

**TUGAS KEAMANAN JARINGAN KOMPUTER
SNORT ALERT FILE PCAP DARI SCANNING**



DISUSUN OLEH:

NAMA : Fahrul Rozi

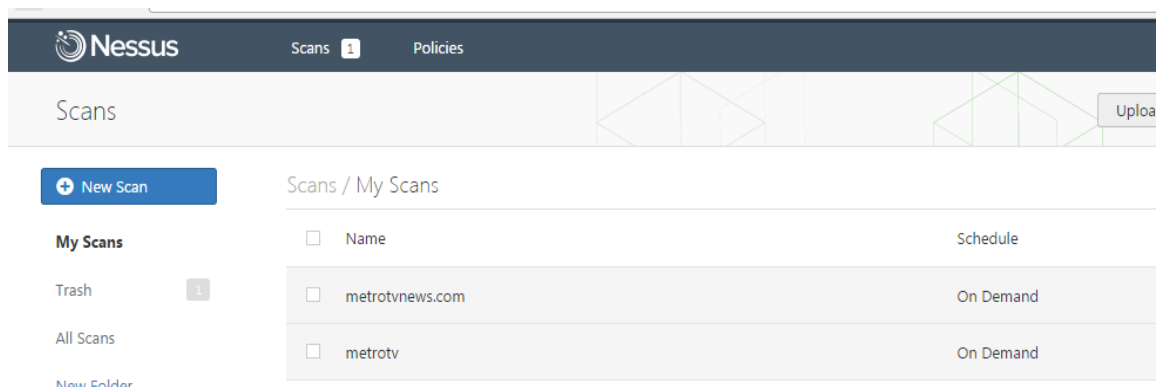
NIM : 09011181320022

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

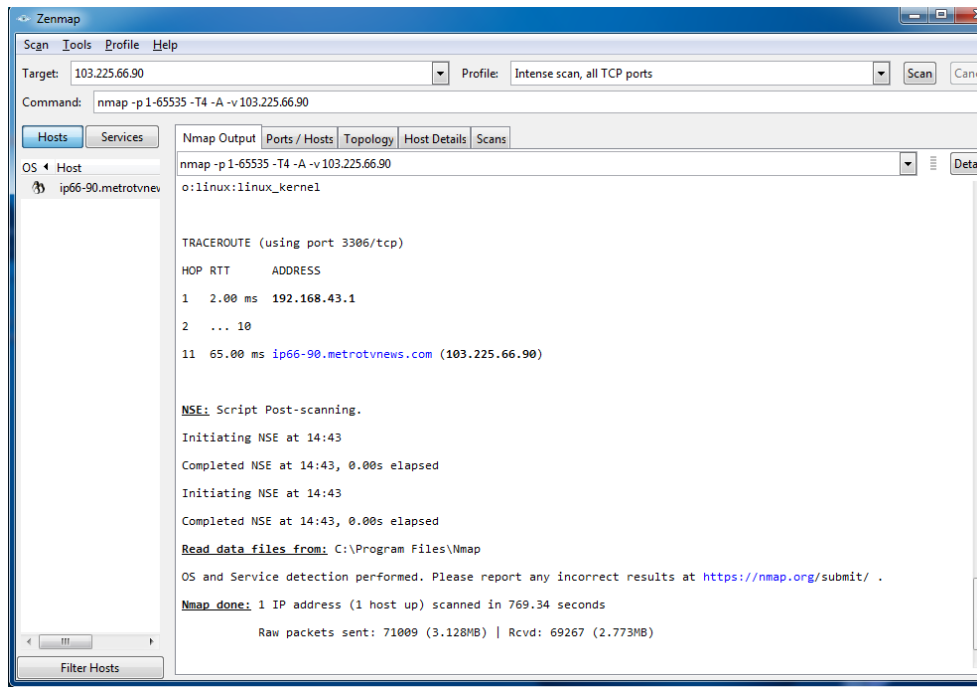
2017

Sebelumnya kita telah melakukan scanning pada target yaitu metrotvnews.com. pada laporan ini akan dilakukan menggunakan snort, yaitu pada saat melakukan scanning secara bersamaan kita mengambil data dengan menggunakan wireshark , wireshark akan menghasilkan file pcap dan file ini lah yang akan dianalisis dengan menggunakan snort. Apa itu snort , snort adalah sebuah software ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu Network Intrusion Detection System (NIDS) yang berskala ringan (lightweight), dan software ini menggunakan sistem peraturan-peraturan (rules system) yang relatif mudah dipelajari untuk melakukan deteksi dan pencatatan (logging) terhadap berbagai macam serangan terhadap jaringan komputer.

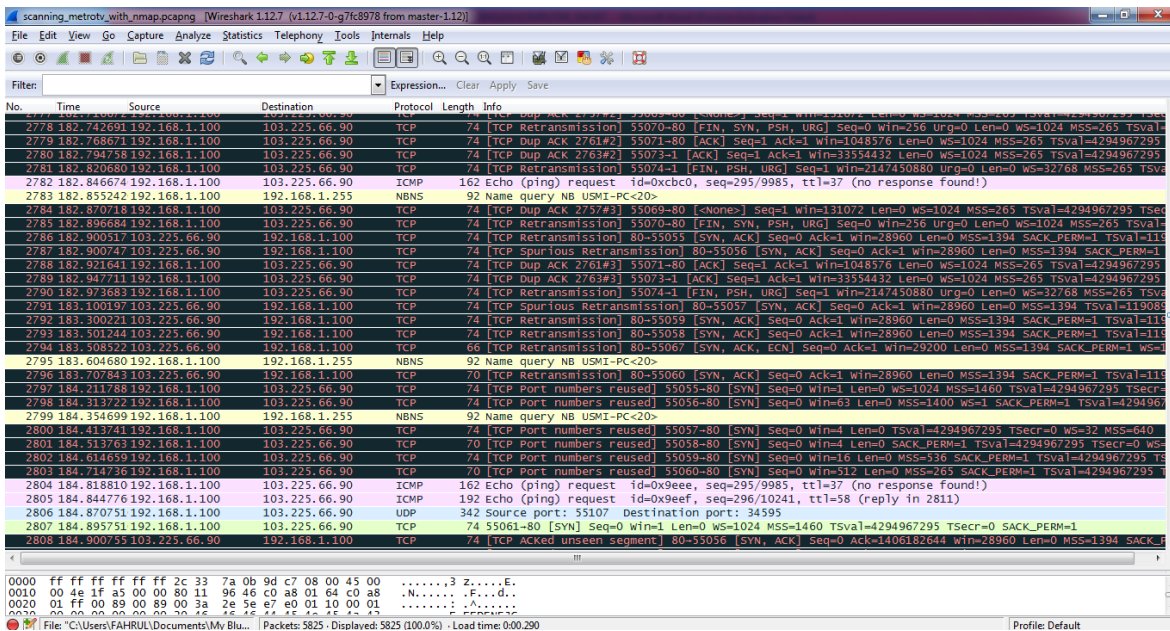
Target yang akan dilakukan scanning adalah **MetroTV** dengan domain **metrotvnews.com (103.225.66.90)**. Tools yang digunakan dalam scanning ini adalah NMAP/ZENMAP, NESSUS,dan wireshark digunakan untuk mengamati saat melakukan scanning. Scanning dilakukan selama 8 menit.



Gambar 1: Scanning menggunakan Nessus



Gambar 2 : scanning menggunakan NMAP/ZENMAP



Gambar 3 : wireshark

Pada wireshark terdapat 5082 packet yang terlihat dengan menggunakan tools ini, terdapat biabawh ini yaitu

```

alert - Notepad
File Edit Format View Help
03/08-14:55:08.460771 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP}
192.168.43.4 -> 103.225.66.9003/08-14:55:08.460771 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.43.4 -> 103.225.66.9003/08-14:55:08.463867 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:55:08.833103 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-14:55:27.698964 [**] [1:142:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.4:33965 -> 103.225.66.90:70503/08-14:55:35.341199 [**]
[1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.4:33965 ->
103.225.66.90:16103/08-14:56:55.962651 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a
Network Scan] [Priority: 3] {UDP} 192.168.43.4:49162 -> 239.255.255.250:190003/08-14:56:56.963538 [**] [1:1917:6] SCAN UPnP service
discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.43.4:49162 -> 239.255.255.250:1900
03/08-14:56:57.963583 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
[Priority: 3] {UDP} 192.168.43.4:49162 -> 239.255.255.250:190003/08-14:56:58.963609 [**] [1:1917:6] SCAN UPnP service discover
attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.43.4:49162 -> 239.255.255.250:190003/08-
14:58:09.883796 [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.4 ->
103.225.66.9003/08-14:58:09.910765 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.4 ->
103.225.66.9003/08-14:58:11.292886 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.43.4:41712 -> 103.225.66.90:103/08-14:58:11.318896 [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:11.344854 [**] [1:384:5] ICMP PING [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:12.638016 [**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-14:58:12.638270 [**] [1:402:7] ICMP
Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-
14:58:12.638323 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3]
{ICMP} 103.225.66.90 -> 192.168.43.403/08-14:58:12.641427 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information
Leak] [Priority: 2] {TCP} 192.168.43.4:41712 -> 103.225.66.90:103/08-14:58:12.665742 [**] [1:365:8] ICMP PING undefined code [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:12.690843 [**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:12.75463 [**] [1:408:5] ICMP Echo
Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-14:58:13.720003 [**] [1:402:7]
ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.4
03/08-14:58:13.920963 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.43.4:41712 -> 103.225.66.90:103/08-14:58:13.946973 [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:14.888981 [**] [1:384:5] ICMP PING [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:14.963497 [**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-14:58:15.007470 [**] [1:402:7] ICMP
Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-
14:58:15.198026 [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.43.4:41712 -> 103.225.66.90:103/08-14:58:19.323209 [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:19.349137 [**] [1:384:5] ICMP PING [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.43.4 -> 103.225.66.9003/08-14:58:19.407280 [**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90 -> 192.168.43.403/08-14:58:19.529318 [**] [1:1228:7] SCAN nmap
XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.4:41712 -> 103.225.66.90:103/08-14:58:19.858019
[**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.225.66.90
-> 192.168.43.403/08-14:58:20.574210 [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc activity] [Priority: 3]

```

Gambar 4 : alert pada pcap

Tabel 1. Alert dari snort

Total: 1	Priority: 2	alert ICMP PING NMAP
Total: 1	Priority: 3	alert ICMP Timestamp Request
Total: 1	Priority: 1	alert POLICY PPTP Start Control Request attempt
Total: 1	Priority: 2	alert SNMP AgentX/tcp request
Total: 1	Priority: 2	alert SNMP request tcp
Total: 1	Priority: 2	alert WEB-MISC robots.txt access
Total: 5	Priority: 3	alert ICMP Destination Unreachable Port Unreachable
Total: 5	Priority: 3	alert ICMP Echo Reply
Total: 6	Priority: 3	alert ICMP PING
Total: 8	Priority: 3	alert ICMP PING undefined code
Total: 8	Priority: 2	alert SCAN nmap XMAS
Total: 20	Priority: 3	alert SCAN UPnP service discover attempt
Total: 33	Priority: 3	alert ICMP Time-To-Live Exceeded in Transit

Diatas merupakan tabel hasil dari snort pada file pcap, dimana alert dengan jenis icmp ping nmap ini memiliki priority 2 dan total 1 kali , icmp timestamp request priority 3, policy pptp priority 1 dan total 1 , snmp agentx dan snmp request tcp memiliki priority dan total yang sama yaitu 2 dan 1, icmp destination dan echo reply juga memiliki data priority

dan total yang sama yaitu 3 dan 5, sedangkan icmp ping dan icmp ping undefined memiliki priority yng sama yaitu 3 tetapi total berbeda yaitu 6 dan 8 , scan nmap xmas memiliki priority 2 dan total 8, dan scan upnp service memiliki priority 3 dan total yang dimilikinya cukup besar yaitu 20 ,dan yang terakhir icmp time to live ini merupakan total terbesar dari alert yang lainnya yaitu sebesar 33 dan priority rata-rata sama seperti yang lain yaitu 3. Dibawah ini tampilan graf dari tabel diatas.

