

Network Security: SNORT

Intrusion detection adalah proses mendeteksi penggunaan yang tidak sah, atau serangan terhadap suatu jaringan komputer. *Intrusion Detection Systems (IDS)* dirancang dan digunakan untuk membantu dalam menghalangi atau mengurangi ancaman, kerusakan yang dapat ditimbulkan dari aktivitas *hacking* [1]. IDS merupakan kombinasi perangkat lunak atau perangkat keras yang dapat melakukan deteksi penyusupan pada sebuah jaringan. IDS mendeteksi adanya aktifitas mencurigakan berdasarkan *signature based* dan *anomali based* yang merupakan metode analisis *event* IDS. *Signature based* dapat diumpamakan seperti virus yang memiliki ciri khas. *Signature based* menggunakan pendekatan dengan cara pencocokan kejadian (*event*) dengan jenis serangan yang telah dikenal pada *database* IDS. Teknik ini sangat efektif dan merupakan metode utama yang digunakan pada beberapa perangkat atau produk IDS untuk mendeteksi serangan, sedangkan *anomali based* berdasakan kejanggalan yang terjadi pada pola lalu lintas jaringan yang diawasi, *Anomaly based* menggunakan pendekatan dengan cara mengidentifikasi perilaku atau aktivitas yang tidak biasa yang terjadi pada suatu *host* atau jaringan. *Anomaly based* membentuk perilaku dasar pada sebuah kondisi jaringan “normal” dengan profil pengguna tertentu kemudian mengukur dan membandingkannya ketika aktivitas jaringan berjalan tidak “normal”. [1, 2].

Berikut adalah *tools* yang digunakan dalam mengerjakan tugas *snort network security*:

- Wireshark: digunakan untuk *capture paket*
- Nmap: digunakan untuk melakukan *scanning* target
- Snort: digunakan untuk deteksi IDS
- Program *counteralert.py*: digunakan untuk mendapatkan total dan *priority* dari hasil log alert snort.



➤ Wireshark dan Nmap

Wireshark merupakan sebuah *Network Packet Analyzer*. *Network Packet Analyzer* akan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut sedetail mungkin. Sedangkan Nmap merupakan tools yang digunakan untuk melakukan *scanning* pada target. Target dalam percobaan ini merupakan website Universitas Airlangga www.unair.ac.id.

Pada saat melakukan *scanning*, kita harus menjalankan Wireshark secara bersamaan untuk mengcapture paket. Paket dari hasil *scanning* dari hasil wireshark berjumlah 5341.

The screenshot shows the Wireshark interface with a capture filter applied. The packet list pane shows 17 packets, all of which are TCP connections from 91.189.88.162 to 192.168.43.172 on port 80. The selected packet (No. 1) is a TCP packet with the following details:

- Ethernet II, Src: XiaomiCo_3a:d6:47 (78:02:f8:3a:d6:47), Dst: Azurewaw_7f:e0:57 (74:c6:3b:7f:e0:57)
- Internet Protocol Version 4, Src: 91.189.88.162, Dst: 192.168.43.172
- Transmission Control Protocol, Src Port: 80, Dst Port: 35040, Seq: 1, Ack: 1, Len: 1388

The packet bytes pane shows the raw data of the captured packet, including the Ethernet II header, IP header, and TCP header.

Gambar 1: hasil capture Wireshark *scanning* target

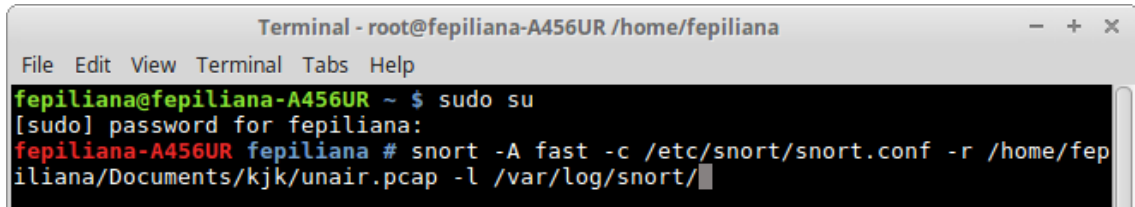
➤ Snort dan Program `counteralert.py`

Pada pengerjaan tugas *network security*, penulis menggunakan perangkat lunak Snort. Snort adalah salah satu tool atau aplikasi *open source Intrusion Detection Systems (IDS)* terbaik yang tersedia dan dikembangkan hingga saat ini. Pada pengerjaan tugas mata kuliah *network security* Snort dirancang untuk beroperasi berbasis *command line* dengan menggunakan metode *signature based*. Snort menganalisis semua lalu lintas jaringan untuk mengendus (*sniff*) dan mencari beberapa jenis penyusupan dalam



sebuah jaringan [2]. Snort tersusun atas *rules* yang disimpan dalam *signature database* [3]. Output dari Snort berupa *log alert* yang terletak pada direktori `/var/log/snort` di sistem operasi linux.

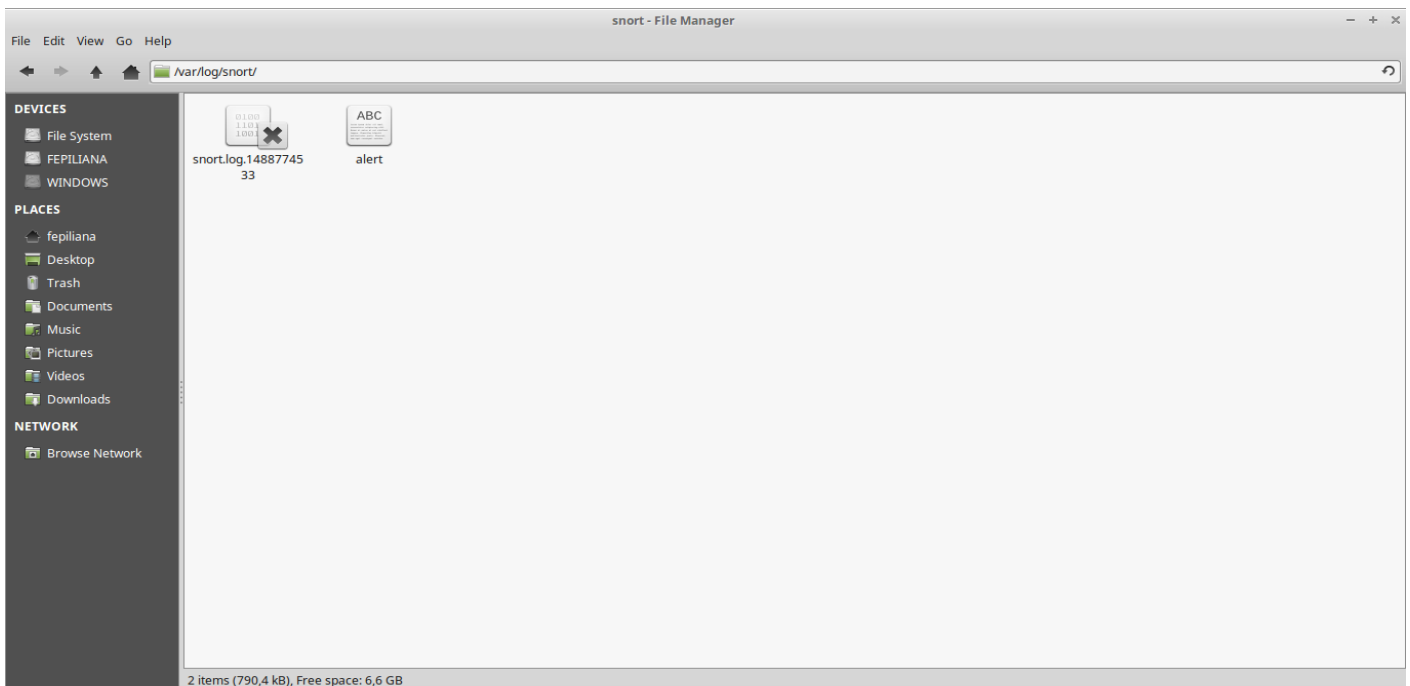
Untuk menjalankan snort pada sistem operasi Linux, kita gunakan *command* `snort -A fast -c /etc/snort/snort.conf -r (masukan_path_file_pcap) -l /var/log/snort`.



```
Terminal - root@fepiliana-A456UR /home/fepiliana
File Edit View Terminal Tabs Help
fepiliana@fepiliana-A456UR ~ $ sudo su
[sudo] password for fepiliana:
fepiliana-A456UR fepiliana # snort -A fast -c /etc/snort/snort.conf -r /home/fepiliana/Documents/kjk/unair.pcap -l /var/log/snort/
```

Gambar 2: *command* menjalankan snort.

Snort menggunakan *rules* yang disimpan dalam file teks yang dapat dimodifikasi dengan editor teks. Rules terbagi-bagi dalam beberapa kategori yang tersimpan dalam file-file yang berbeda-beda. File-file tersebut merupakan bagian dari file konfigurasi Snort, yang secara *default* disimpan dengan nama file konfigurasi `snort.conf`. Rule snort digunakan untuk mendeteksi adanya serangan atau aktivitas yang dilakukan oleh client-client terhadap server. Untuk melihat hasil alert yang dihasilkan oleh snort, kita dapat lihat pada direktori `/var/log/snort`.

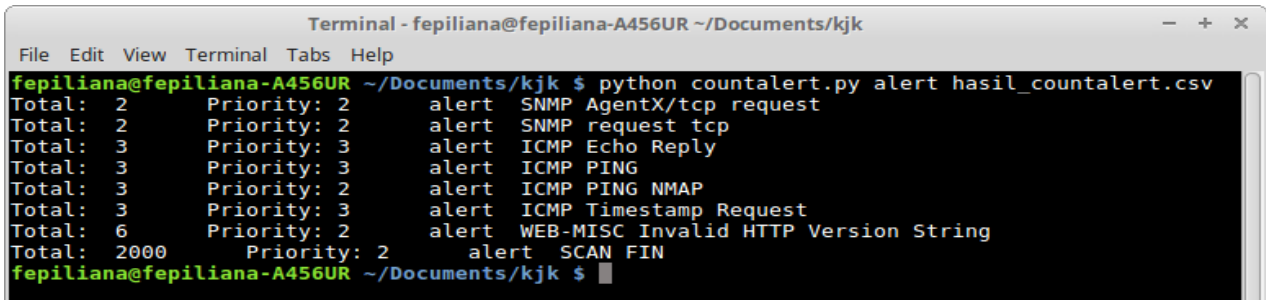


Gambar 3: hasil alert dari snort.



Berdasarkan gambar 4, ada banyak jenis alert yang dapat kita lihat dari hasil snort. Untuk mendapatkan total dari setiap alert yang dihasilkan, jika dihitung setiap baris akan sangat melelahkan dan tidak menutup kemungkinan akan adanya kekeliruan. Untuk hasil yang lebih efisien, maka penulis menggunakan program `countalert.py` untuk mendapatkan total dan *priority* dari setiap jenis alert. Program `countalert.py` merupakan program yang berbasis bahasa Python. Untuk menjalankan program tersebut kita ketik di *command* linux :

```
python countalert.py alert (nama_file_yang_diinginkan).csv
```

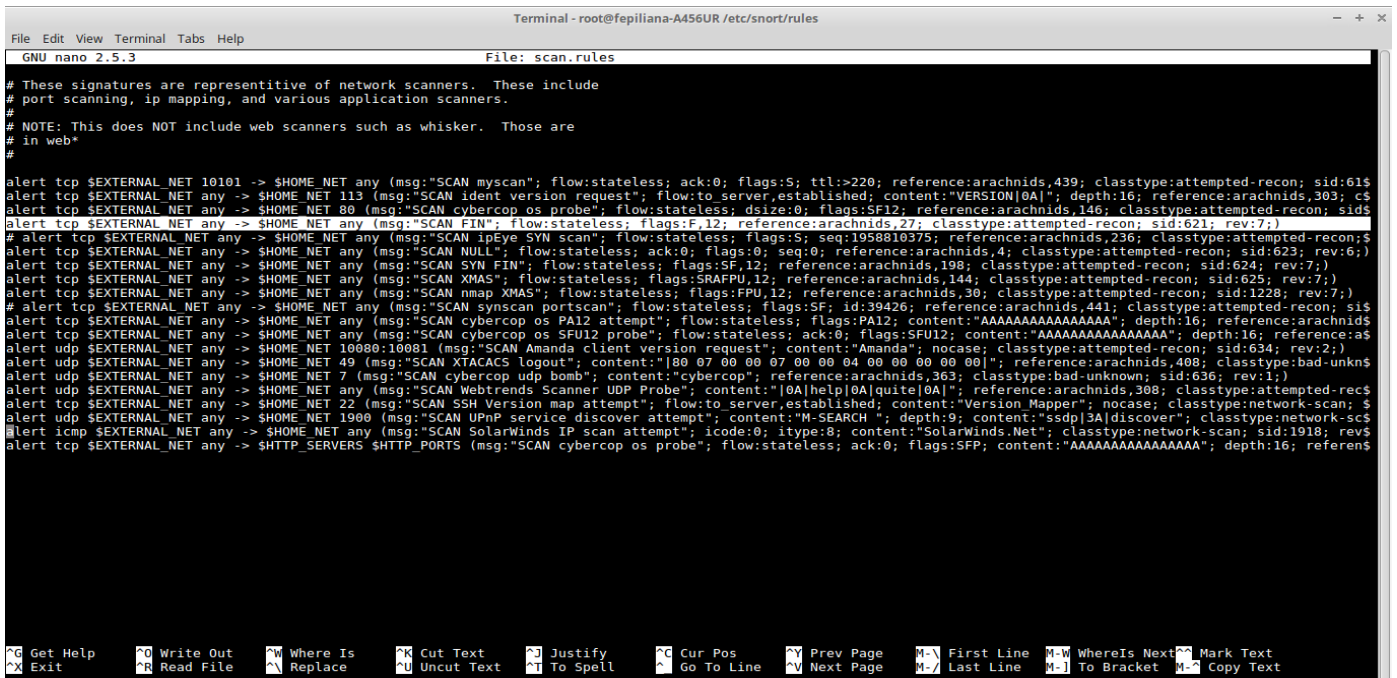


```
Terminal - fepiliana@fepiliana-A456UR ~/Documents/kjk
File Edit View Terminal Tabs Help
fepiliana@fepiliana-A456UR ~/Documents/kjk $ python countalert.py alert hasil_countalert.csv
Total: 2      Priority: 2      alert  SNMP AgentX/tcp request
Total: 2      Priority: 2      alert  SNMP request tcp
Total: 3      Priority: 3      alert  ICMP Echo Reply
Total: 3      Priority: 3      alert  ICMP PING
Total: 3      Priority: 2      alert  ICMP PING NMAP
Total: 3      Priority: 3      alert  ICMP Timestamp Request
Total: 6      Priority: 2      alert  WEB-MISC Invalid HTTP Version String
Total: 2000   Priority: 2      alert  SCAN FIN
fepiliana@fepiliana-A456UR ~/Documents/kjk $
```

Gambar 5: hasil *count* alert

Berdasarkan hasil dari gambar 5, dapat kita lihat bahwa alert SCAN FIN memiliki total 2000 yang terdapat pada file alert dari snort. SCAN FIN merupakan alert untuk mendeteksi *port scanning*.

Berikut adalah beberapa rules alert snort yang dicocokkan dengan gambar 3 dan gambar 4, sehingga dapatkanlah hasil alert pada gambar 5:



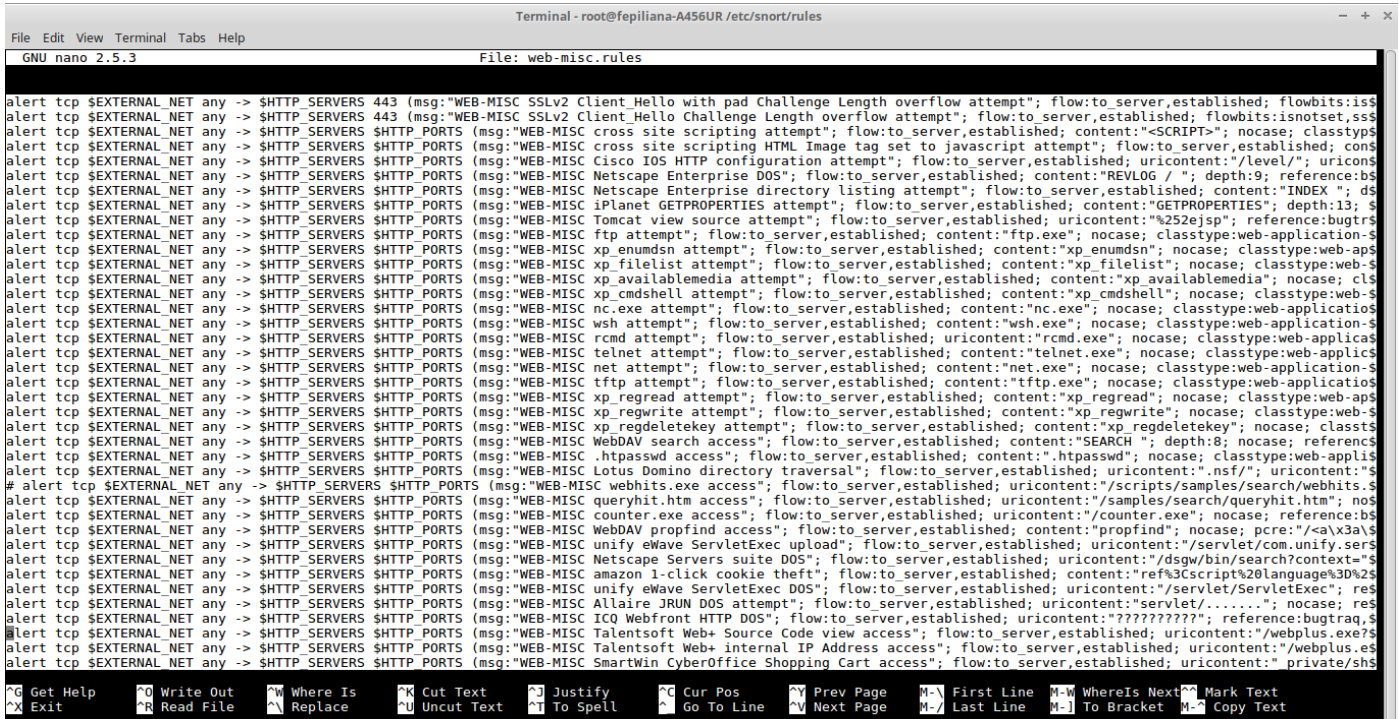
```
Terminal - root@fepiliana-A456UR /etc/snort/rules
File Edit View Terminal Tabs Help
GNU nano 2.5.3 File: scan.rules
# These signatures are representative of network scanners. These include
# port scanning, ip mapping, and various application scanners.
#
# NOTE: This does NOT include web scanners such as whisker. Those are
# in web*
#
alert tcp $EXTERNAL_NET 10101 -> $HOME_NET any (msg:"SCAN mscan"; flow:stateless; ack:0; flags:S; ttl:>220; reference:arachnids,439; classtype:attempted-recon; sid:615)
alert tcp $EXTERNAL_NET any -> $HOME_NET 113 (msg:"SCAN ident version request"; flow:to server,established; content:"VERSION|0A|"; depth:16; reference:arachnids,303; cs
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"SCAN cybercop os probe"; flow:stateless; dsize:0; flags:SF12; reference:arachnids,146; classtype:attempted-recon; sid5
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN FIN"; flow:stateless; flags:F,12; reference:arachnids,27; classtype:attempted-recon; sid:621; rev:7;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN ipEye SYN scan"; flow:stateless; flags:S; seq:1958810375; reference:arachnids,236; classtype:attempted-recon;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN NULL"; flow:stateless; ack:0; flags:0; seq:0; reference:arachnids,4; classtype:attempted-recon; sid:623; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN SYN FIN"; flow:stateless; flags:SF,12; reference:arachnids,198; classtype:attempted-recon; sid:624; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN XMAS"; flow:stateless; flags:SRAFFPU,12; reference:arachnids,144; classtype:attempted-recon; sid:625; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12; reference:arachnids,30; classtype:attempted-recon; sid:1228; rev:7;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN synscan portscan"; flow:stateless; flags:SF; id:39426; reference:arachnids,441; classtype:attempted-recon; sid5
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN cybercop os PA12 attempt"; flow:stateless; flags:PA12; content:"AAAAAAAAAAAAAAAAAAAA"; depth:16; reference:arachnids5
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN cybercop os SFU12 probe"; flow:stateless; ack:0; flags:SFU12; content:"AAAAAAAAAAAAAAAAAAAA"; depth:16; reference:a5
alert udp $EXTERNAL_NET any -> $HOME_NET 10080:10081 (msg:"SCAN Amanda client version request"; content:"Amanda"; nocase; classtype:attempted-recon; sid:634; rev:2;)
alert udp $EXTERNAL_NET any -> $HOME_NET 49 (msg:"SCAN XTACACS logout"; content:"|00 07 00 00 07 00 00 04 00 00 00 00|"; reference:arachnids,408; classtype:bad-unknown)
alert udp $EXTERNAL_NET any -> $HOME_NET 7 (msg:"SCAN cybercop udp bomb"; content:"cybercop"; reference:arachnids,363; classtype:bad-unknown; sid:636; rev:1;)
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN Webtrends Scanner UDP Probe"; content:"|0A|help|0A|quite|0A|"; reference:arachnids,308; classtype:attempted-rec5
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SCAN SSH Version map attempt"; flow:to server,established; content:"Version Mapper"; nocase; classtype:network-scan; s
alert udp $EXTERNAL_NET any -> $HOME_NET 1900 (msg:"SCAN UPnP service discover attempt"; content:"M-SEARCH "; depth:9; content:"ssdp|3A|discover"; classtype:network-sc5
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN SolarWinds IP scan attempt"; icode:0; itype:8; content:"SolarWinds.Net"; classtype:network-scan; sid:1918; rev5
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN cybercop os probe"; flow:stateless; ack:0; flags:SFP; content:"AAAAAAAAAAAAAAAAAAAA"; depth:16; referens
```

Gambar 6: rules alert SCAN FIN



Alert SCAN FIN

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN FIN"; flow:stateless; flags:F,12; reference:arachnids,27; classtype:attempted-recon; sid:621; rev:7);
```



```
Terminal - root@fepiliana-A456UR/etc/snort/rules
GNU nano 2.5.3 File: web-misc.rules
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt"; flow:to_server,established; flowbits:is$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting attempt"; flow:to_server,established; content:"<SCRIPT>"; nocase; classtyp$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting HTML Image tag set to javascript attempt"; flow:to_server,established; con$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Cisco IOS HTTP configuration attempt"; flow:to_server,established; uricontent:"/level/"; uricon$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise DOS"; flow:to_server,established; content:"REVLOG / "; depth:9; reference:b$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise directory listing attempt"; flow:to_server,established; content:"INDEX "; d$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC iPlanet GETPROPERTIES attempt"; flow:to_server,established; content:"GETPROPERTIES"; depth:13; $
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Tomcat view source attempt"; flow:to_server,established; uricontent:"%252ejsp"; reference:bugtr$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC ftp attempt"; flow:to_server,established; content:"ftp.exe"; nocase; classtype:web-application-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_enumsn attempt"; flow:to_server,established; content:"xp_enumsn"; nocase; classtype:web-app$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_filelist attempt"; flow:to_server,established; content:"xp_filelist"; nocase; classtype:web-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_availablemedia attempt"; flow:to_server,established; content:"xp_availablemedia"; nocase; cl$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_cmdshell attempt"; flow:to_server,established; content:"xp_cmdshell"; nocase; classtype:web-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC nc.exe attempt"; flow:to_server,established; content:"nc.exe"; nocase; classtype:web-application-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC wsh attempt"; flow:to_server,established; content:"wsh.exe"; nocase; classtype:web-application-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC rcmd attempt"; flow:to_server,established; uricontent:"rcmd.exe"; nocase; classtype:web-appliac$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC telnet attempt"; flow:to_server,established; content:"telnet.exe"; nocase; classtype:web-applics$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC net attempt"; flow:to_server,established; content:"net.exe"; nocase; classtype:web-application-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC tftp attempt"; flow:to_server,established; content:"tftp.exe"; nocase; classtype:web-applicatio$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regread attempt"; flow:to_server,established; content:"xp_regread"; nocase; classtype:web-app$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regwrite attempt"; flow:to_server,established; content:"xp_regwrite"; nocase; classtype:web-$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regdeletekey attempt"; flow:to_server,established; content:"xp_regdeletekey"; nocase; classt$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC WebDAV search access"; flow:to_server,established; content:"SEARCH "; depth:8; nocase; referenc$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC .htpasswd access"; flow:to_server,established; content:".htpasswd"; nocase; classtype:web-applis$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Lotus Domino directory traversal"; flow:to_server,established; uricontent:".nsf/"; uricontent:"$
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC webhits.exe access"; flow:to_server,established; uricontent:"/scripts/samples/search/webhits.$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC queryhit.htm access"; flow:to_server,established; uricontent:"/samples/search/queryhit.htm"; nos$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC counter.exe access"; flow:to_server,established; uricontent:"/counter.exe"; nocase; reference:b$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC WebDAV propfind access"; flow:to_server,established; content:"propfind"; nocase; pcre:"/<a>\x3a/$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC unify eWave ServletExec upload"; flow:to_server,established; uricontent:"/servlet/com.unify.sers$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Servers suite DOS"; flow:to_server,established; uricontent:"/dsgw/bin/search?context="$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC amazon 1-click cookie theft"; flow:to_server,established; content:"ref%3Cscript%20language%3D%2$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC unify eWave ServletExec DOS"; flow:to_server,established; uricontent:"/servlet/ServletExec"; re$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Allaire JRUN DOS attempt"; flow:to_server,established; uricontent:"/servlet/....."; nocase; re$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC ICQ Webfront HTTP DOS"; flow:to_server,established; uricontent:"propfind"; reference:bugtraq,$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Talentsoft Web+ Source Code view access"; flow:to_server,established; uricontent:"/webplus.exe?e$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Talentsoft Web+ Internal IP Address access"; flow:to_server,established; uricontent:"/webplus.es$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC SmartWin CyberOffice Shopping Cart access"; flow:to_server,established; uricontent:"private/sh$
```

Gambar 7: rules alert WEB-MISC

Alert WEB-MISC

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt"; flow:to_server,established; flowbits:is$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello Challenge Length overflow attempt"; flow:to_server,established; flowbits:isnotset,ss$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting attempt"; flow:to_server,established; content:"<SCRIPT>"; nocase; classtyp$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting HTML Image tag set to javascript attempt"; flow:to_server,established; con$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Cisco IOS HTTP configuration attempt"; flow:to_server,established; uricontent:"/level/"; uricon$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise DOS"; flow:to_server,established; content:"REVLOG / "; depth:9; reference:b$
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise directory listing attempt"; flow:to_server,established; content:"INDEX "; d$
```



Alert WEB-MISC

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_availablemedia attempt";
flow:to_server,established; content:"xp_availablemedia"; nocase; cl$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_cmdshell attempt";
flow:to_server,established; content:"xp_cmdshell"; nocase; classtype:web-$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC nc.exe attempt";
flow:to_server,established; content:"nc.exe"; nocase; classtype:web-applicatio$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC wsh attempt";
flow:to_server,established; content:"wsh.exe"; nocase; classtype:web-application-$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC rcmd attempt";
flow:to_server,established; uricontent:"rcmd.exe"; nocase; classtype:web-applica$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC telnet attempt";
flow:to_server,established; content:"telnet.exe"; nocase; classtype:web-applie$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC net attempt";
flow:to_server,established; content:"net.exe"; nocase; classtype:web-application-$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC tftp attempt";
flow:to_server,established; content:"tftp.exe"; nocase; classtype:web-applicatio$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regread attempt";
flow:to_server,established; content:"xp_regread"; nocase; classtype:web-ap$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regwrite attempt";
flow:to_server,established; content:"xp_regwrite"; nocase; classtype:web-$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_regdeletekey attempt";
flow:to_server,established; content:"xp_regdeletekey"; nocase; classt$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC .htpasswd access";
flow:to_server,established; content:".htpasswd"; nocase; classtype:web-appli$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Lotus Domino directory
traversal"; flow:to_server,established; uricontent:".nsf/"; uricontent:"$

# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC webhits.exe access";
flow:to_server,established; uricontent:"/scripts/samples/search/webhits.$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC queryhit.htm access";
flow:to_server,established; uricontent:"/samples/search/queryhit.htm"; no$

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC counter.exe access";
flow:to_server,established; uricontent:"/counter.exe"; nocase; reference:b$
```



Nama : FEPILIANA | Nim : 09011181320024
TUGAS 04 KEAMANAN JARINGAN KOMPUTER

```
Terminal - root@fepiliana-A456UR /etc/snort/rules
File Edit View Terminal Tabs Help
GNU nano 2.5.3 File: icmp-info.rules
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Registration Reply"; icode:0; itype:36; classtype:misc-activity; sid:421; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Registration Reply undefined code"; icode:>0; itype:36; classtype:misc-activity; sid:422; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Registration Request"; icode:0; itype:35; classtype:misc-activity; sid:423; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Registration Request undefined code"; icode:>0; itype:35; classtype:misc-activity; sid:424; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Parameter Problem Bad Length"; icode:2; itype:12; classtype:misc-activity; sid:425; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Parameter Problem Missing a Required Option"; icode:1; itype:12; classtype:misc-activity; sid:426; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Parameter Problem Unspecified Error"; icode:0; itype:12; classtype:misc-activity; sid:427; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Parameter Problem undefined Code"; icode:>2; itype:12; classtype:misc-activity; sid:428; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris Reserved"; icode:0; itype:40; classtype:misc-activity; sid:429; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris Unknown Security Parameters Index"; icode:1; itype:40; classtype:misc-activity; sid:430; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris Valid Security Parameters, But Authentication Failed"; icode:2; itype:40; classtype:misc-activity; sid:431; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris Valid Security Parameters, But Decryption Failed"; icode:3; itype:40; classtype:misc-activity; sid:432; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris undefined code!"; icode:>3; itype:40; classtype:misc-activity; sid:433; rev:8;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Redirect for TOS and Host"; icode:3; itype:5; classtype:misc-activity; sid:436; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Redirect for TOS and Network"; icode:2; itype:5; classtype:misc-activity; sid:437; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Redirect undefined code"; icode:>3; itype:5; classtype:misc-activity; sid:438; rev:9;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Reserved for Security Type 19"; icode:0; itype:19; classtype:misc-activity; sid:439; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Reserved for Security Type 19 undefined code"; icode:>0; itype:19; classtype:misc-activity; sid:440; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Router Advertisement"; icode:0; itype:9; reference:arachnids,173; classtype:misc-activity; sid:441; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Router Selection"; icode:0; itype:10; reference:arachnids,174; classtype:misc-activity; sid:443; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP SKIP"; icode:0; itype:39; classtype:misc-activity; sid:445; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP SKIP undefined code"; icode:>0; itype:39; classtype:misc-activity; sid:446; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench undefined code"; icode:>0; itype:4; classtype:misc-activity; sid:448; rev:7;)
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Time-To-Live Exceeded in Transit"; icode:0; itype:11; classtype:misc-activity; sid:449; rev:6;)
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Time-To-Live Exceeded in Transit undefined code"; icode:>1; itype:11; classtype:misc-activity; sid:450; rev:8;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Reply"; icode:0; itype:14; classtype:misc-activity; sid:451; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Reply undefined code"; icode:>0; itype:14; classtype:misc-activity; sid:452; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Request"; icode:0; itype:13; classtype:misc-activity; sid:453; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Request undefined code"; icode:>0; itype:13; classtype:misc-activity; sid:454; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Traceroute"; icode:0; itype:30; classtype:misc-activity; sid:456; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Traceroute undefined code"; icode:>0; itype:30; classtype:misc-activity; sid:457; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 1"; icode:0; itype:1; classtype:misc-activity; sid:458; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 1 undefined code"; itype:1; classtype:misc-activity; sid:459; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 2"; icode:0; itype:2; classtype:misc-activity; sid:460; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 2 undefined code"; itype:2; classtype:misc-activity; sid:461; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 7"; icode:0; itype:7; classtype:misc-activity; sid:462; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP unassigned type 7 undefined code"; itype:7; classtype:misc-activity; sid:463; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING undefined code"; icode:>0; itype:8; classtype:misc-activity; sid:365; rev:8;)
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page ^M- First Line ^M-W WhereIs Next ^M Mark Text
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^V Next Page ^M-/ Last Line ^M-] To Bracket ^M- Copy Text
```

Gambar 8: rules alert ICMP Timestamp

Alert ICMP Timestamp

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Request"; icode:0; itype:13; classtype:misc-activity; sid:453; rev:5;)
```

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Timestamp Request undefined code"; icode:>0; itype:13; classtype:misc-activity; sid:454; rev:7;)
```



Alert ICMP PING

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING BSDtype"; itype:8; content:"|08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17|"; depth:32; reference:arach\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING BayRS Router"; itype:8; content:"|01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F|"; depth:32; reference:ara\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING BeOS4.x"; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 08 09 0A 0B|"; depth:32; reference:arach\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Cisco Type.x"; itype:8; content:"|AB CD AB CD AB CD AB CD AB CD AB CD AB CD|"; depth:32; reference:\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Delphi-Piette Windows"; itype:8; content:"Pinging from Del"; depth:32; reference:arachnids,155; classtype\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Flowpoint2200 or Network Management Software"; itype:8; content:"|01 02 03 04 05 06 07 08 09 0A 0B 0C 0D \$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING IP NetMonitor Macintosh"; itype:8; content:"|A9| Sustainable So"; depth:32; reference:arachnids,157; clas\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING LINUX/*BSD"; dsize:8; id:13170; itype:8; reference:arachnids,447; classtype:misc-activity; sid:375; rev:6\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Microsoft Windows"; itype:8; content:"0123456789abcdefghijklmnop"; depth:32; reference:arachnids,159; cla\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Network Toolbox 3 Windows"; itype:8; content:"===== "; depth:32; reference:arachnids,161; class\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Ping-O-MeterWindows"; itype:8; content:"OMeterObeseArmad"; depth:32; reference:arachnids,164; classtype:m\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Pinger Windows"; itype:8; content:"Data|00 00 00 00 00 00 00 00 00 00 00 00|"; depth:32; reference:arachn\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Seer Windows"; itype:8; content:"|88 04| "; depth:32; reference:arachnids,166; classtype:mis\$

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Sun Solaris"; dsize:8; itype:8; reference:arachnids,448; classtype:misc-activity; sid:381; rev:6;)

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING Windows"; itype:8; content:"abcdefghijklmnop"; depth:16; reference:arachnids,169; classtype:misc-activity\$

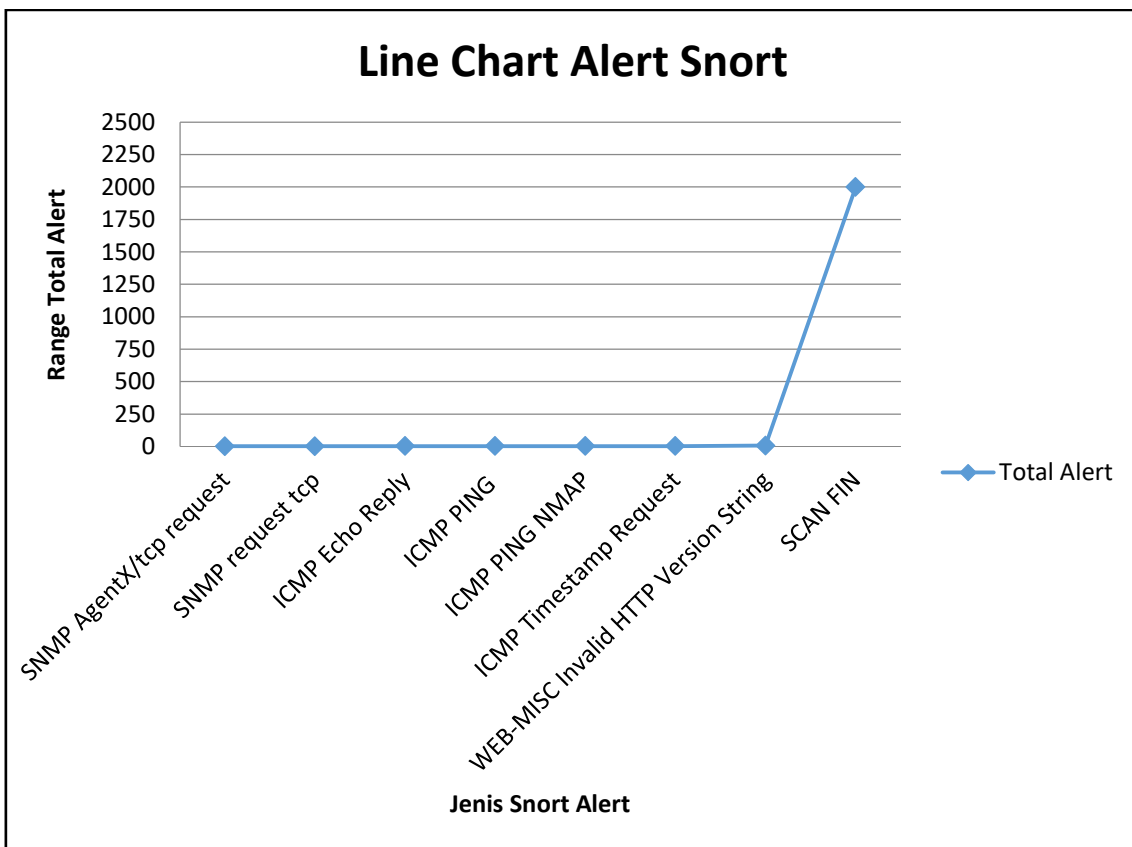
alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP traceroute"; itype:8; ttl:1; reference:arachnids,118; classtype:attempted-recon; sid:385; rev:4;)

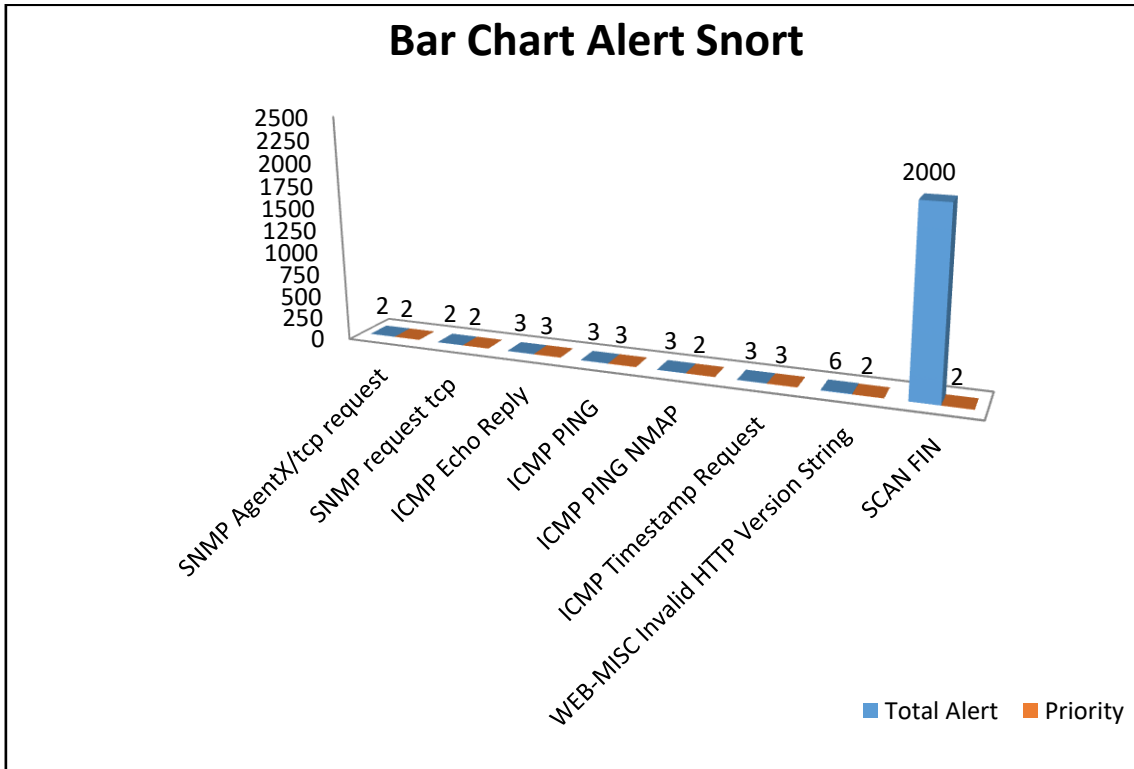
alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP PING"; icode:0; itype:8; classtype:misc-activity; sid:384; rev:5;)



➤ Tabel Alert Snort dan Diagramnya

No	Jenis Alert	Total	Prioritas
1.	SNMP AgentX/tcp request	2	2
2.	SNMP request tcp	2	2
3.	ICMP Echo Reply	3	3
4.	ICMP PING	3	3
5.	ICMP PING NMAP	3	2
6.	ICMP Timestamp Request	3	3
7.	WEB-MISC Invalid HTTP Version String	6	2
8.	SCAN FIN	2000	2





Daftar Pustaka

- [1] M. Affandi and S. Setyowibowo, “Implementasi Snort Sebagai Alat Pendeteksi Intrusi,” vol. 4, no. 2.
- [2] M. Jannah, Hustinawati, and R. Wildani, “Implementasi Intrusion System (Ids) Snort Pada Laboratorium Jaringan Komputer,” *UG J.*, vol. 6 No 5, pp. 1–4, 2012.
- [3] M. Ridwan Zalbina, “Sistem Deteksi HTTP Inspect Preprocessor dan Rule Options”, 2016

