2 libyaml-dev zlib1g-dev
0 upgraded, 15 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,132kB of archives.
After this operation, 3,662kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  libcap-ng-dev libnet1 libnet1-dev libpcap0.8-dev libpcap-dev libpcrecpp0 libpcre3-dev
  libyaml-0-2 libyaml-dev zlib1g-dev libhtp1 libnfnetlink0 libnetfilter-queue1
  libnfnetlink-dev libnetfilter-queue-dev
Install these packages without verification [y/N]? y
```

Gambar -1. Instalasi paket perangkat lunak dan pustaka yang dibutuhkan suricata

Langkah selanjutnya membuat user dan group suricata dengan perintah berikut:

```
bangnaufal@pcrouter:~$ sudo useradd -s /bin/false -c "Suricata user" suricata
```

Hasil perintah diatas dapat dibuktikan dengan perintah berikut:

```
abangnaufal@pcrouter:~/suricata-1.0.1$ getent passwd suricata
suricata:x:1001:1001:Suricata user:/home/suricata:/bin/false
```

Selanjutnya membuat direktori konfigurasi dan log suricata, dengan perintah berikut:

```
bangnaufal@pcrouter:~$ sudo mkdir /etc/suricata
bangnaufal@pcrouter:~$ sudo mkdir /var/log/suricata
bangnaufal@pcrouter:~$ sudo chown suricata.suricata /var/log/suricata
```

Selanjutnya Anda ekstrak suricata dengan perintah berikut:

```
bangnaufal@pcrouter:~$ tar -xzf suricata-1.0.1.tar.gz
```

Setelah mengekstrak lakukan konfigurasi perangkat lunak suricata agar mendukung IPS (*Intrusion Prevention System*) menggunakan *Netfilter netlink-queue library* (nfqueue) dengan mengeksekusi perintah berikut:

```
bangnaufal@pcrouter:~$ cd suricata-1.0.1
bangnaufal@pcrouter:~$ ./configure --enable-nfqueue --enable-debug
```

Selanjutnya lakukan kompilasi suricata dengan perintah berikut:

```
bangnaufal@pcrouter:~$ make
```

Jika pada saat kompilasi tidak terdapat kegagalan maka langkah berikutnya ini bersifat opsional, hanya saja karena penulis ingin menghasilkan file paket binary deb suricata maka langkah berikut ini harus dilakukan, yaitu sebagai berikut:

```
bangnaufal@pcrouter:~$ sudo checkinstall
```

Hasil eksekusi perintah checkinstall akan menghasilkan paket binary deb suricata (suricata_1.0.1-1_i386.deb) pada *current directory*. Kemudian instal paket binary deb tersebut dengan perintah berikut:

```
bangnaufal@pcrouter:~$ sudo dpkg -i suricata_1.0.1-1_i386.deb
```

Konfigurasi suricata

Setelah instalasi suricata selesai dilakukan Anda harus melakukan konfigurasi suricata terlebih dahulu, namun untuk kemudahan dalam menggunakan suricata Anda dapat menyalin sample konfigurasi yang terdapat pada direktori source code suricata. Untuk itu salinlah file suricata.yaml dan classification.config kedalam direktori konfigurasi suricata dengan perintah berikut:

```
bangnaufal@pcrouter:~$ sudo cp suricata.yaml /etc/suricata/
bangnaufal@pcrouter:~$ sudo cp classification.config /etc/suricata/
```

Selanjutnya Edit file suricata.yaml dan sesuaikan beberapa section konfigurasi (outputs, default-rule-path, vars) sesuai dengan kebutuhan. Untuk rule Anda dapat memanfaatkan rule bawaan perangkat lunak snort atau menggunakan rule dari www.emergingthreats.net (<http://www.emergingthreats.net/rules/emerging.rules.tar.gz>). Dalam artikel ini penulis menggunakan daftar rule yang diunduh dari www.emergingthreats.net, untuk itu unduh dengan perintah berikut:

```
bangnaufal@pcrouter:~$ wget
http://www.emergingthreats.net/rules/emerging.rules.tar.gz
```

Kemudian ekstrak rule tersebut dengan perintah berikut:

```
bangnaufal@pcrouter:~$ sudo tar -xzvf emerging.rules.tar.gz -C /etc/suricata/
```

Selanjutnya edit file `/etc/suricata/suricata.yaml` ubah bagian section `rule-files` hapus semua nama file rule yang tidak mengandung kata '**emerging**' dan biarkan nama file rule yang mengandung kata '**emerging**' sehingga menjadi seperti berikut:

```
# Set the default rule path here to search for the files.
# if not set, it will look at the current working dir
default-rule-path: /etc/suricata/rules/
rule-files:
- emerging-attack_response.rules
- emerging-dos.rules
- emerging-exploit.rules
- emerging-game.rules
- emerging-inappropriate.rules
- emerging-malware.rules
- emerging-p2p.rules
- emerging-policy.rules
- emerging-scan.rules
- emerging-virus.rules
- emerging-voip.rules
- emerging-web.rules
- emerging-web_client.rules
- emerging-web_server.rules
- emerging-web_specific_apps.rules
- emerging-user_agents.rules
- emerging-current_events.rules
```

catatan:

*Jika ingin melengkapi rule dengan rule dari snort Anda dapat menginstal snort terlebih dahulu dengan perintah '**sudo apt-get install snort**'. Kemudian salin semua file rule yang ada di `/etc/snort/rules` (yang nama filenya tidak ada kata '**emerging**') kedalam `/etc/suricata/rules` dan daftarkan (seperti cara diatas) semua nama file rule bawaan snort tersebut .*

Langkah konfigurasi berikutnya adalah mendefinisikan variabel `HOME_NET`, variabel ini menunjukkan alamat jaringan atau alamat komputer yang akan dipantau oleh suricata. Edit file `/etc/suricata/rules` sehingga variabel `HOME_NET` sesuai dengan alamat jaringan atau alamat komputer yang akan dipantau, seperti berikut ini:

```
HOME_NET: "[192.168.56.0/24,10.0.0.0/8]"
```

Mengaktifkan Suricata

Setelah selesai melakukan konfigurasi suricata maka Anda dapat segera mengaktifkan atau menjalankan suricata dengan perintah berikut:

```
bangnaufal@pcrouter:~$sudo suricata -c /etc/suricata/suricata.yaml -s  
/etc/suricata/classification.config -i eth0
```

atau jika ingin berjalan dalam mode daemon seperti berikut:

```
bangnaufal@pcrouter:~$sudo suricata -c /etc/suricata/suricata.yaml -s  
/etc/suricata/classification.config -i eth0 --pidfile /var/run/suricata -D
```

Jika ketika menjalankan suricata gagal, biasanya itu disebabkan suricata tidak menemukan pustaka libhttp. Untuk mengatasi masalah tersebut Anda buat simbolik link seperti berikut ini:

```
bangnaufal@pcrouter:~$sudo ln -s /usr/local/lib/libhttp-0.2.so.1.0.2  
/usr/lib/libhttp-0.2.so.1
```

Selanjutnya untuk menguji suricata apakah dapat mendeteksi usaha intrusi coba Anda uji dari komputer lain dalam jaringan Anda dan gunakan tool seperti nmap (*port scanner*), kemudian coba lakukan port scanning dengan nmap terhadap mesin suricata Anda (misal ip 192.168.56.101) dengan menggunakan perintah berikut:

```
root@client:~# nmap 192.168.56.101
```

Kemudian pada mesin suricata coba lihat log nya dengan menjalankan perintah berikut:

```
abangnaufal@pcrouter:~$ sudo tail /var/log/suricata/fast.log
```

Perintah diatas akan menghasilkan output seperti berikut yang menandakan adanya upaya port scanning kepada komputer suricata (192.168.56.101):

```
08/23/10-14:25:39.814557  [**] [1:2010937:2] ET POLICY Suspicious inbound to MySQL  
port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 3] {6}  
192.168.56.1:59351 -> 192.168.56.101:3306 [Xref =>  
http://doc.emergingthreats.net/2010937][Xref =>  
http://www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections]  
08/23/10-14:25:39.862326  [**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL
```

```
port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 3] {6}
192.168.56.1:38430 -> 192.168.56.101:1433 [Xref =>
http://doc.emergingthreats.net/2010935][Xref =>
http://www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections]

08/23/10-14:25:39.886248 [**] [1:2010939:2] ET POLICY Suspicious inbound to
PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 3]
{6} 192.168.56.1:53738 -> 192.168.56.101:5432 [Xref =>
http://doc.emergingthreats.net/2010939][Xref =>
http://www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections]
```