TUGAS KEAMANAN JARINGAN KOMPUTER
SNORT ALERT FILE PCAP DARI SCANNING

DISUSUN OLEH:

NAMA : Fahrul Rozi

NIM : 09011181320022

JURUSAN SISTEM KOMPUTER

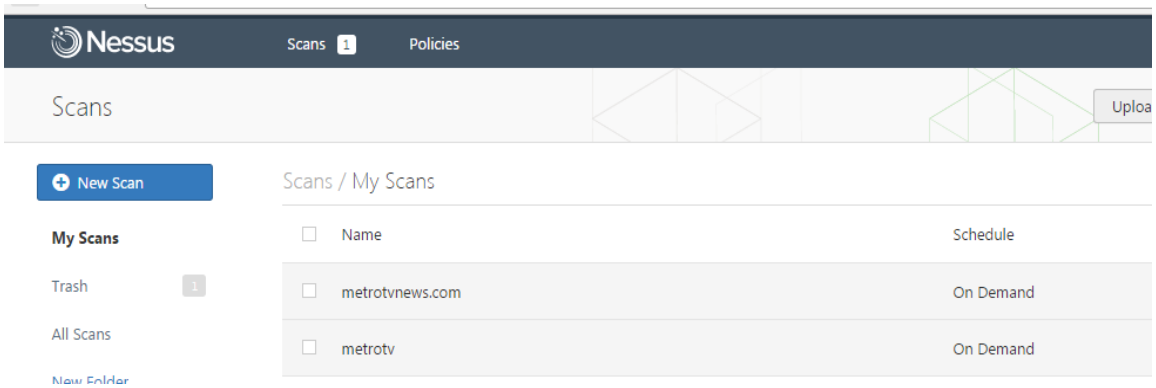
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

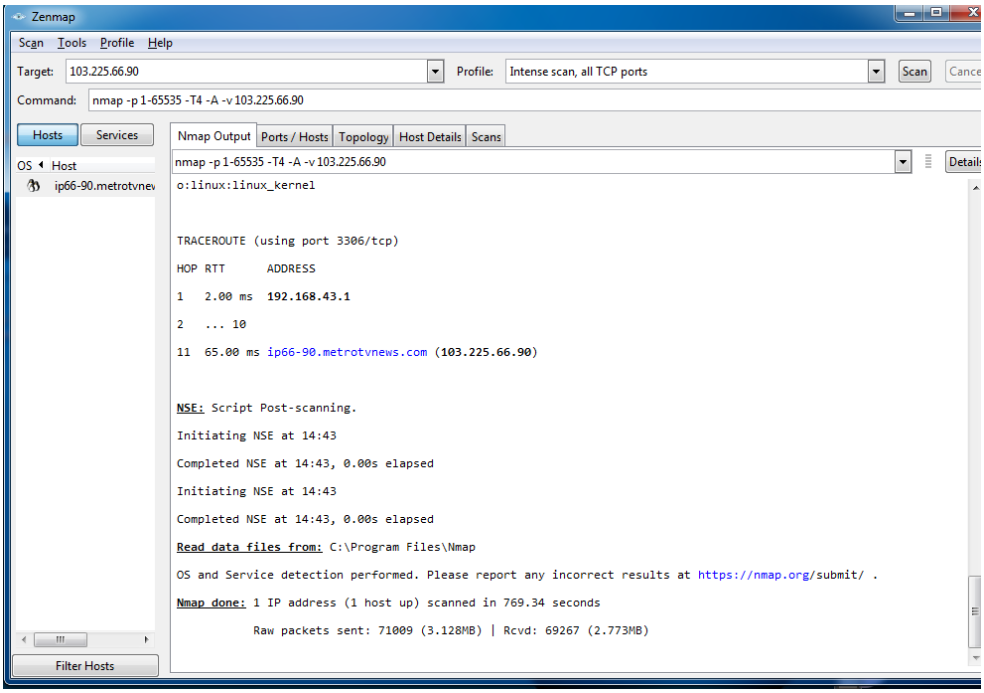
2017

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.

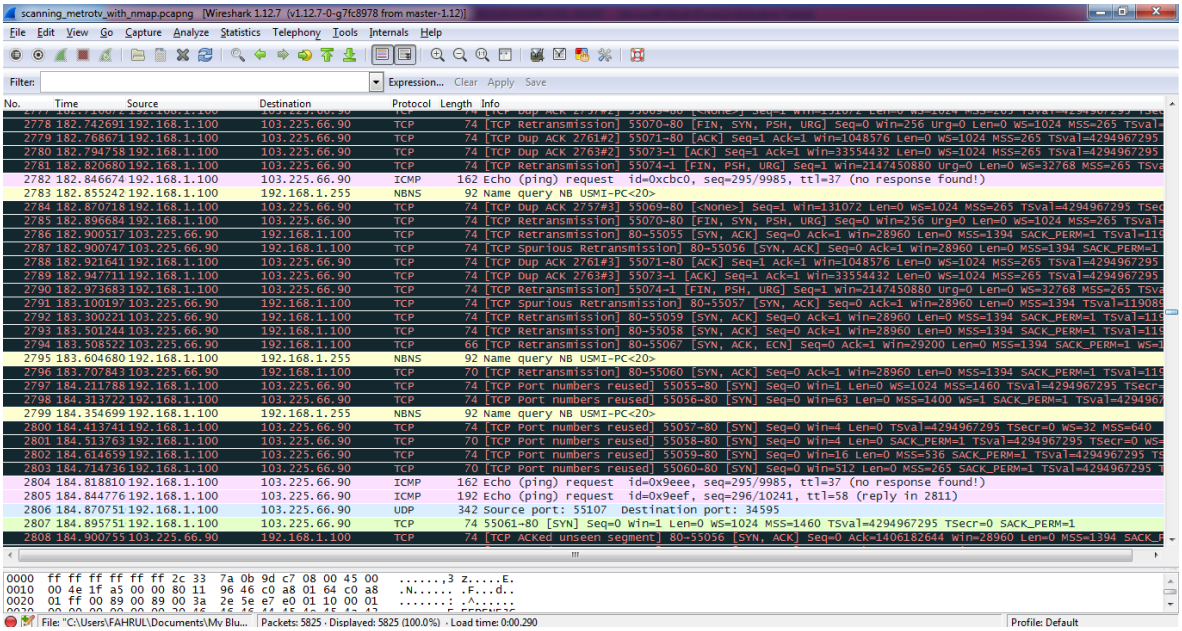
Target yang akan dilakukan scanning adalah **MetroTV** dengan domain **metrotvnews.com** (**103.225.66.90**). Tools yang digunakan dalam scaning ini adalah NMAP/ZENMAP, NESSUS,dan wireshark digunakan untuk mengamati saat melakukan scanning. Scaning dilakukan selama 8 menit.



Gambar 1: Scanning menggunakan Nessus



Gambar 2 : scanning menggunakan NMAP/ZENMAP



Gambar 3 : wireshark

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

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, plicy pptp priority 1 dan total 1 , snmp agenx 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 lainya yaitu sebesar 33 dan priority rata-rata sama seperti yang lain yaitu 3. Dibawah ini tampilan grap dari tabel diatas.