TUGAS KEAMANAN JARINGAN

" SNORT "

OLEH :

NAMA : MARDIAH

NIM : 09011281320005

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDERALAYA

2017

Target : www.unsri.ac.id

IP : 103. 241.4.11

Dalam dunia jaringan komputer diperlukan analisa dalam pertukaran paket data. Ada beberapa manfaat analisa tersebut antara lain, digunakan untuk troubleshooting masalah – masalah jaringan, untuk keamanan jaringan, pengembang software bisa menggunakannya untuk men-debug implementasi protokol jaringan, bisa juga untuk mempelajari protokol jaringan secara detail, dan masih banyak manfaat yang lainnya. Packet Capture adalah sebuah mekanisme menyalin packet yang diterima dalam jaringan dan membawa data yang disalin ke user untuk di analisa lebih lanjut.

Packet Capture adalah tindakan menangkap packet yang melintasi jaringan dengan lalu lintas tinggi. Sebagian besar packet capture dapat merekam header tanpa semua isi datagram. Libpcap merupakan library yang digunakan dalam packet capture. Sebagian besar network tools (Snort, Tcpdump, Ethereal) berbasis pada libpcap, yang dimana menyediakan high-level interface untuk packet capture

Snort merupakan packet sniffer dan logger berbasis libpcap yang dapat digunakan di jaringan sederhana sebagai Network Intrusion Detection System (NIDS). Arsitektur snort terdiri dari tiga komponen, yaitu packet decoder, detection engine, dan logger / alerter.

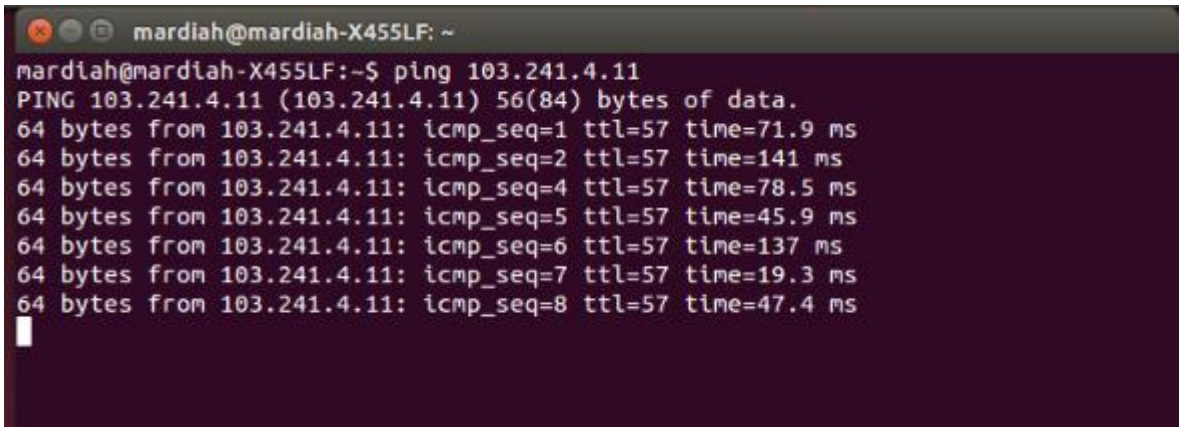
- Packet decoder : decoder packet Snort mendukung media Ethernet, SLIP, dan PPP. Packet decoder melakukan semua perkerjaan untuk mempersiapkan data dengan cara yang sifatnya membantu mesin deteksi
- Detection Engine : merupakan bagian paling penting dari Snort dikarenakan bertanggung jawab untuk menganalisa setiap paket berdasarkan aturan Snort / Snort Rules yang digunakan saat runtime. Detection engine bekerja dengan cara memisahkan Snort rules ke dalam apa yang disebut chain header dan chain options. Atribut umum seperti sumber / tujuan alamat IP dan port mengidentifikasikan chain header. Chain options ditentukan oleh rincian seperti TCP flags, ICMP, payload size, dan lain sebagainya
- Logger / Alerter : logger dan alerter merupakan dua hal yang terpisah. Logging memungkinkan user untuk mencatat informasi yang dikumpulkan oleh packet decoder dalam format yang mudah di baca. User dapat mengkonfigurasi alerts untuk dikirim ke syslog, flat file, UNIX sockets or a database

Tugas kali ini melakukan snort dari hasil scanning yang sudah dilakukan pada tugas – tugas sebelumnya. Proses scanning tersebut di rekam menggunakan tools pada percobaan ini menggunakan wireshark di ubuntu selama beberapa menit. Adapun scanner tools yang digunakan adalah sebagai berikut:

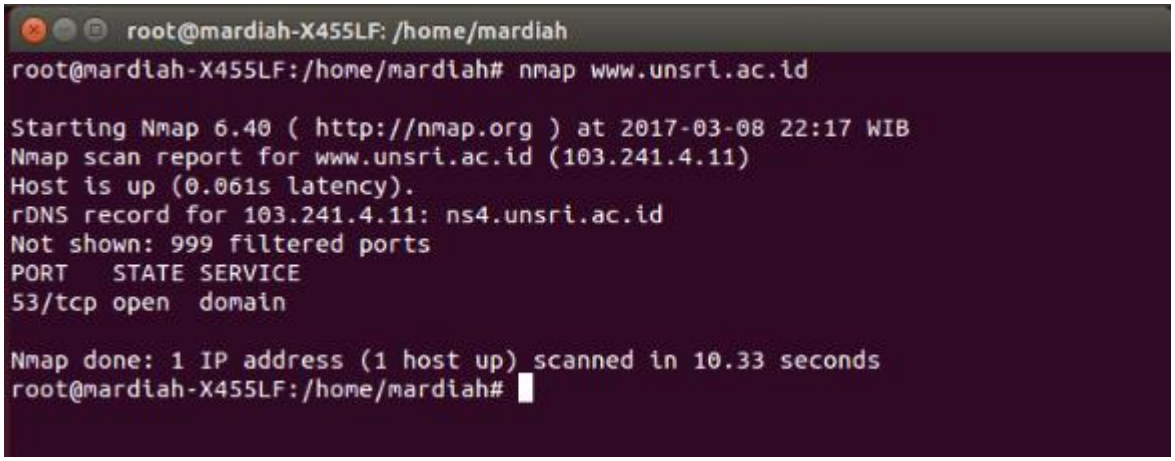
- Nmap
- Xprobe2

Berikut langkah kerja pada percobaan ini :

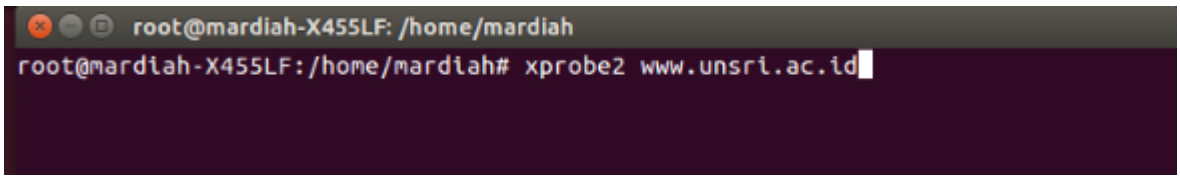
1. Buka tools wireshark dan start
2. Buka terminal dan lakukan proses ping pada ip target



3. Lakukan proses nmap pada domain target



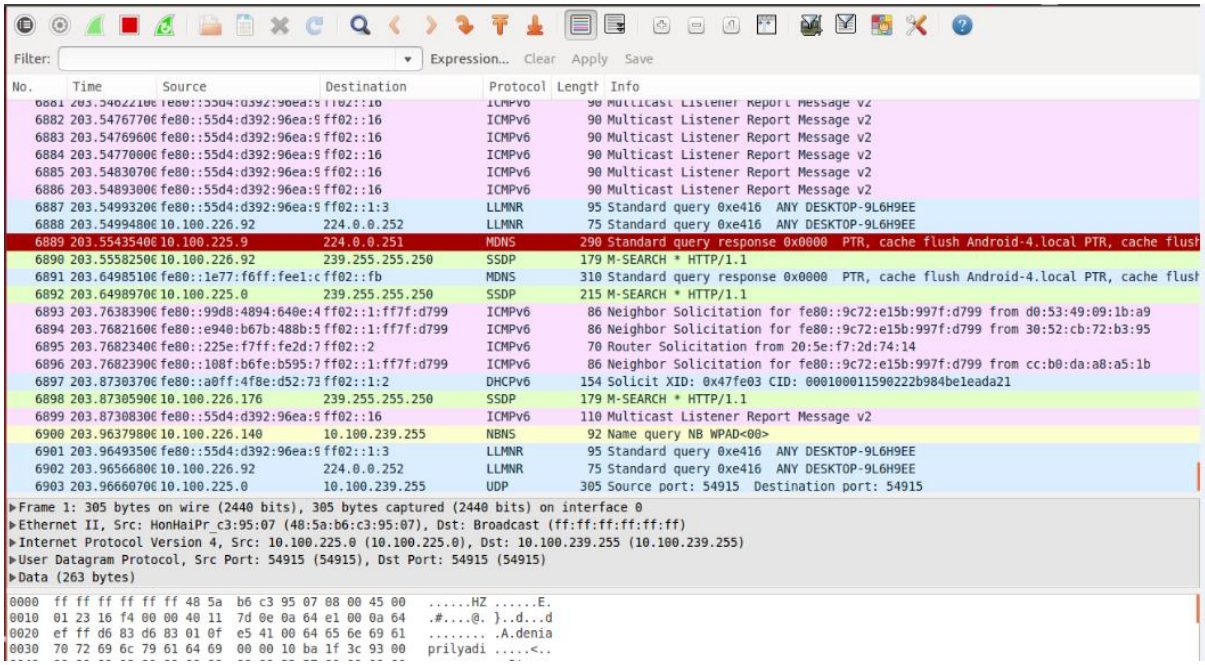
4. Lakukan proses Xprobe2 pada domain target



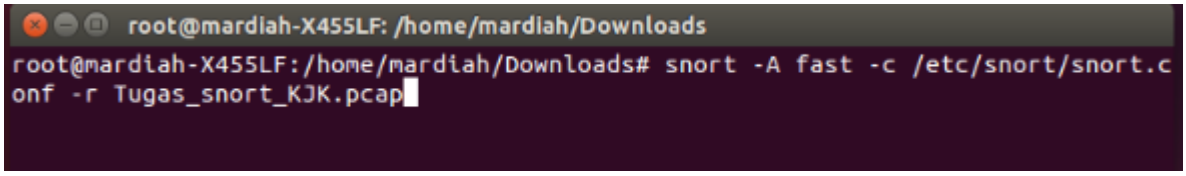
```
[+] Target is www.unsri.ac.id
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting modu
le
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting m
odule
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
```

```
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting modu
le
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting m
odule
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 103.241.4.11. Module
 test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 103.241.4.11. Module
 test failed
[-] No distance calculation. 103.241.4.11 appears to be dead or no ports known
[+] Host: 103.241.4.11 is down (Guess probability: 0%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@mardiah-X455LF:/home/mardiah#
```

5. Wireshark akan merekam semua aktivitas pertukaran paket data yang kita kerjakan



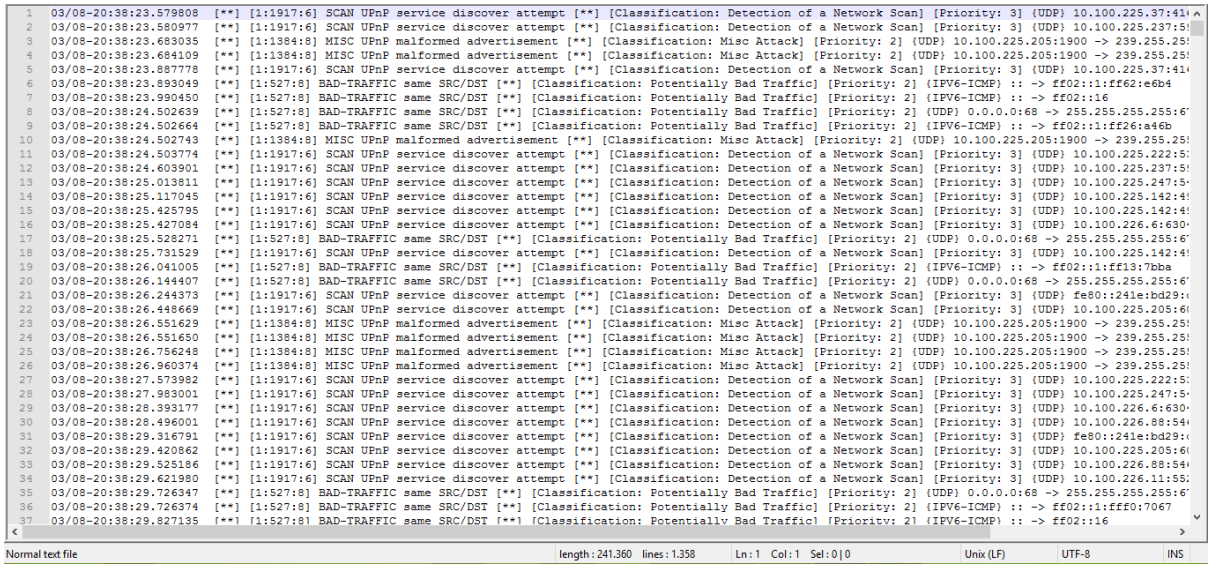
6. Setelah melakukan scanning target , lakukan snort pada hasil perekaman aktivitas pertukaran paket data pada wireshark . Dalam percobaan ini, hasil perekaman wireshark dibuat dengan nama Tugas_snort_KJK



```
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=
60
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=
60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=
60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=
10
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=
2
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=
2
+----------------------[suppression]-----------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->l
og
Verifying Preprocessor Configurations!
ICMP tracking disabled, no ICMP sessions allocated
IP tracking disabled, no IP sessions allocated
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.
```

```
          Internal Events: 0
          TCP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 2050
          UDP Port Filter
                 Filtered: 0
                Inspected: 3797
                  Tracked: 8
===============================================================================
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                   : 0
  Max concurrent sessions                          : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Snort exiting
root@mardiah-X455LF:/home/mardiah/Downloads#
```

7. Berikut merupakan tampilan hasil snort



8. Berikut tabel alert dari hasil snort yang telah di lakukan

No.	ALERT	Jumlah
1	ICMP Echo Reply	33
2	ICMP PING *NIX	32
3	[Classification: Misc activity]	107
4	[Priority: 3] {ICMP}	107
5	ICMP PING	36
6	SNMP request tcp	2
7	[Classification: Attempted Information Leak] [Priority: 2] {TCP}	4
8	SNMP AgentX/tcp request	2
9	ICMP Timestamp Reply	2
10	NMAP [Classification: Attempted Information Leak] [Priority: 2] {ICMP}	1
11	SCAN UPnP service discover attempt	711
12	Classification: Detection of a Network Scan	711
13	MISC UPnP malformed advertisement	393
14	Classification: Misc Attack	393
15	BAD-TRAFFIC same SRC/DST	141

16	Classification: Potentially Bad Traffic	141
17	[Priority: 3] {UDP}	711
18	[Priority: 2] {UDP}	468
19	[Priority: 2] {IPV6-ICMP}	66
20	ICMP Destination Unreachable Network Unreachable	2

9. Berikut grafik dari hasil snort yang telah di lakukan