

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* berdasarkan kejanggalan yang terjadi pada pola lalulintas 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*:

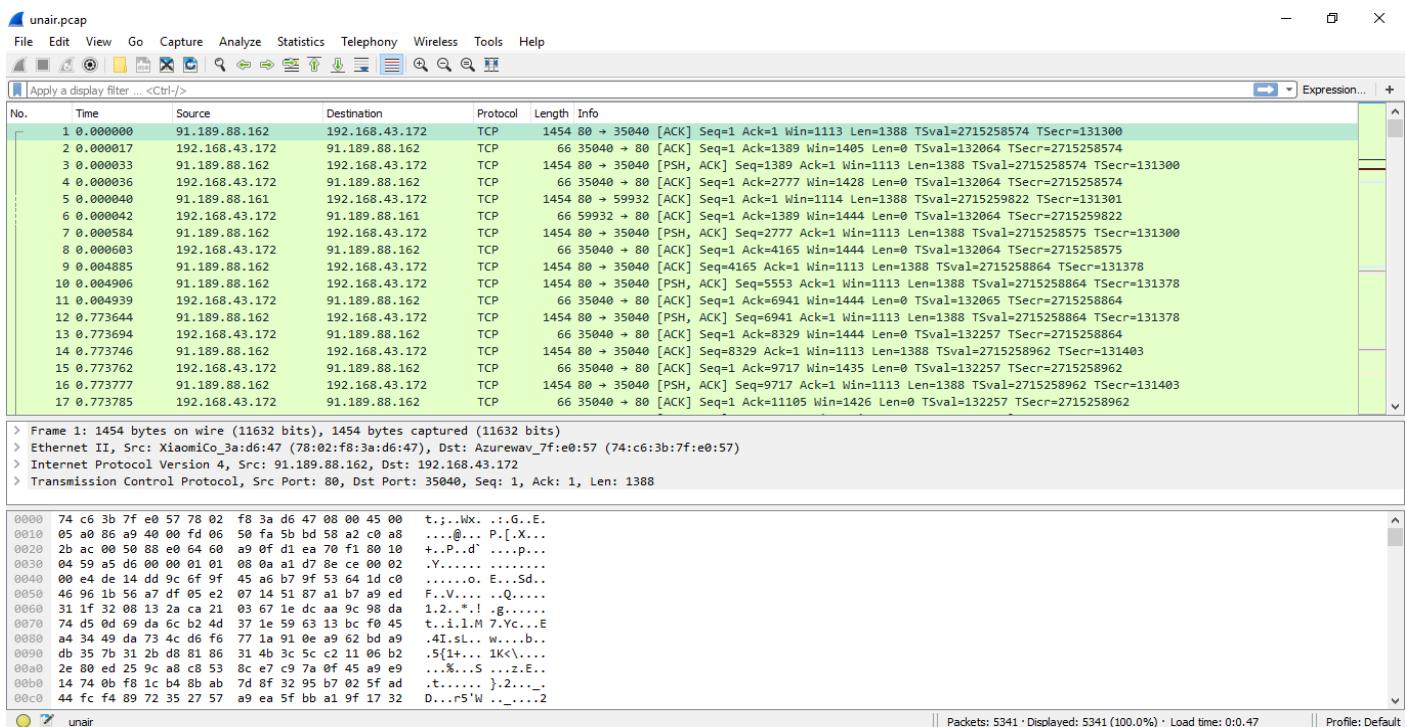
- Wireshark: digunakan untuk *capture paket*
- Nmap: digunakan untuk melakukan *scanning target*
- Snort: digunakan untuk deteksi IDS
- Program counteralert.py: digunakan untuk mendapatkan total dan *priority* dari hasil log alert snort.



➤ 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 sedatail 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.



Gambar 1: hasil capture Wireshark scanning target

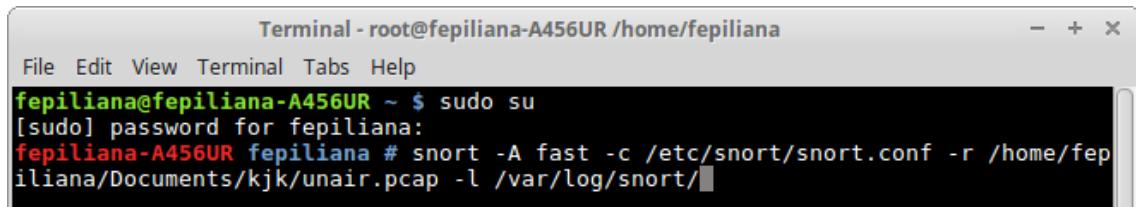
➤ Snort dan Program counteralert.py

Pada penggerjaan 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 penggerjaan 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.

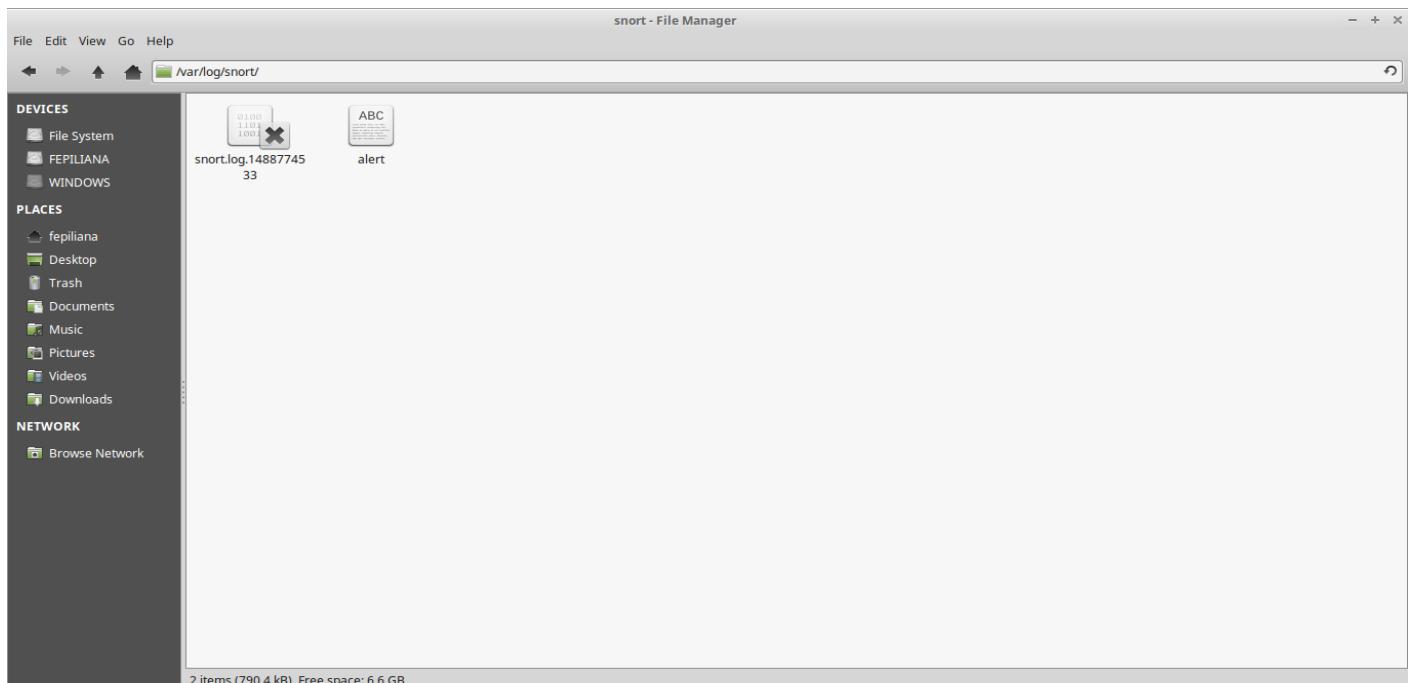
Untuk menjalankan snort pada sistem operasi Linux, kita gunakan *command* `snort -A fast -c /etc/snort/snort.conf -r (masukan_path_file_pcaps) -l /var/log/snort.`



```
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/fep
iliana/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.



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

Pada gambar 3, dapat kita lihat terdapat sebuah file yang bernama alert pada direktori /var/log/snort. Berikut ada beberapa isi dari file alert:

```
alert.(/var/log/snort)
File Edit View Search Tools Documents Help
Open Save Undo Redo Cut Copy Paste Find Find Next
alert.x
03/06-11:19:06.578942 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:33228 -> 91.189.91.23:80
03/06-11:19:08.410216 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:08.410216 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:08.410306 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:10.412831 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:10.412911 [**] [1:453:5] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:10.412911 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:13.644671 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 210.57.208.72 -> 192.168.43.172
03/06-11:19:15.741103 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 210.57.208.72 -> 192.168.43.172
03/06-11:19:18.561224 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:39218 -> 91.189.88.152:80
03/06-11:19:24.610600 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:39218 -> 91.189.88.152:80
03/06-11:19:24.663024 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:39220 -> 91.189.88.152:80
03/06-11:19:35.088412 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:56522 -> 91.189.88.149:80
03/06-11:19:45.790940 [**] [1:2570:7] WEB-MISC Invalid HTTP Version String [**] [Classification: Detection of a non-standard protocol or event] [Priority: 2] {TCP}
192.168.43.172:59492 -> 91.189.88.161:80
03/06-11:19:53.450266 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:53.450266 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:53.450366 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.172 -> 210.57.208.72
03/06-11:19:53.622132 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 210.57.208.72 -> 192.168.43.172
03/06-11:20:06.686251 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:23
03/06-11:20:06.686304 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5900
03/06-11:20:06.686319 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:53
03/06-11:20:06.686330 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:22
03/06-11:20:06.686341 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:80
03/06-11:20:06.686351 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:8888
03/06-11:20:06.686360 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:3306
03/06-11:20:06.686369 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1720
03/06-11:20:06.686379 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:445
03/06-11:20:06.686391 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:21
03/06-11:20:07.929983 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49343 -> 210.57.208.72:21
03/06-11:20:07.930038 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49343 -> 210.57.208.72:445
03/06-11:20:07.930053 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49343 -> 210.57.208.72:1720
03/06-11:20:07.930064 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49343 -> 210.57.208.72:3306
03/06-11:20:08.275715 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:631
03/06-11:20:08.275725 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:306
03/06-11:20:08.275735 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:50636
03/06-11:20:08.275745 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:30000
03/06-11:20:08.275754 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5922
03/06-11:20:08.275763 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:11111
03/06-11:20:08.275773 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:65129
03/06-11:20:08.275782 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:49175
03/06-11:20:08.275792 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:9535
03/06-11:20:08.275802 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:2725
03/06-11:20:08.275813 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5911
03/06-11:20:08.275824 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1201
03/06-11:20:08.275833 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:2382
03/06-11:20:08.275844 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5030
03/06-11:20:08.275853 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:30718
03/06-11:20:08.275864 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:6901
03/06-11:20:08.275874 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:18101
03/06-11:20:08.275885 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5959
03/06-11:20:08.275894 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5544
03/06-11:20:08.275903 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1185
03/06-11:20:08.275913 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:52673
03/06-11:20:08.275922 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:3878
03/06-11:20:08.275931 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5800
03/06-11:20:08.275941 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1038
03/06-11:20:08.275951 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:4129
03/06-11:20:08.275962 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1113
03/06-11:20:08.275973 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1434
03/06-11:20:08.275983 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:280
03/06-11:20:08.275993 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:545
03/06-11:20:08.276002 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1875
03/06-11:20:08.276011 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:8402
03/06-11:20:08.276020 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:6788
03/06-11:20:08.276030 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:8222
03/06-11:20:08.276041 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:5560
03/06-11:20:08.276051 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1433
03/06-11:20:08.276060 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:8180
03/06-11:20:08.276069 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:3000
03/06-11:20:08.276080 [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.172:49342 -> 210.57.208.72:1062
```

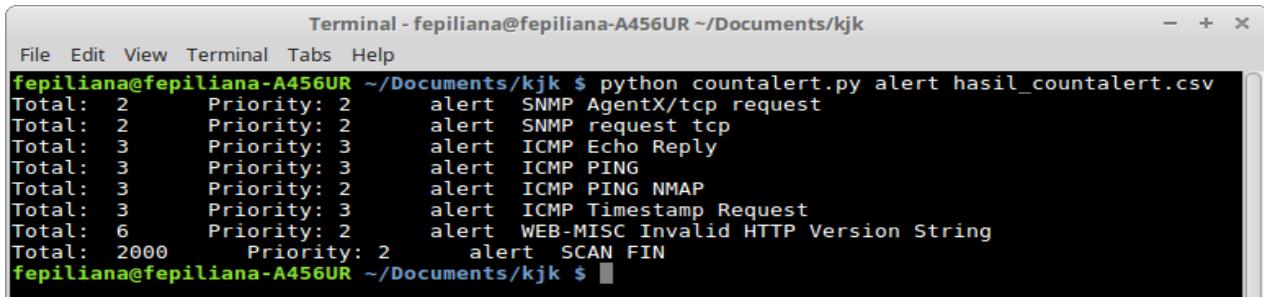
Plain Text ▾ Tab Width: 4 ▾ Ln 32, Col 11 INS

Gambar 4: isi file 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 counteralert.py untuk mendapatkan total dan *priority* dari setiap jenis alert. Program counteralert.py merupakan program yang berbasis bahasa Python. Untuk menjalankan program tersebut kita ketik di *command linux* :

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

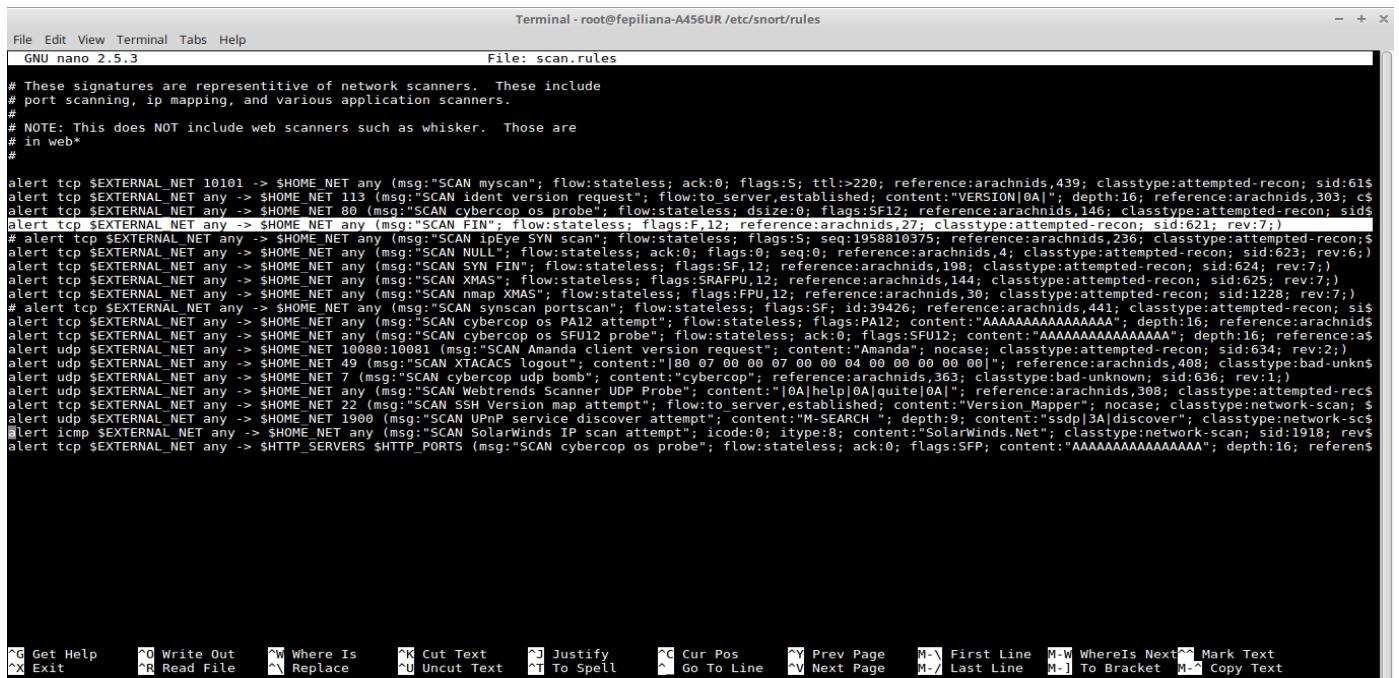


```
Terminal - fepiliana@fepiliana-A456UR ~/Documents/kjk
File Edit View Terminal Tabs Help
fepiliana@fepiliana-A456UR ~/Documents/kjk $ python counteralert.py alert hasil_countalert.csv
Total: 2 Priority: 2 alert SNMP AgentX/tcp request
Total: 2 Priority: 2 alert SNMP request tcp
Total: 3 Priority: 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 dicocokan 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 -> $HOME_NET any (msg:"SCAN myscan"; flow:stateless; ack:0; flags:S; ttl:>220; reference:arachnids,439; classtype:attempted-recon; sid:61$)
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; dsz:0; flags:SF12; reference:arachnids,146; classtype:attempted-recon; sids
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; s
alert tcp $EXTERNAL_NET any (msg:"SCAN NULL"; flow:stateless; ack:0; flags:O; 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 (msg:"SCAN XMAS"; flow:stateless; flags:SFPU,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:FFPU,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:S; id:39426; reference:arachnids,441; classtype:attempted-recon; sis
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN cybercop os PA12 attempt"; flow:stateless; flags:PA12; content:"AAAAAAAAAAAAAAA"; depth:16; reference:arachnids
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN cybercop os SFU12 probe"; flow:stateless; ack:0; flags:SFU12; content:"AAAAAAAAAAAAAAA"; depth:16; reference:arachnids
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 04 00 00 00 00 00 00 00|"; reference:arachnids,408; classtype:bad-unkns
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 tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN Webtrends Scanner UDP Probe"; content:"|0A|help|0A|quit|0A|"; reference:arachnids,308; classtype:attempted-reco
alert udp $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 icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN UPnP service discover attempt"; flow:to_server,established; content:"M-SEARCH "; depth:9; content:"ssdp|3A|discover"; classtype:network-scan; sid:1918; rev
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN cybercop os probe"; flow:stateless; ack:0; flags:SFP; content:"AAAAAAAAAAAAAAA"; depth:16; referen
```

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@fepliana-A456UR /etc/snort/rules

```
File Edit View Terminal Tabs Help
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 -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello Challenge Length overflow attempt"; flow:to_server,established; flowbits:isnotset,ss$)
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 $HTTP_PORTS (msg:"WEB-MISC Cisco IOS HTTP configuration attempt"; flow:to_server,established; uricontent:"/level/"; uricon$)
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 $HTTP_PORTS (msg:"WEB-MISC iPlanet GETPROPERTIES attempt"; flow:to_server,established; content:"GETPROPERTIES"; depth:13; s$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Tomcat view source attempt"; flow:to_server,established; uricontent:"%252ejsp"; reference:bugtrs$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC ftp attempt"; flow:to_server,established; content:"ftp.exe"; nocase; classtype:web-application-s$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_enumdsn attempt"; flow:to_server,established; content:"xp_enumdsn"; nocase; classtype:web-aps$)
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 $HTTP_PORTS (msg:"WEB-MISC xp_availablemedia attempt"; flow:to_server,established; content:"xp_availablemedia"; nocase; clt$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_cmdbshell attempt"; flow:to_server,established; content:"xp_cmdbshell"; nocase; classtype:web-s$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC nc.exe attempt"; flow:to_server,established; content:"nc.exe"; nocase; classtype:web-applications$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC wsh attempt"; flow:to_server,established; content:"wsh.exe"; nocase; classtype:web-applications$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC rcmd attempt"; flow:to_server,established; uricontent:"rcmd.exe"; nocase; classtype:web-applications$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC telnet attempt"; flow:to_server,established; content:"telnet.exe"; nocase; classtype:web-applications$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC net attempt"; flow:to_server,established; content:"net.exe"; nocase; classtype:web-application-s$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC tftp attempt"; flow:to_server,established; content:"tftp.exe"; nocase; classtype:web-applications$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_reread attempt"; flow:to_server,established; content:"xp_reread"; nocase; classtype:web-aps$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_rewrite attempt"; flow:to_server,established; content:"xp_rewrite"; nocase; classtype:web-$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC xp_redeletekey attempt"; flow:to_server,established; content:"xp_redeletekey"; nocase; classts$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC WebDAV search access"; flow:to_server,established; content:"SEARCH "; depth:8; nocase; references$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC .htpasswd access"; flow:to_server,established; content:".htpasswd"; nocase; classtype:web-applications$)
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 $HTTP_PORTS (msg:"WEB-MISC webhbits.exe access"; flow:to_server,established; uricontent:"/scripts/samples/search/webhbits.s$)
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 $HTTP_PORTS (msg:"WEB-MISC counter.exe access"; flow:to_server,established; uricontent:"/counter.exe"; nocase; reference:bs$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Webpropfind access"; flow:to_server,established; content:"propfind"; nocase; pcre:"/<a>x3a$")
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC unify eWave ServletExec upload"; flow:to_server,established; uricontent:"/servlet/com.unify.ser$)
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 $HTTP_PORTS (msg:"WEB-MISC amazon 1-click cookie theft"; flow:to_server,established; content:"ref%3Cscript%20language%3Dzs$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC unify eWave ServletExec DOS"; flow:to_server,established; uricontent:"/servlet/ServletExec"; res$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Allaire JRUN DOS attempt"; flow:to_server,established; uricontent:"servlet/....."; nocase; res$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC ICQ Webfront HTTP DOS"; flow:to_server,established; uricontent: "?????????"; reference:bugtraq,$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Talentsoft Web+ Source Code view access"; flow:to_server,established; uricontent:"/webplus.exe?$")
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Talentsoft Web+ internal IP Address access"; flow:to_server,established; uricontent:"/webplus.e$)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC CyberWin Office Shopping Cart access"; flow:to_server,established; uricontent:" private/shs$)

^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   ^U Replace   ^L Uncut Text   ^T To Spell   ^A Go To Line   ^N Next Page   M-[ Last Line   M-] To Bracket   M-^ Copy Text
```

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 $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise directory listing attempt"; flow:to_server,established; content:"INDEX "; d$)
```

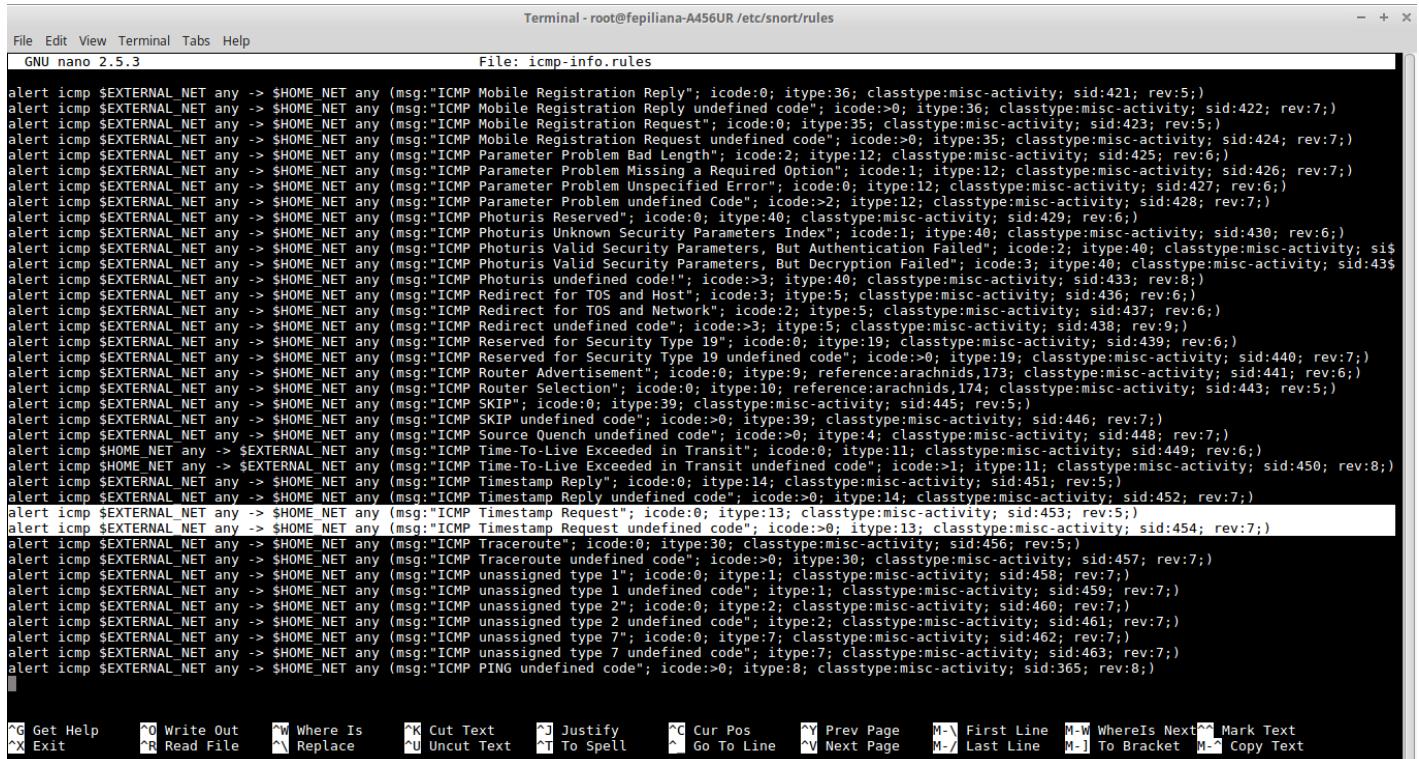


Alert WEB-MISC

```
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 $HTTP_PORTS (msg:"WEB-MISC telnet attempt"; flow:to_server,established; content:"telnet.exe"; nocase; classtype:web-applic$  
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@fepliana-A456UR /etc/snort/rules
File Edit View Terminal Tabs Help
File: icmp-info.rules
GNU nano 2.5.3

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 code1"; 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 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:rachnids: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 $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"; icode: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"; icode: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"; icode: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;)
```

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;)
```



Nama : FEPILIANA | Nim : 09011181320024

TUGAS 04 KEAMANAN JARINGAN KOMPUTER

Gambar 9: rules alert ICMP PING NMAP

Alert ICMP PING NMAP

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsizer:0; itype:8; reference:arachnids,162; classtype:attempted-recon; sid:469; rev:3;)
```



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

Gambar 9: rules alert ICMP PING

Alert ICMP PING

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING *NIX"; itype:8; content:"|10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|"; depth:32; classtype:misc-act$
```



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 -> $HOME_NET any (msg:"ICMP PING BeOS4.x"; itype:8; content:"|00 00 00 00  
00 00 00 00 00 00 00 08 09 0A 0B|"; depth:32; reference:arach$  
  
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 -> $HOME_NET any (msg:"ICMP PING LINUX/*BSD"; dsiz:8; id:13170; itype:8;  
reference:arachnids,447; classtype:misc-activity; sid:375; rev:6$  
  
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Microsoft Windows"; itype:8;  
content:"0123456789abcdefghijklmnopqrstuvwxyz"; depth:32; reference:arachnids,159; cla$  
  
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"; dsiz:8; itype:8;  
reference:arachnids,448; classtype:misc-activity; sid:381; rev:6;)  
  
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Windows"; itype:8;  
content:"abcdefghijklmnopqrstuvwxyz"; depth:16; reference:arachnids,169; classtype:misc-activity$  
  
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;)
```



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

```

Terminal - root@fepliana-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 Destination Unreachable for Type of Service"; icode:11; itype:3; classtype:misc-activity; sid:401; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Network Unreachable"; icode:0; itype:3; classtype:misc-activity; sid:402; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Port Unreachable"; icode:1; itype:3; classtype:misc-activity; sid:403; revs
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Precedence Unreachable"; icode:2; itype:3; classtype:misc-activity; sid:404; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Protocol Unreachable"; icode:2; itype:3; classtype:misc-activity; sid:405; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Source Host Isolated"; icode:2; itype:3; classtype:misc-activity; sid:406; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable Source Route Failed"; icode:5; itype:3; classtype:misc-activity; sid:407; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable undefined code"; icode:15; itype:3; classtype:misc-activity; sid:407; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Echo Reply"; icode:0; itype:0; classtype:misc-activity; sid:408; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Echo Reply undefined code"; icode:>0; itype:0; classtype:misc-activity; sid:409; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Fragment Reassembly Time Exceeded"; icode:1; itype:11; classtype:misc-activity; sid:410; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP IPv6 I-Am-Here"; icode:0; itype:34; classtype:misc-activity; sid:411; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP IPv6 I-Am-Here undefined code"; icode:>0; itype:34; classtype:misc-activity; sid:412; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP IPv6 Where-Are-You"; icode:0; itype:33; classtype:misc-activity; sid:413; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP IPv6 Where-Are-You undefined code"; icode:>0; itype:33; classtype:misc-activity; sid:414; rev:7;)
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Information Reply"; icode:0; itype:16; classtype:misc-activity; sid:415; rev:5;)
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Information Reply undefined code"; icode:>0; itype:16; classtype:misc-activity; sid:416; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Information Request"; icode:0; itype:15; classtype:misc-activity; sid:417; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Information Request undefined code"; icode:>0; itype:15; classtype:misc-activity; sid:418; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Host Redirect"; icode:0; itype:32; classtype:misc-activity; sid:419; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Mobile Host Redirect undefined code"; icode:>0; itype:32; classtype:misc-activity; sid:420; rev:7;)
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:8;)
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 Unexpected Option"; icode:0; itype:5; classtype:misc-activity; sid:427; rev:6;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photon Reserved"; icode:0; itype:4; classtype:misc-activity; sid:428; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Photuris Unknown Security Parameters Index"; icode:1; itype:40; classtype:misc-activity; sid:429; 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:430; 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:431; rev:6;)
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 undefined code"; icode:>3; itype:5; classtype:misc-activity; sid:437; rev:6;)
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;)

^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  ^U Replace   ^E Uncut Text ^T To Spell   ^I Go To Line  ^V Next Page   M-/ Last Line   M-] To Bracket M-^ Copy Text

```

Gambar 10: rules alert ICMP Echo Reply

Alert ICMP Echo Reply

```

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Echo Reply"; icode:0; itype:0; classtype:misc-activity; sid:408; rev:5;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Echo Reply undefined code"; icode:>0; itype:0; classtype:misc-activity; sid:409; rev:7;)

```

```

Terminal - root@fepliana-A456UR /etc/snort/rules
File Edit View Terminal Tabs Help
GNU nano 2.5.3
File: snmp.rules

# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created, tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
# rules that were created by Sourcefire and other third parties and
# distributed under the GNU General Public License (the "GPL Rules"). The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
# Reserved. All other GPL Rules are owned and copyrighted by their
# respective owners (please see www.snort.org/contributors for a list of
# owners and their respective copyrights). In order to determine what
# rules are VRT Certified Rules or GPL Rules, please refer to the VRT
# Certified Rules License Agreement.
#
#
# $Id: snmp.rules,v 1.17.2.1.2.1 2005/05/16 22:17:52 mwatchinski Exp $
#
# SNMP RULES
#
#
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP missing community string attempt"; content:"|04 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:cve
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP null community string attempt"; content:"|04 01 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:bugs
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt"; content:"|02 01 00 04 82 01 00|"; offset:4; reference:bugtraq,408
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt with evasion"; content:"|04 82 01 00|"; depth:5; offset:7; referes
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access udp"; content:"public"; reference:bugtraq,2112; reference:bugtraq,4088; reference:bugtraq,4089; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access tcp"; content:"public"; reference:bugtraq,2112; reference:bugtraq,4088; reference:bugtraq,4089; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access udp"; content:"private"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access tcp"; content:"private"; reference:bugtraq,4088; reference:bugtraq,4088; reference:bugtraq,4132; rs
alert udp any any -> 255.255.255.161 (msg:"SNMP Broadcast request"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve_2002-0012; rs
alert udp any any -> 255.255.255.162 (msg:"SNMP broadcast trap"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve_2002-0012; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request udp"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve_2002-0012; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request tcp"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve_2002-0012; rs
alert tcp $EXTERNAL_NET any -> $HOME_NET 705 (msg:"SNMP Agent/Tcp request"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; rs
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP PROTOs test-suite-req-app attempt"; content:"06|02 01 00 04 06|[public]A0 19 02 01 00 02 01 00 01 00|0|0E|0|05"; reference:url,www.ee.oulu.fi/s
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"SNMP PROTOs test-suite-trap-app attempt"; content:"08|02 01 00 04 06|[public]A4|+|06"; reference:url,www.ee.oulu.fi/s

^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  ^U Replace   ^E Uncut Text ^T To Spell   ^I Go To Line  ^V Next Page   M-/ Last Line   M-] To Bracket M-^ Copy Text

```

Gambar 11: rules alert SNMP Request



Alert SNMP Request

```
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request udp"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve,2002-0012; $
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request tcp"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:$
```

```
File Edit View Terminal Tabs Help
File: snmp.rules
GNU nano 2.5.3

# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created, tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
# rules that were generated by Sourcefire and other third parties and
# distributed under the GNU General Public License (the "GPL Rules"). The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
# Reserved. All other GPL Rules are owned and copyrighted by their
# respective owners (please see www.snort.org/contributors for a list of
# owners and their respective copyrights). In order to determine what
# rules are VRT Certified Rules or GPL Rules, please refer to the VRT
# Certified Rules License Agreement.
#
#
# $Id: snmp.rules,v 1.17.2.1.2.1 2005/05/16 22:17:52 mwatchinski Exp $
# -----
# SNMP RULES
# -----
#
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP missing community string attempt"; content:"[04 00]"; depth:15; offset:5; reference:bugtraq,2112; reference:cve-2002-0012; reference:bugtraq,4088)
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP null community string attempt"; content:"[04 01 00]"; depth:15; offset:5; reference:bugtraq,2112; reference:bugs,4088)
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt"; content:"[02 01 00 04 82 01 00]"; offset:4; reference:bugtraq,4085)
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt with evasion"; content:"[04 82 01 00]"; depth:4; offset:5; reference:bugtraq,4085)
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access udp"; content:"public"; reference:bugtraq,2112; reference:bugtraq,4088; reference:bugtraq,4089; r$)
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access tcp"; flow:to,server,established; content:"public"; reference:bugtraq,2112; reference:cve-2002-0012; reference:bugtraq,4088)
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access udp"; content:"private"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132;s)
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access tcp"; flow:to,server,established; content:"private"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; s)
alert udp any any -> 255.255.255.255 161 (msg:"SNMP Broadcast request"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve-2002-0012;s)
alert udp any any -> 255.255.255.255 162 (msg:"SNMP broadcast trap"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve-2002-0012; rs)
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request udp"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve-2002-0012; s)
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request tcp"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; references)
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"SNMP trap udp"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve-2002-0012; r$)
alert tcp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"SNMP trap tcp"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cvs)
alert udp $EXTERNAL_NET any -> $HOME_NET 705 (msg:"SNMP AgentX/tcp request"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; re$)
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP PROTOS test-suite-req-app attempt"; content:"[04 02 01 00 04 06]public[A0 19 02 01 00 02 01 00 01 00]@[0E]0[0]s")
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"SNMP PROTOS test-suite-trap-app attempt"; content:"[08 02 01 00 04 06]public[A4]+[06]" ; reference:url,www.ee.uolu.fi/s
```

Gambar 11: rules alert SNMP AgentX/tcp

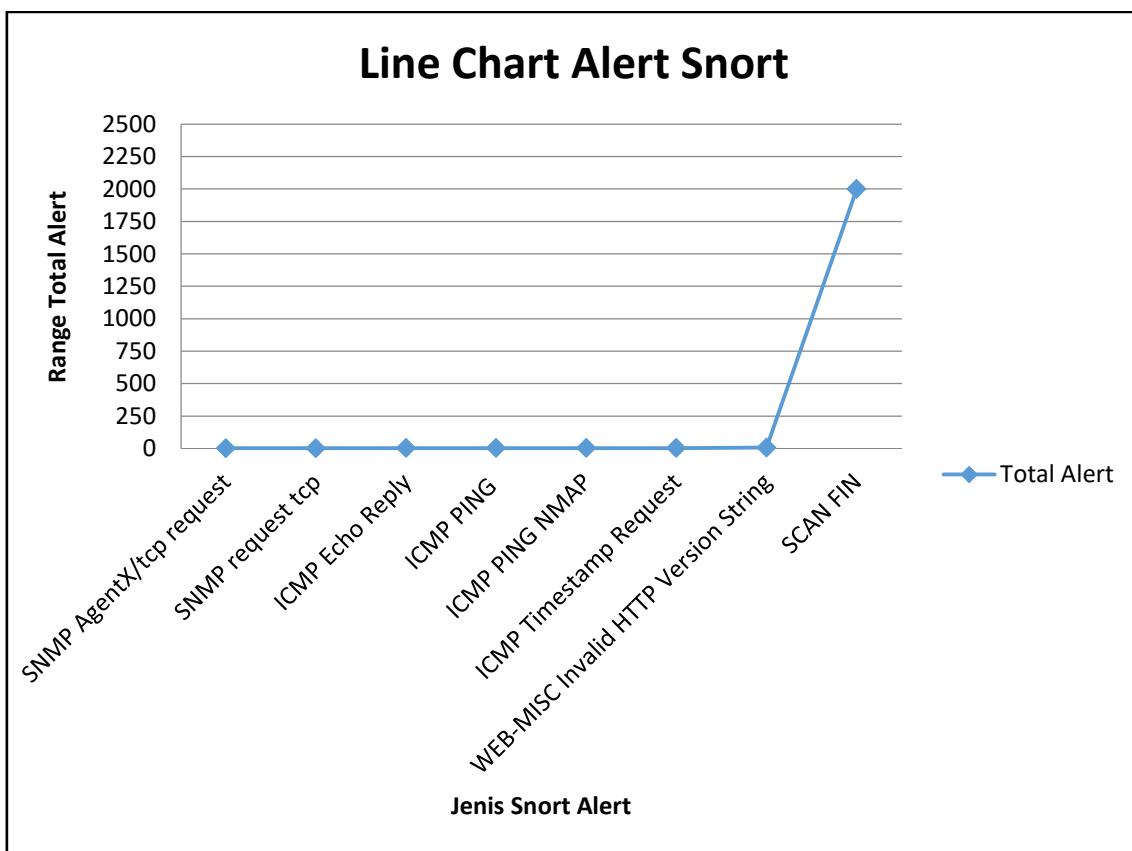
Alert SNMP AgentX/tcp

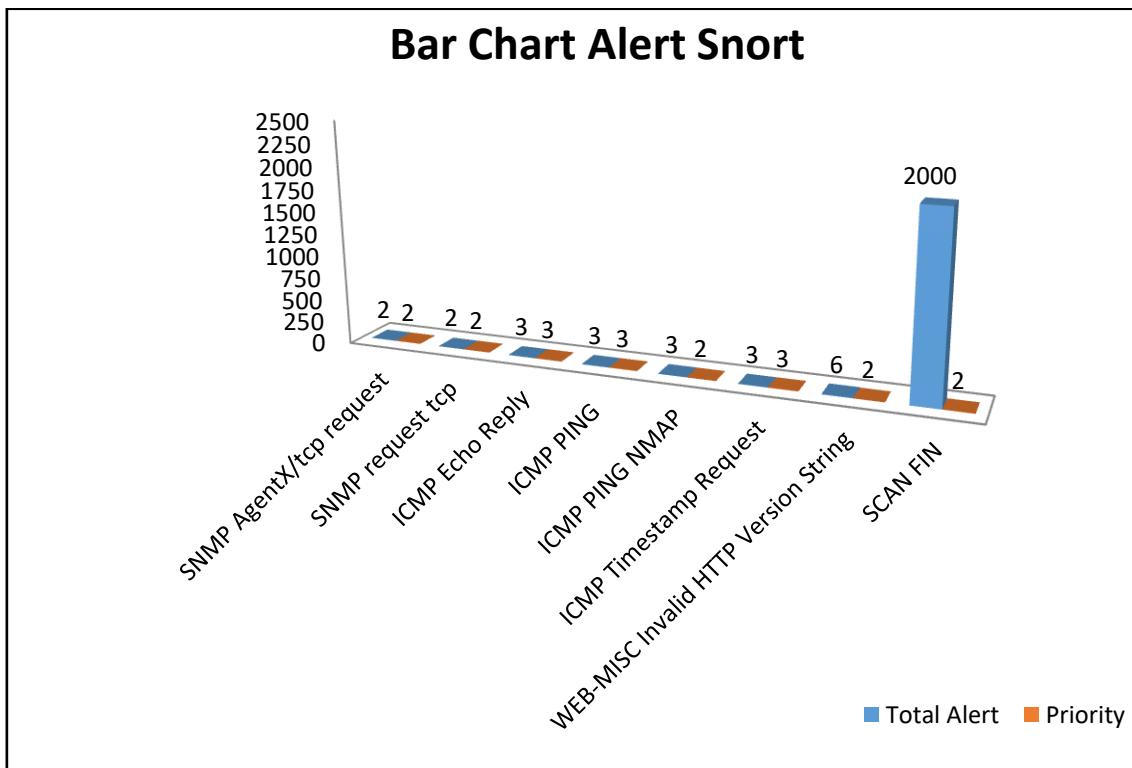
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 705 (msg:"SNMP AgentX/tcp request"; flow:stateless; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; re$
```



➤ 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 Pendekripsi 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

