PROJECT 11
Snort

Kebutuhan Projek:

- Sebuah komputer Linux machine, real atau virtual. Bisa menggunakan BackTrack 5 virtual machine.
- Komputer kedua yang diinstal Nmap. Bisa menggunakan Windows XP atau Windows 7

Pemilihan Operating System

1. Jalankan komputer. Setiap komputer di lab. Foresec memiliki banyak Sistem Operasi virtual, dan saudara bisa menggunakan salah satunya.
2. Untuk projek ini, direkomendasikan menggunakan Windows 7 atau XP. Project 15 for CNIT

Menjalankan Komputer Linux

1. Jalankan komputer Linux Backtrack. Buka jendela Terminal.
2. Pada jendela Terminal window, ketikan perintah berikut, dan lanjutkan dengan Enter:

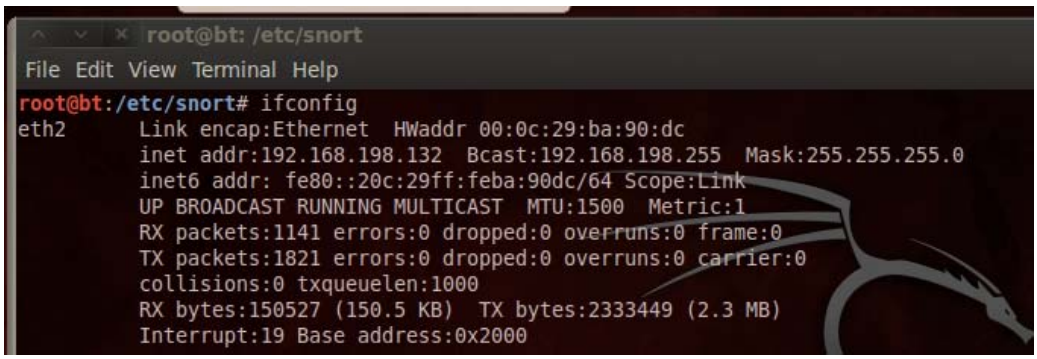
   ```
   ping www.binadarma.ac.id
   ```

3. Pastikan mendapatkan reply, dan tekan **Ctrl+C** untuk mengakhiri ping. (Untuk memasikan networknya jalan, jika bermasalah cek kabel dan koneksi)

4. Pada jendela Terminal, masukan perintah berikut, dan kemudian tekan Enter:

   ```
   ifconfig
   ```

5. Temukan interface yang terkoneksi ke internet dan catat interface dan ip address. Sebagai contoh pada gambar eth2, seperti terlihat (kemungkinan bisa eth0 atau eth1):



Konfigurasi Snort untuk Mendeteksi Ping

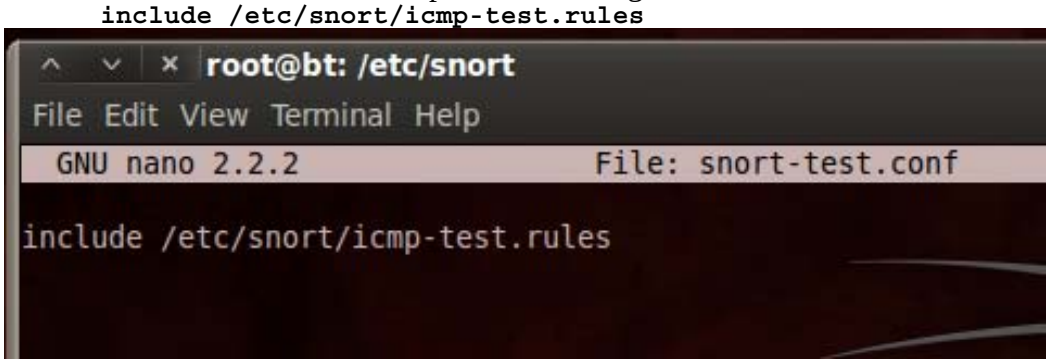
6. Snort memiliki serangkaian konfigurasi default, tapi di sini kita mulai dengan konfigurasi sederhana untuk mendeteksi ping.

7. Pada jendela Terminal, masukan perintah berikut, tekan Enter setelahnya:

```
root@bt:~# cd /etc/snort
root@bt:/etc/snort# nano snort-test.conf
```

```
cd /etc/snort
nano snort-test.conf
```

8. Masukan baris berikut, seperti terlihat di gambar:
```
include /etc/snort/icmp-test.rules
```



9. Simpan file dengan menekan **Ctrl+X**, **Y**, **Enter**.
10. Pada jendela Terminal, masukan perintah berikut, tekan Enter setelah selesai tiap baris :

```
nano icmp-test.rules
```

11. Masukan baris berikut, seperti terlihat pada gambar:
```
alert icmp any any -> any any (msg:"ICMP Packet"; sid:477;
rev:3;)
```

12. Simpan file dengan menekan **Ctrl+X**, **Y**, **Enter**.

Berikut merupakan struktur alert:

```
<Rule Actions> <Protocol> <Source IP Address> <Source Port> <Direction
Operator> <Destination IP Address> <Destination > (rule options)
```

Tabel: Struktur Rule dan contoh

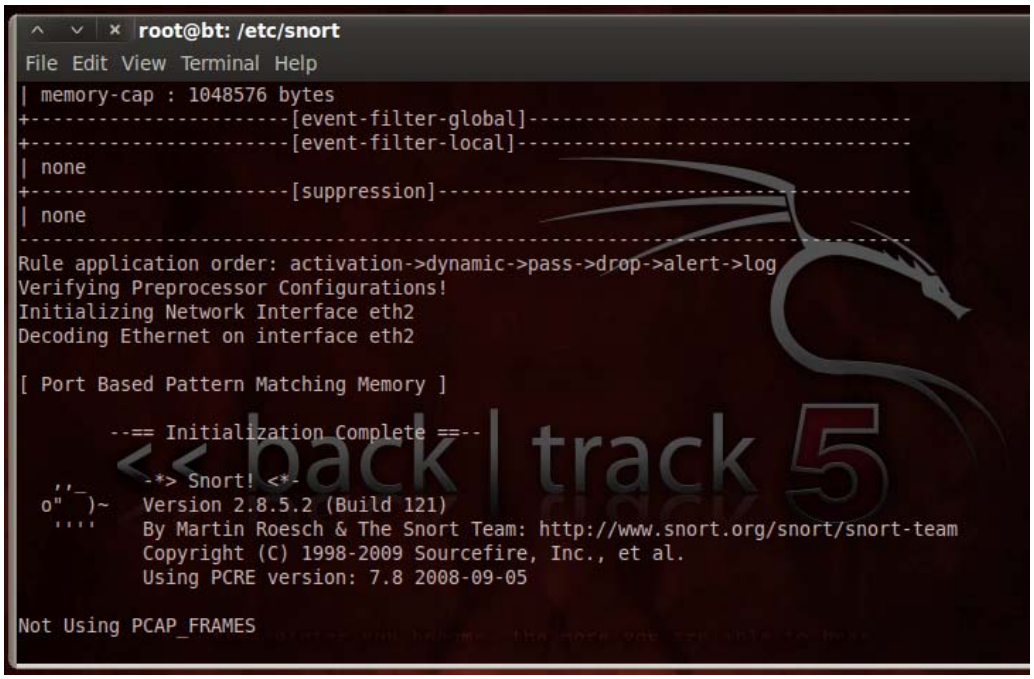
Structure	Example
Rule Actions	alert
Protocol	icmp
Source IP Address	any
Source Port	any
Direction Operator	->
Destination IP Address	any
Destination Port	any
(rule options)	(msg:"ICMP Packet"; sid:477; rev:3;)

Menjalankan Snort dengan hanya Satu Rule

13. Pada jendela Terminal, masukan perintah berikut, diakhiri dengan tombol Enter:

    `snort -i eth2 -c /etc/snort/snort-test.conf -l /var/log/snort`
    catatan : huruf yang terakhir adalah L huruf kecil, bukan angka 1.
    Gunakan nama interface sesuai dengan komputer, yang bisa saja berbeda bukan ***eth2****.*

14. Snort mulai berjalan, memperlihatkan pesan "Initialization Complete", seperti terlihat berikut:



15. Buka jendela Terminal yang lain, ketikan perintah berikut diikuti Enter:

    `ping -c 1 8.8.8.8`
16. Pada jendela Terminal, masukan perintah berikut, diikuti Enter :
    `cat /var/log/snort/alert`
17. Maka akan terlihat dua pesan, seperti terlihat di bawah ini. Baris pertama memperlihatkan outgoing ICMP type 8 ECHO request, dan baris kedua memperlihatkan incoming ICMP type 0 ECHO response.

```
root@bt:/etc/snort# cat /var/log/snort/alert

[**] [1:477:3] ICMP Packet [**]
[Priority: 0]
09/29-16:59:21.529633 192.168.198.132 -> 8.8.8.8
ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:12297  Seq:1  ECHO

[**] [1:477:3] ICMP Packet [**]
[Priority: 0]
09/29-16:59:21.582460 8.8.8.8 -> 192.168.198.132
ICMP TTL:128 TOS:0x0 ID:65253 IpLen:20 DgmLen:84
Type:0  Code:0  ID:12297  Seq:1  ECHO REPLY
```

Simpan Screen Image

18. Pastikan ICMP Type:8 dan ICMP Type 0: packets terlhat di file. Simpan screen capture dengan nama file "**NamaKamu_Proj 11a**".

Memberhentikan Snort

19. Pada jendela Terminal yang menjalankan Snort, tekan **Ctrl+C**.

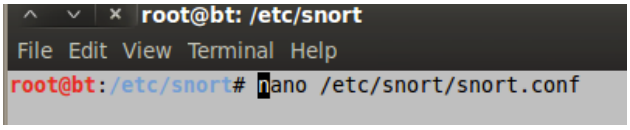
    Snort memperlihatkan halaman statistik paket, seperti terlihat di bawah:

```
    ICMP: 18          (18.182%)
  TCPdisc: 0          (0.000%)
  UDPdisc: 0          (0.000%)
  ICMPdis: 0          (0.000%)
     FRAG: 0          (0.000%)
   FRAG 6: 0          (0.000%)
      ARP: 8          (8.081%)
    EAPOL: 0          (0.000%)
  ETHLOOP: 0          (0.000%)
      IPX: 0          (0.000%)
    OTHER: 0          (0.000%)
  DISCARD: 0          (0.000%)
InvChkSum: 0          (0.000%)
   S5 G 1: 0          (0.000%)
   S5 G 2: 0          (0.000%)
    Total: 99
===============================
Action Stats:
ALERTS: 18
LOGGED: 18
PASSED: 0
===============================
Snort exiting
root@bt:/etc/snort#
```

Menjalankan Snort dengan Default Rules

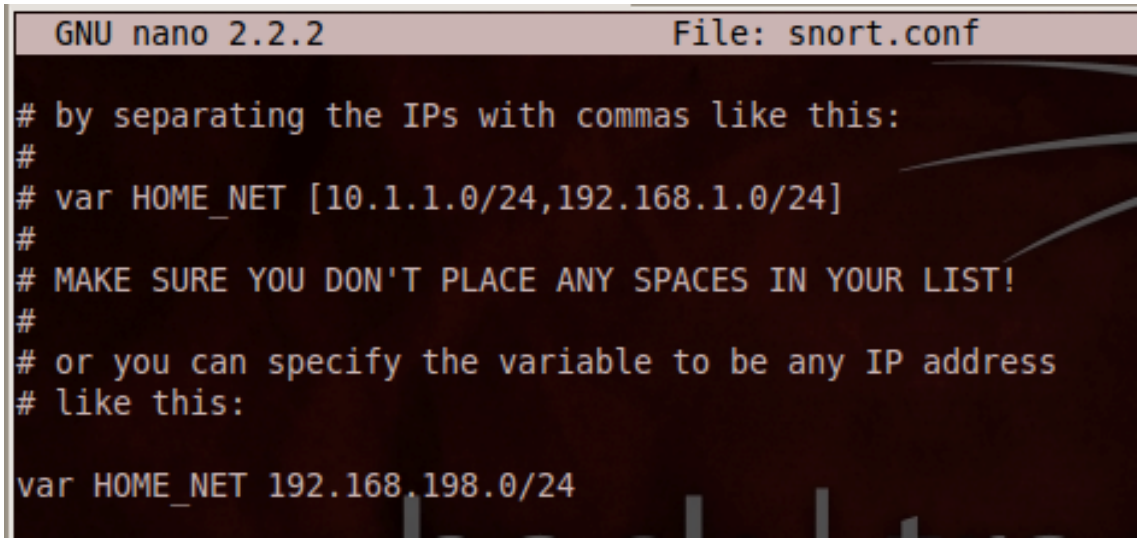
20. Pada jendela Terminal, masukan perintah berikut, akhiri dengan Enter :

    `nano /etc/snort/snort.conf`



21. Pada text editor, scroll down dan cari baris yang berawalan dengan **`var HOME_NET`**.

22. Set nilai ini dengan subnet address, seperti terlihat dibawah (**`var HOME_NET 192.168.77.0/24`**). Jika kurang yakin untuk melihat subnet address, buka jendela Terminal dan jalankan perintah **ifconfig** untuk melihatnya.



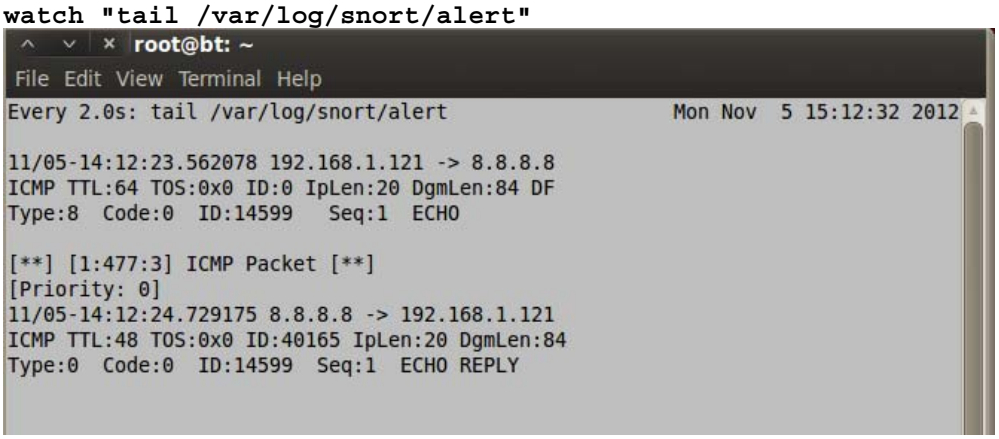
23. Simpan file dengan menekan **Ctrl+X**, **Y**, **Enter**.
24. Pada jendela Terminal, masukan perintah berikut, diikuti dengan Enter :

    `snort -i eth2 -l /var/log/snort -c /etc/snort/snort.conf`
    Catatan -l merupakan huruf L kecil, bukan angka 1.

    *Gunakan nama interface saudara, yang bisa saja bukan **eth2** (bisa **eth0** atau **eth1** lihat perintah 5).*

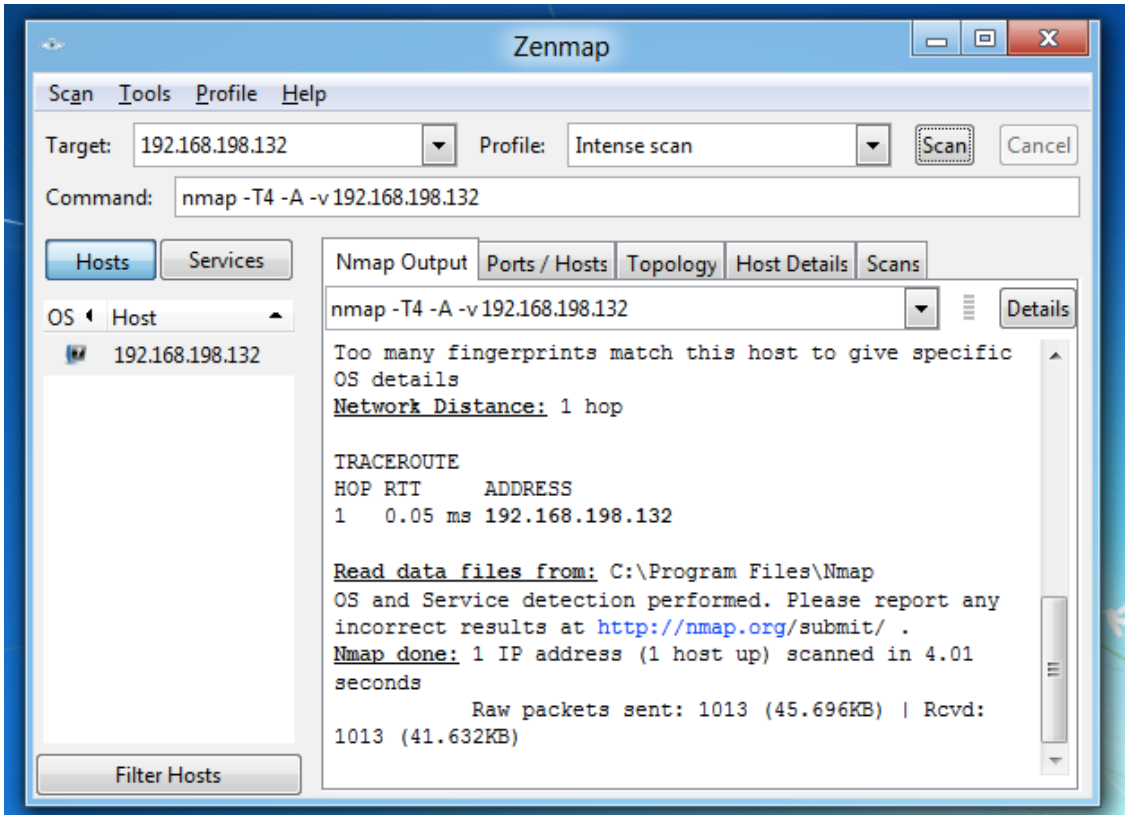
25. Snort berjalan, memperlihatkan pesan "Initialization Complete". Buka jendela Terminal lain dan masukan perintah berikut, diikuti dengan Enter key:

    `watch "tail /var/log/snort/alert"`



Instalasi dan Menjalankan Nmap di Windows

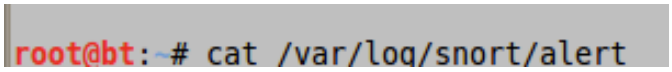
26. Buka browser di Windows dan download dan install nmap dari halaman berikut: http://nmap.org/book/inst-windows.html
27. Scroll down dan cari yang versi binaries (nmap-6.01-setup.exe).
28. Setelah download lakukan instalasi, dan jalankan nmap untuk melakukan scaning ke komputer Linux (masukan ip address Backtrack yang didapat dari perintah no 5), seperti terlihat di gambar berikut:



Monitoring Aktivitas Scanning di Backtrack

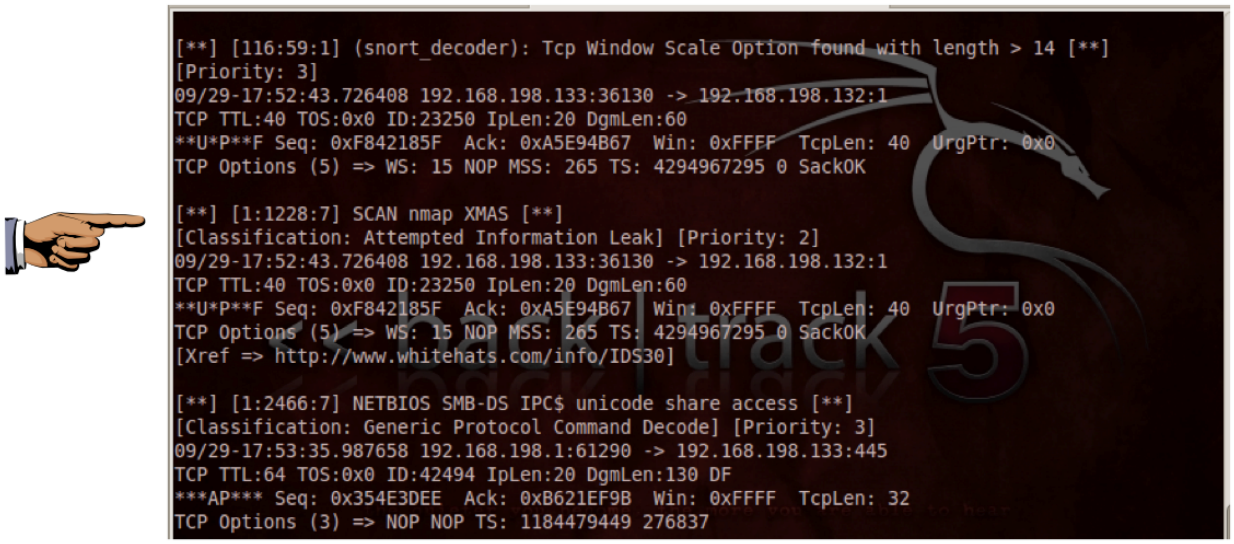
29. Akan terlihat pada jendela Backtrack muncul pesan yang menampilkan snort mengirim peringatan adanya aktifitas scan.
30. Ketika aktifitas scan selesai, click pada jendela Windows untuk melihat peringatan, dan tekan **Ctrl+C** untuk menghentikan aktifitas monitoring.

31. Pada jendela Terminal, masukan perintah berikut diakhiri dengan Enter :



`cat /var/log/snort/alert`

Maka akan terlihat beberapa pesan yang mendeteksi nmap scans, seperti berikut:



Simpan Screen Image

32. Pastikan bisa terlihat pesan "SCAN nmap" pada file peringatan. Simpan screen capture dengan nama file "**NamaKamu_Proj11b**".

Kumpulkan Project

33. Kirim melalui elearning untuk proj11.

Last Modified: 5-11-12