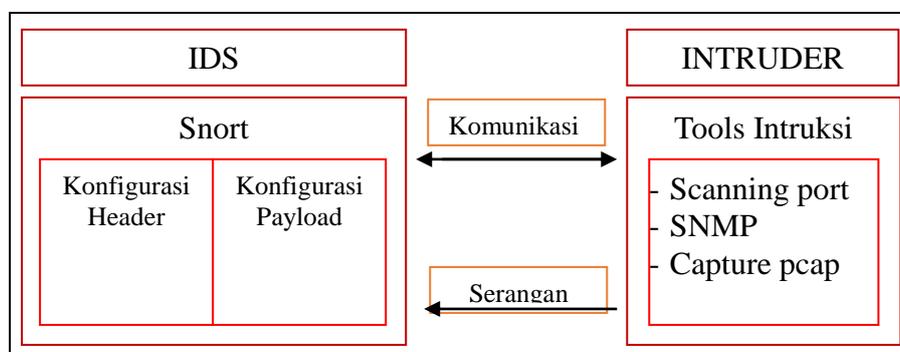


Nama : Riki Andika
NIM : 09011181320015

Intrusion Detection System (IDS) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan, yang selanjutnya akan disingkat dengan nama IDS. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP (Internet Protocol). IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi traffic yang mencurigakan didalam sebuah jaringan. Beberapa jenis IDS adalah : yang berbasis jaringan (NIDS) dan berbasis host (HIDS).

Ada IDS yang bekerja dengan cara mendeteksi berdasarkan pada pencarian ciri-ciri khusus dari percobaan yang sering dilakukan. Cara ini hampir sama dengan cara kerja perangkat lunak antivirus dalam mendeteksi dan melindungi sistem terhadap ancaman. Kemudian ada juga IDS yang bekerja dengan cara mendeteksi berdasarkan pada perbandingan pola traffic normal yang ada dan kemudian mencari ketidaknormalan traffic yang ada. Ada IDS yang fungsinya hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja tidak hanya sebagai pengawas dan pemberi peringatan melainkan juga dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem jaringan dan komputer, berikut topologi dari penggunaan IDS pada scanning website target;



Gambar 1. Topologi Jaringan Scanning

Pada tugas ini pengambilan data dengan menggunakan aplikasi wireshark dalam rentan waktu selama 366 detik atau sama dengan 6 menit, dengan menggunakan tools NMAP yang digunakan untuk melakukan scanning pada target, dengan alamat domain target www.polsri.ac.id (202.9.69.34) yang dicapture dengan menggunakan aplikasi wireshark yang menghasilkan capture sebanyak 11455 paket. Berikut hasil capture yang telah dilakukan;

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.94.16.164	10.100.130.10	DNS	84	Standard query 0xed2b PTR 34.69.9.202.in-addr.arpa
2	0.00798000	10.94.16.72	224.0.0.251	MDNS	82	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
3	0.008637000	fe80::2414:be2b:821f::ff02::fb	224.0.0.251	MDNS	102	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
4	0.009424000	10.94.16.72	224.0.0.251	MDNS	82	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
5	0.009528000	fe80::2414:be2b:821f::ff02::fb	224.0.0.251	MDNS	102	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
6	0.352323000	10.94.16.172	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
7	0.360502000	10.94.16.172	224.0.0.251	MDNS	82	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
8	0.361254000	fe80::f975:500:cc7e::ff02::fb	224.0.0.251	MDNS	102	Standard query 0x0000 PTR googlecast.tcp.local, "QM" question
9	0.484571000	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
10	0.691665000	10.100.130.10	10.94.16.164	DNS	164	Standard query response 0xed2b PTR www.polsri.ac.id
11	0.703591000	10.94.16.164	202.9.69.34	TCP	58	54333 > microsoft-ds [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.706369000	10.94.16.164	202.9.69.34	TCP	58	54333 > sunrpc [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.706474000	10.94.16.164	202.9.69.34	TCP	58	54333 > pptp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.706648000	10.94.16.164	202.9.69.34	TCP	58	54333 > https [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.706749000	10.94.16.164	202.9.69.34	TCP	58	54333 > epmap [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.706786000	10.94.16.164	202.9.69.34	TCP	58	54333 > pop3 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.706906000	10.94.16.164	202.9.69.34	TCP	58	54333 > rtsp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.706991000	10.94.16.164	202.9.69.34	TCP	58	54333 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.707542000	10.94.16.164	202.9.69.34	TCP	58	54333 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.707673000	10.94.16.164	202.9.69.34	TCP	58	54333 > smtp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.707976000	202.9.69.34	10.94.16.164	TCP	60	domain > 54333 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
22	0.719802000	10.94.16.164	202.9.69.34	TCP	58	54333 > ms-wbt-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.719903000	10.94.16.164	202.9.69.34	TCP	58	54333 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	0.740013000	202.9.69.34	10.94.16.164	TCP	60	pop3 > 54333 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.740099000	202.9.69.34	10.94.16.164	TCP	60	sunrpc > 54333 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.741667000	202.9.69.34	10.94.16.164	TCP	60	pptp > 54333 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.742460000	202.9.69.34	10.94.16.164	TCP	60	https > 54333 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.743447000	202.9.69.34	10.94.16.164	TCP	60	rtsp > 54333 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

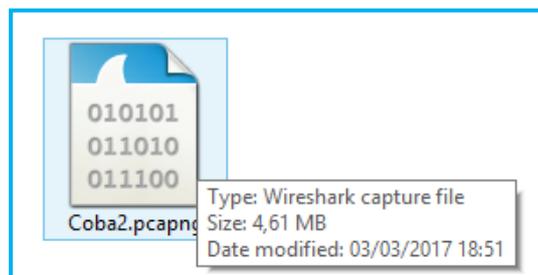
Gambar 2.a. Hasil Capture 1

Gambar diatas menunjukkan hasil capture paket-paket yang melakukan komunikasi antara server dengan client, yang dimulai dalam satu detik dengan menghasilkan file capture sebanyak 63 paket yang tercapture.

No.	Time	Source	Destination	Protocol	Length	Info
11420	301.2413990	10.94.10.174	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
11429	361.3682860	10.94.17.79	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
11430	361.5430390	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
11431	362.0324810	Routerbo b3:c7:c6	Spanning-tree-(for-br) STP	60	RST, Root = 32768/0/4c5e0c:b3:c7:c3 Cost = 0 Port = 0x8002	
11432	362.2957960	fe80::457:ef09:b977:a	ff02::1:2	DHCPv6	157	Solicit XID: 0xb23070 CID: 000100011fa44026086266ba5eb5
11433	362.4360650	fe80::1106:2b6c:10b1:	ff02::1:2	DHCPv6	144	Solicit XID: 0xb680b4 CID: 000100011cd241af3ca82aa149a6
11434	362.5261180	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
11435	363.1041310	fe80::2414:be2b:821f:	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
11436	363.1127530	fe80::2414:be2b:821f:	ff02::1:ff49:cde2	ICMPv6	86	Neighbor Solicitation for fe80::956b:7c2e:9949:cde2 from d4:c9:ef:70:75:c4
11437	363.1133610	fe80::2414:be2b:821f:	ff02::1:ff09:ffe6	ICMPv6	86	Neighbor Solicitation for fe80::9dc6:87a4:bf89:ffe6 from d4:c9:ef:70:75:c4
11438	363.4200900	10.94.16.44	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
11439	363.5221810	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
11440	363.7385260	10.94.16.80	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
11441	363.9888990	fe80::2414:be2b:821f:	ff02::1:ff49:cde2	ICMPv6	86	Neighbor Solicitation for fe80::956b:7c2e:9949:cde2 from d4:c9:ef:70:75:c4
11442	363.9902430	fe80::2414:be2b:821f:	ff02::1:ff09:ffe6	ICMPv6	86	Neighbor Solicitation for fe80::9dc6:87a4:bf89:ffe6 from d4:c9:ef:70:75:c4
11443	364.0276160	Routerbo b3:c7:c6	Spanning-tree-(for-br) STP	60	RST, Root = 32768/0/4c5e0c:b3:c7:c3 Cost = 0 Port = 0x8002	
11444	364.5333670	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
11445	364.9854630	fe80::2414:be2b:821f:	ff02::1:ff49:cde2	ICMPv6	86	Neighbor Solicitation for fe80::956b:7c2e:9949:cde2 from d4:c9:ef:70:75:c4
11446	364.9862130	fe80::2414:be2b:821f:	ff02::1:ff09:ffe6	ICMPv6	86	Neighbor Solicitation for fe80::9dc6:87a4:bf89:ffe6 from d4:c9:ef:70:75:c4
11447	365.0651330	fe80::24ee:ee36:a39f:	ff02::1:2	DHCPv6	146	Solicit XID: 0xb99f2 CID: 000100011f8f2158086266d769ba
11448	365.5283140	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
11449	366.0245200	Routerbo 44:6b:80	Ieee8021 00:88:bf	0x88bf	60	Ethernet II
11450	366.0304020	Routerbo b3:c7:c6	Spanning-tree-(for-br) STP	60	RST, Root = 32768/0/4c5e0c:b3:c7:c3 Cost = 0 Port = 0x8002	
11451	366.1049570	fe80::2414:be2b:821f:	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
11452	366.2488830	10.94.16.174	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
11453	366.3681600	10.94.17.79	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
11454	366.4235880	fe80::1106:2b6c:10b1:	ff02::1:2	DHCPv6	144	Solicit XID: 0xb680b4 CID: 000100011cd241af3ca82aa149a6
11455	366.5335990	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915

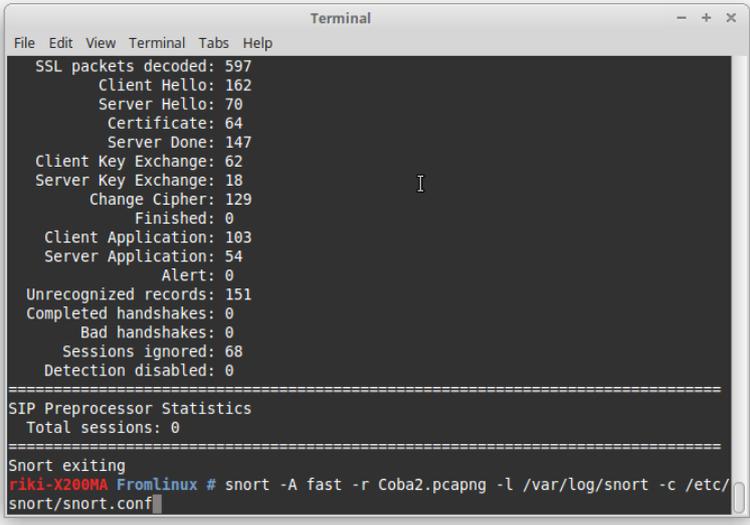
Gambar 2.a Hasil Capture 2

Banyaknya paket yang tercapture dengan menggunakan aplikasi wireshark, dapat dilihat pada gambar 2.a, dalam waktu 6 menit mengcapture paket yang saling berkomunikasi sebanyak 11455 paket. File pcap yang diperoleh di compile dengan menggunakan tools snort yang digunakan untuk mendeteksi serangan pada suatu network, snort dapat mendeteksi serangan sebesar 100Mbps. Output yang dihasilkan berupa report dan alert. Ada banyak variasi output yang dihasilkan snort, seperti teks (ASCII), XML, syslog, tcpdump, binary format, atau Database (MySQL, MsSQL, PostgreSQL, dsb). Berikut screenshot hasil pcap yang diperoleh dengan besar 4,61 MB.



Gambar 3. Hasil capture file pcap

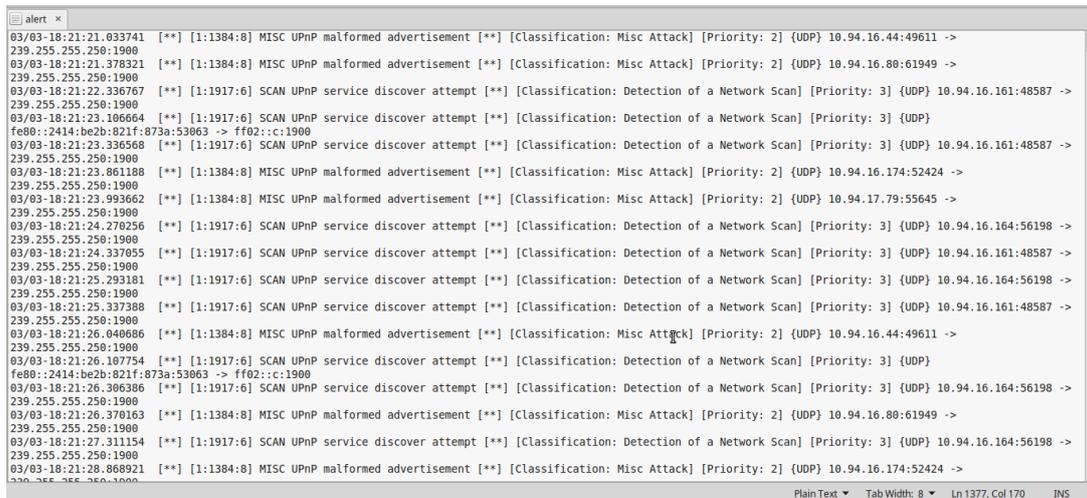
Kompilasi file pcap dengan menggunakan snort akan menghasilkan file alert yang berisi informasi-informasi paket yang terdapat dalam capture dari file pcap yang dilakukan dengan menggunakan Wireshark, dengan perintah snort `-A fast -r namafile.pcapng -l /var/log/snort/ -c /etc/snort/snort.conf`. Perintah tersebut akan menghasilkan file alert yang akan tersimpan pada folder `/var/log/snort`. Berikut screenshot compile dari file pcap dengan menggunakan snort;



```
Terminal
File Edit View Terminal Tabs Help
SSL packets decoded: 597
  Client Hello: 162
  Server Hello: 70
  Certificate: 64
  Server Done: 147
  Client Key Exchange: 62
  Server Key Exchange: 18
  Change Cipher: 129
  Finished: 0
  Client Application: 103
  Server Application: 54
  Alert: 0
Unrecognized records: 151
Completed handshakes: 0
  Bad handshakes: 0
  Sessions ignored: 68
  Detection disabled: 0
-----
SIP Preprocessor Statistics
Total sessions: 0
-----
Snort exiting
riki-X209MA FromLinux # snort -A fast -r Coba2.pcapng -l /var/log/snort -c /etc/snort/snort.conf
```

Gambar 4. Compile file pcap dengan menggunakan snort

Web yang dilakukan scanning dipantau selama kurang lebih 6 menit pengintaian, ada banyak sekali paket data yang mengalir. Terdapat beberapa paket data yang mengalir merupakan ancaman, sehingga IDS akan memberikan warning (alert). Beberapa alert yang muncul pada IDS Snort seperti yang ditunjukkan pada Gambar 5. Baris pertama sampai baris terakhir menunjukkan adanya beberapa serangan yang diluncurkan. Dengan hasil alert yang diperoleh dari file pcap yang telah dikompilasi dengan menggunakan snort menghasilkan sebanyak 1386 snort yang dihasilkan, dengan klasifikasi yang berbeda-beda sebanyak 20. Berikut hasil alert yang diperoleh;



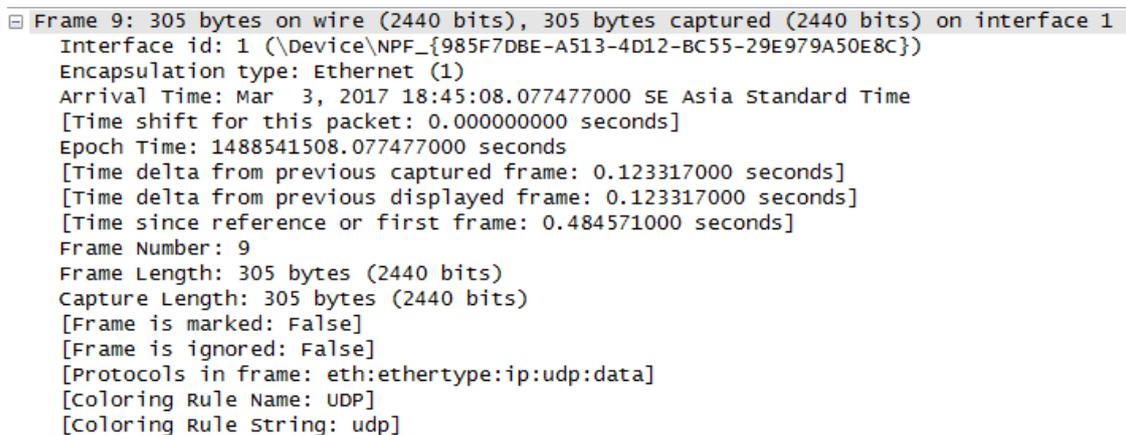
```

alert x
03/03-18:21:21.033741 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.44:49611 ->
239.255.255.250:1900
03/03-18:21:21.378321 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.80:61949 ->
239.255.255.250:1900
03/03-18:21:22.336767 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.161:48587 ->
239.255.255.250:1900
03/03-18:21:23.106664 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
fe08::2414:b2b:821f:873a:53063 -> ff02::c:1900
03/03-18:21:23.336568 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.161:48587 ->
239.255.255.250:1900
03/03-18:21:23.861188 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.174:52424 ->
239.255.255.250:1900
03/03-18:21:23.993662 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.17.79:55645 ->
239.255.255.250:1900
03/03-18:21:24.279256 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.164:56198 ->
239.255.255.250:1900
03/03-18:21:24.337055 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.161:48587 ->
239.255.255.250:1900
03/03-18:21:25.293181 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.164:56198 ->
239.255.255.250:1900
03/03-18:21:25.337388 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.161:48587 ->
239.255.255.250:1900
03/03-18:21:26.040686 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.44:49611 ->
239.255.255.250:1900
03/03-18:21:26.107754 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
fe08::2414:b2b:821f:873a:53063 -> ff02::c:1900
03/03-18:21:26.306386 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.164:56198 ->
239.255.255.250:1900
03/03-18:21:26.370163 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.80:61949 ->
239.255.255.250:1900
03/03-18:21:27.311154 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.94.16.164:56198 ->
239.255.255.250:1900
03/03-18:21:28.868921 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 10.94.16.174:52424 ->
239.255.255.250:1900

```

Gambar 5. Hasil snort berupa alert

Gambar 6 menunjukkan salah satu frame paket data yang mengalir pada jaringan. Paket data ini di-capture pada tanggal 03 maret 2017, dengan panjang frame 305 bytes (bits). Protokol jaringan yang digunakan adalah UDP.



```

Frame 9: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 1
Interface id: 1 (\Device\NPF_{985F7DBE-A513-4D12-BC55-29E979A50E8C})
Encapsulation type: Ethernet (1)
Arrival Time: Mar  3, 2017 18:45:08.077477000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1488541508.077477000 seconds
[Time delta from previous captured frame: 0.123317000 seconds]
[Time delta from previous displayed frame: 0.123317000 seconds]
[Time since reference or first frame: 0.484571000 seconds]
Frame Number: 9
Frame Length: 305 bytes (2440 bits)
Capture Length: 305 bytes (2440 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

```

Gambar 6. Frame paket data

Pada range Ethernet berikutnya merupakan lapisan fisik dan data link pada local area network, pada gambar 7 menunjukkan ethernet yang digunakan, baik dari sumber dan tujuan paket data di jaringan yang telah tercapture, berikut hasil screen paket ethernetnya.

```

Ethernet II, Src: AsustekC_d2:de:79 (ac:9e:17:d2:de:79), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 1. .... = LG bit: Locally administered address (this is NOT the factory default)
    .... 1. .... = IG bit: Group address (multicast/broadcast)
  Source: AsustekC_d2:de:79 (ac:9e:17:d2:de:79)
    Address: AsustekC_d2:de:79 (ac:9e:17:d2:de:79)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)

```

Gambar 7. Ethernet paket data

Paket data yang mengalir pada jaringan menggunakan IP Versi 4, dengan alamat sumber adalah 192.168.1.4 dengan tujuan 223.165.7.209. Informasi detailnya seperti yang ditunjukkan pada gambar 8.

```

Internet Protocol Version 4, Src: 10.94.17.14 (10.94.17.14), Dst: 10.94.17.255 (10.94.17.255)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... 00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 291
  Identification: 0x6faf (28591)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0xd252 [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 10.94.17.14 (10.94.17.14)
  Destination: 10.94.17.255 (10.94.17.255)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]

```

Gambar 8. IP paket data pada jaringan

Hasil dari alert yang diperoleh memperlihatkan banyaknya dan jenis-jenis dari alert yang ada didalam file pcap yang telah dicaputre, hasil dari alert selanjutnya akan dikelompokkan berdasarkan nama alert yang ada, yang diurutkan dengan menggunakan program pengelompokan alert dengan perintah python countalert.py alert hasilahir.txt dimana kata pertama untuk mengcompile program python, kata kedua memangi program yang akan dieksekusi, kata ketiga nama alert yang akan dihitung dan kata terahir nama file serta format hasil dari perhitungan alert tersebut (*Program countalert.py Eko Arip Winanto*). Berikut hasil screenshot dari pengurutan alert berdasarkan nama dan jumlahnya pada gambar 9.

```

riki@riki-X200MA /media/riki/My Drive/My Study/Mata Kuliah/Semester VIII/[3 SKS]
Keamanan Jaringan Komputer/tugas4/Fromlinux/Screen_New $ su
Password:
riki-X200MA Screen_New # python countalert.py alert hasilahir
Total: 2 Priority: 3 alert BAD-TRAFFIC 0 ttl
Total: 2 Priority: 3 alert ICMP Time-To-Live Exceeded in Transit
Total: 2 Priority: 2 alert SNMP AgentX/tcp request
Total: 2 Priority: 2 alert SNMP request tcp
Total: 2 Priority: 2 alert WEB-CGI finger access
Total: 2 Priority: 2 alert WEB-MISC robots.txt access
Total: 4 Priority: 2 alert DNS named version attempt
Total: 4 Priority: 3 alert ICMP Destination Unreachable Port Unreach
able
Total: 4 Priority: 3 alert ICMP Echo Reply
Total: 4 Priority: 3 alert ICMP Echo Reply undefined code
Total: 4 Priority: 3 alert ICMP PING
Total: 4 Priority: 3 alert ICMP PING undefined code
Total: 8 Priority: 3 alert ICMP Destination Unreachable Communicatio
n Administratively Prohibited
Total: 8 Priority: 3 alert ICMP Destination Unreachable Host Unreach
able
Total: 16 Priority: 2 alert SCAN nmap XMAS
Total: 24 Priority: 3 alert COMMUNITY WEB-MISC Proxy Server Access
Total: 30 Priority: 1 alert COMMUNITY WEB-MISC mod_jrun overflow att
empt
Total: 44 Priority: 2 alert BAD-TRAFFIC same SRC/DST
Total: 421 Priority: 2 alert MISC UPnP malformed advertisement
Total: 799 Priority: 3 alert SCAN UPnP service discover attempt
riki-X200MA Screen_New #

```

Gambar 9. Hasil pengelompokkan alert

Dengan hasil file yang dihasilkan dari program tersebut berupa pengurutan berdasarkan jenis alert yang ada dengan tipe file txt, berikut hasilnya dapat dilihat pada gambar 10.

Total: 2	Priority: 3	alert	BAD-TRAFFIC 0 ttl
Total: 2	Priority: 3	alert	ICMP Time-To-Live Exceeded in Transit
Total: 2	Priority: 2	alert	SNMP AgentX/tcp request
Total: 2	Priority: 2	alert	SNMP request tcp
Total: 2	Priority: 2	alert	WEB-CGI finger access
Total: 2	Priority: 2	alert	WEB-MISC robots.txt access
Total: 4	Priority: 2	alert	DNS named version attempt
Total: 4	Priority: 3	alert	ICMP Destination Unreachable Port Unreachable
Total: 4	Priority: 3	alert	ICMP Echo Reply
Total: 4	Priority: 3	alert	ICMP Echo Reply undefined code
Total: 4	Priority: 3	alert	ICMP PING
Total: 4	Priority: 3	alert	ICMP PING undefined code
Total: 8	Priority: 3	alert	ICMP Destination Unreachable Communication Administratively Prohibited
Total: 8	Priority: 3	alert	ICMP Destination Unreachable Host Unreachable
Total: 16	Priority: 2	alert	SCAN nmap XMAS
Total: 24	Priority: 3	alert	COMMUNITY WEB-MISC Proxy Server Access
Total: 30	Priority: 1	alert	COMMUNITY WEB-MISC mod_jrun overflow attempt
Total: 44	Priority: 2	alert	BAD-TRAFFIC same SRC/DST
Total: 421	Priority: 2	alert	MISC UPnP malformed advertisement
Total: 799	Priority: 3	alert	SCAN UPnP service discover attempt

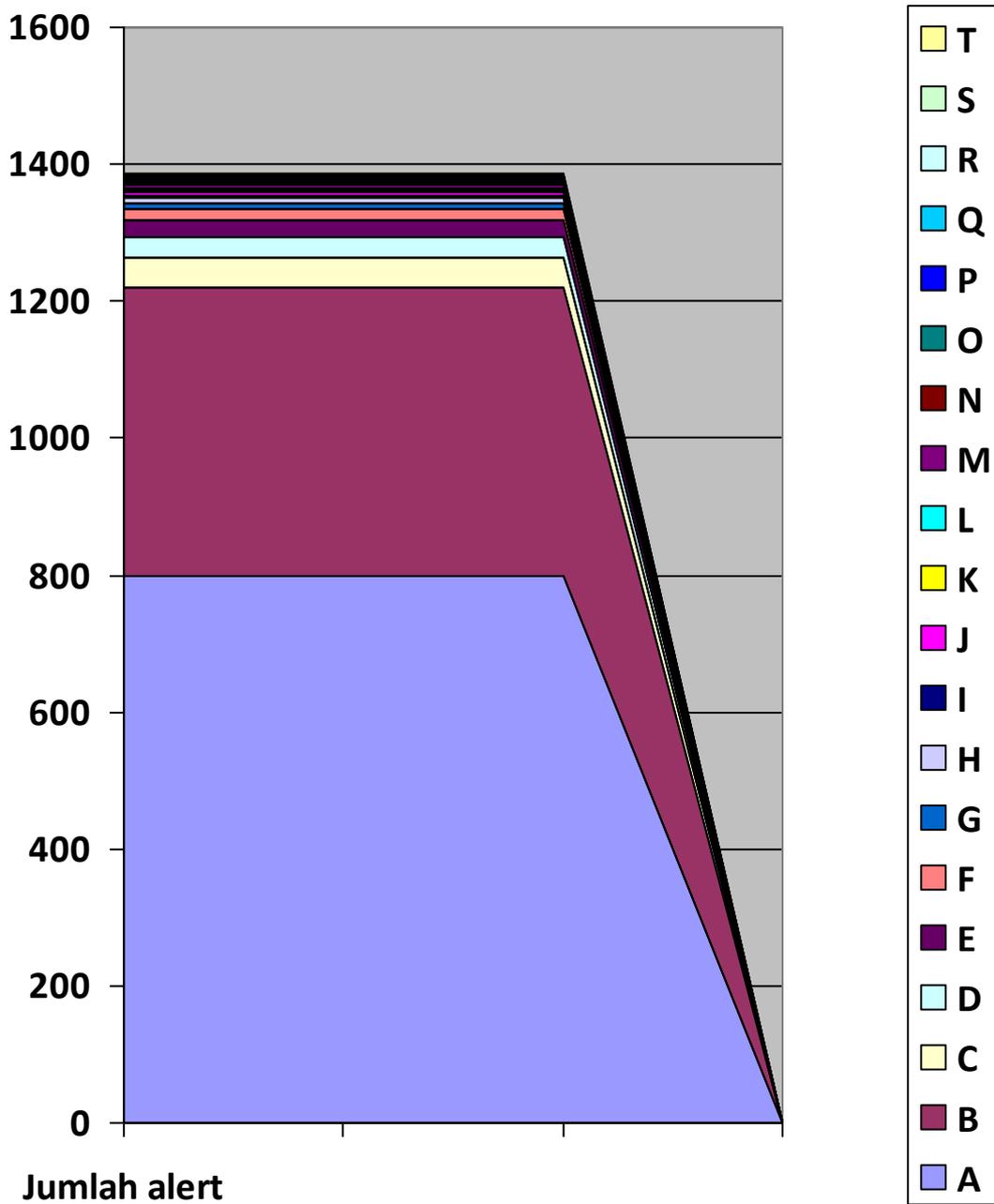
Gambar 10. Hasil dari program

Dari hasil alert yang diperoleh akan dibuat sebuah tabel beserta grafik yang menunjukkan hasil dari alert yang diperoleh, berikut hasil yang telah diperoleh dari scanning yang di capture dengan menggunakan aplikasi wireshark yang disajikan dalam bentuk tabel beserta grafik.

Tabel 1. Hasil pengurutan jumlah alert

No	Nama alert	Jumlah alert
1	BAD-TRAFFIC 0 ttl	2
2	ICMP Time-To-Live Exceeded in Transit	2
3	SNMP AgentX/tcp request	2
4	SNMP request tcp	2
5	WEB-CGI finger access	2
6	WEB-MISC robots.txt access	2
7	DNS named version attempt	4
8	ICMP Destination Unreachable Port Unreachable	4
9	ICMP Echo Reply	4
10	ICMP Echo Reply undefined code	4
11	ICMP PING	4
12	ICMP PING undefined code	4
13	ICMP Destination Unreachable Communication Administratively Prohibited	8
14	ICMP Destination Unreachable Host Unreachable	8
15	SCAN nmap XMAS	16
16	COMMUNITY WEB-MISC Proxy Server Access	24
17	COMMUNITY WEB-MISC mod_jrun overflow attempt	30
18	BAD-TRAFFIC same SRC/DST	44
19	MISC UPnP malformed advertisement	421
20	SCAN UPnP service discover attempt	799
J u m l a h a l e r t		1387

Tabel 1 diatas menunjukkan banyaknya alert yang diperoleh, beserta banyaknya jumlah alert dalam alert yang tercapture. Dari tabel diatas akan divisualisasikan dalam bentuk sebuah diagram yang menunjukkan banyaknya alert yang tercapture.



Grafik 1. Jumlah alert

Dengan keterangan grafik yang dibuat sebagai berikut;

- A : SCAN UPnP service discover attempt
- B : MISC UPnP malformed advertisement
- C : BAD-TRAFFIC same SRC/DST

D	: COMMUNITY WEB-MISC mod_jrun overflow attempt
E	: COMMUNITY WEB-MISC Proxy Server Access
F	: SCAN nmap XMAS
G	: ICMP Destination Unreachable Host Unreachable
H	: ICMP Destination Unreachable Communication Administratively Prohibited
I	: ICMP PING undefined code
J	: ICMP PING
K	: ICMP Echo Reply undefined code
L	: ICMP Echo Reply
M	: ICMP Destination Unreachable Port Unreachable
N	: DNS named version attempt
O	: WEB-MISC robots.txt access
P	: WEB-CGI finger access
Q	: SNMP request tcp
R	: SNMP AgentX/tcp request
S	: ICMP Time-To-Live Exceeded in Transit
T	: BAD-TRAFFIC 0 ttl

Pada percobaan scanning ini terdapat paket SYN Flood yang merupakan Denial of Service yang memanfaatkan 'loophole' pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih baru) telah mempunyai opsi konfigurasi untuk mencegah Denial of Service dengan mencegah atau menolak cracker mengakses sistem. Pada kondisi normal, client akan mengirimkan paket data yang berupa SYN untuk mensinkronkan diri kepada server. Lalu server menerima request dari client dan akan memberikan jawaban ke client berupa ACK (Acknowledgement) sebagai tanda transaksi sudah dimulai (pengiriman dan penerimaan data), maka client akan mengirimkan kembali sebuah paket SYN lagi.

Serangan ini memenuhi server dengan banyak paket SYN, karena saat pengiriman paket SYN oleh client, maka server juga akan mengirim paket SYN ACK ke client. Paket TCP SYN ACK yang masuk diantrian backlog hanya akan dibuang dari backlog pada saat terjadi time out dari timer TCP yang menandakan bahwa tidak ada respon dari pengirim, paket SYN ini tidak terdeteksi oleh aplikasi snort, sehingga akan

menjadi berbahaya bagi target. Berikut paket SYN yang tercapture oleh wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.94.16.164	10.100.130.10	DNS	84	Standard query 0xed2b PTR 34.69.9.202.in-addr.arpa
2	0.00790800	10.94.16.72	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
3	0.00863700	fe80::2414:be2b:821ff02::fb	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
4	0.00942400	10.94.16.72	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
5	0.00952800	fe80::2414:be2b:821ff02::fb	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
6	0.35232300	10.94.16.172	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
7	0.36050200	10.94.16.172	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
8	0.36125400	fe80::f975:500:cc7eff02::fb	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
9	0.48457100	10.94.17.14	10.94.17.255	UDP	305	Source port: 54915 Destination port: 54915
10	0.69166500	10.100.130.10	10.94.16.164	DNS	164	Standard query response 0xed2b PTR www.polsri.ac.id
11	0.70359100	10.94.16.164	202.9.69.34	TCP	58	54333->445 [SYN] Seq=0 win=1024 Len=0 MSS=1460
12	0.70636900	10.94.16.164	202.9.69.34	TCP	58	54333->111 [SYN] Seq=0 win=1024 Len=0 MSS=1460
13	0.70647400	10.94.16.164	202.9.69.34	TCP	58	54333->1723 [SYN] Seq=0 win=1024 Len=0 MSS=1460
14	0.70664800	10.94.16.164	202.9.69.34	TCP	58	54333->443 [SYN] Seq=0 win=1024 Len=0 MSS=1460
15	0.70674900	10.94.16.164	202.9.69.34	TCP	58	54333->135 [SYN] Seq=0 win=1024 Len=0 MSS=1460
16	0.70678600	10.94.16.164	202.9.69.34	TCP	58	54333->110 [SYN] Seq=0 win=1024 Len=0 MSS=1460
17	0.70690600	10.94.16.164	202.9.69.34	TCP	58	54333->554 [SYN] Seq=0 win=1024 Len=0 MSS=1460
18	0.70699100	10.94.16.164	202.9.69.34	TCP	58	54333->22 [SYN] Seq=0 win=1024 Len=0 MSS=1460
19	0.70754200	10.94.16.164	202.9.69.34	TCP	58	54333->53 [SYN] Seq=0 win=1024 Len=0 MSS=1460
20	0.70767300	10.94.16.164	202.9.69.34	TCP	58	54333->25 [SYN] Seq=0 win=1024 Len=0 MSS=1460
21	0.70797600	202.9.69.34	10.94.16.164	TCP	60	53->54333 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460
22	0.71980200	10.94.16.164	202.9.69.34	TCP	58	54333->3389 [SYN] Seq=0 win=1024 Len=0 MSS=1460
23	0.71990300	10.94.16.164	202.9.69.34	TCP	58	54333->21 [SYN] Seq=0 win=1024 Len=0 MSS=1460
24	0.74001300	202.9.69.34	10.94.16.164	TCP	60	110->54333 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
25	0.74090900	202.9.69.34	10.94.16.164	TCP	60	111->54333 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
26	0.74166700	202.9.69.34	10.94.16.164	TCP	60	1723->54333 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
27	0.74246800	202.9.69.34	10.94.16.164	TCP	60	443->54333 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

Gambar 11. Paket syn