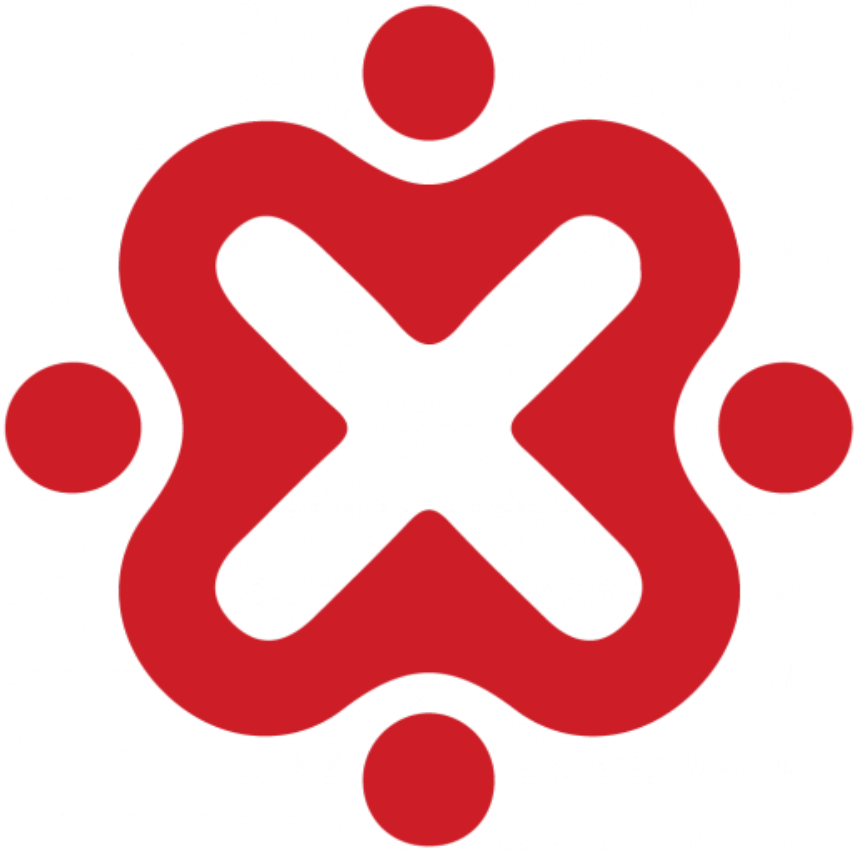
Bootcamp Cyber Security

Materi Minggu 2 (Sesi 2) : Firewall

IDS with SNORT



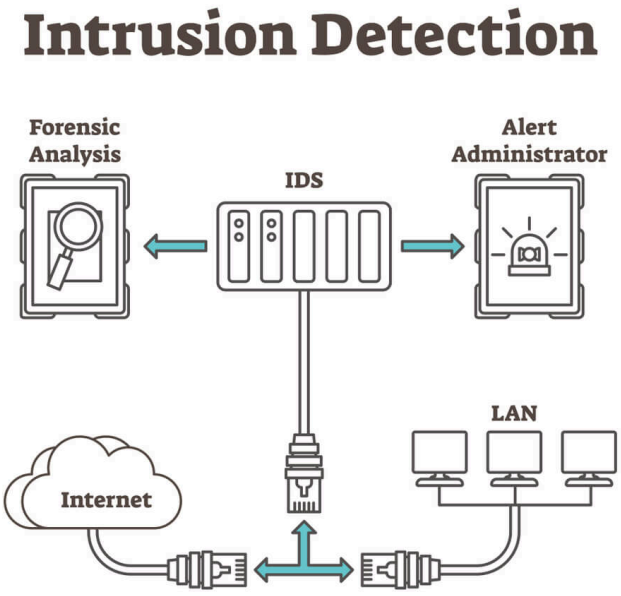
ID-Networkers
Indonesian IT Expert Factory

Table Of Contents

1. Introduction IDS

1.1 Overview

IDS adalah singkatan dari Intrusion Detection System (IDS) sebuah keamanan jaringan yang digunakan untuk mendekteksi adanya aktivity mencurigakan/Tidak sah. IDS ketika mendeteksi adanya pattern/pola mencurigakan, IDS akan langsung memberikan Alert ke Administrator, semisal IDS di intregasikan ke Email maka IDS akan memberikan alert ke email.



1.2 How to Work

- Menganalisis Traffic Jaringan secara pasif
- Menggunakan Signature-based atau Behavior-based Detection
- Jika ditemukan Aktivity mencurigakan , IDS akan mencatat kejadian dan memberikan alert ke Administrator

1.3 Examples Detection IDS

- Port Scanning (Nmap)
- SQL Injection
- Denial of Service (DoS)

- Access tidak sah ke System Internal

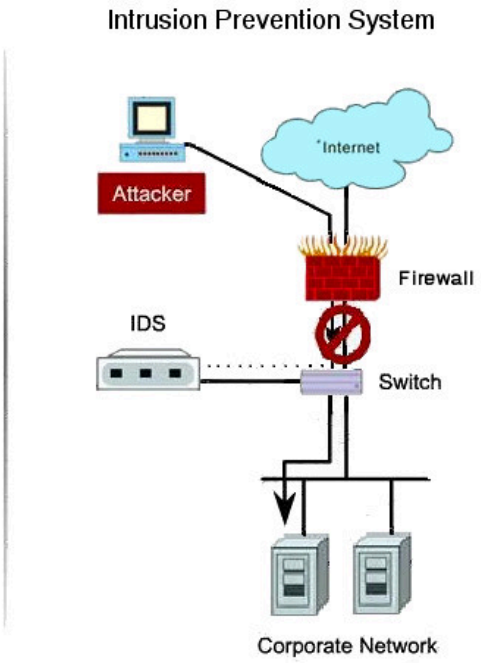
1.4 Example Tools IDS OpenSource

- SNORT
- Suricata
- Bro/Zeek
- OSSEC

2. Introduction to IPS

2.1 Overview

IPS adalah singkatan dari Intrusion Prevention System (IPS) yang dimana itu adalah teknologi keamanan jaringan yang berbeda dengan IDS, karena IPS tidak hanya mendeteksi Ancaman, namun IPS bisa sekaligus otomatis mencegah serangan untuk mengambil tindakan tertentu, seperti Blok IP, Drop Connection,etc.



2.2 How to Work

- Bekerja Inline antara jaringan dan destination (Server /Host)
- Analisis Traffic secara Real-time
- Setelah mendeteksi, IPS akan bekerja memutus koneksi

2.3 Action IPS

- Block Paket jaringan
- Reset Connection TCP
- Block IP Address Penyerang/Attack
- Send Alert ke SIEM/SOC

2.4 Example Tools IPS

- SNORT (ada rules untuk IPS)
- Suricata
- Paloalto Threat Prevention

Practice IDS/IPS in SNORT

1.1 What is SNORT

SNORT adalah tool IDS/IPS Opensource yang di implementasikan langsung di OS , biasa digunakan untuk Firewall Linux. SNORT akan menganalisis Traffic lewat interface jaringan seperti Ethernet, WLAN, etc.

Kelebihan Snort

1. Open Source dan Gratis
2. Komunitas Besar dan Dukungan Luas
3. Fleksibilitas dan Konfigurasi Tinggi

Kekurangan Snort

1. False Positive yang Cukup Tinggi
2. Kurang Efektif untuk Serangan Zero-day
3. Konfigurasi dan Manajemen Rule yang Kompleks

1. How to Install SNORT in Ubuntu 22.04

- **Update & Upgrade Ubuntu**

  sudo apt-get update && sudo apt-get upgrade -y

```
snort@snort-virtual-machine:~$ sudo apt-get update && sudo apt-get upgrade -y
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://id.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  alsa-ucm-conf amd64-microcode apparmor bind9-dnsutils bind9-host bind9-libs bluez bluez-cups bluez-obexd
  bubblewrap ca-certificates cups cups-browsed cups-bsd cups-client cups-common cups-core-drivers cups-daemon
  cups-filters cups-filters-core-drivers cups-ipp-utils cups-ppdc cups-server-common dirmngr distro-info-data
  dmidecode dmsetup dns-root-data fonts-noto-color-emoji fonts-opensymbol ghostscript ghostscript-x
  gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-harfbuzz-0.0 gir1.2-javascriptcoregtk-4.0
  gir1.2-mutter-10 gir1.2-nm-1.0 gir1.2-packagekitglib-1.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0 gjs
  gnome-control-center gnome-control-center-data gnome-control-center-faces gnome-shell gnome-shell-common
  gnome-shell-extension-ubuntu-dock gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server
  gpgconf gpgsm gpgv gstreamer1.0-alsa gstreamer1.0-gl gstreamer1.0-gtk3 gstreamer1.0-packagekit
  gstreamer1.0-plugins-base gstreamer1.0-plugins-base-apps gstreamer1.0-plugins-good gstreamer1.0-pulseaudio
  gstreamer1.0-tools gstreamer1.0-x intel-microcode ipp-usb libabsl20210324 libapparmor1 libarchive13
  libbluetooth3 libc-bin libc6 libc6-dbg libcap2 libcap2-bin libcryptsetup12 libcups2 libcupsfilters1
  libcupsimage2 libcurl3-gnutls libcurl4 libdebuginfod-common libdebuginfod1 libdevmapper1.02.1 libdw1
```

- **Aktifkan fungsi Capture pada Interface.**

  ip a

  ip link show ens33

  sudo ip link set ens33 promisc on

  #disini kita aktifkan fungsi capture pada interface tersebut (ens33)

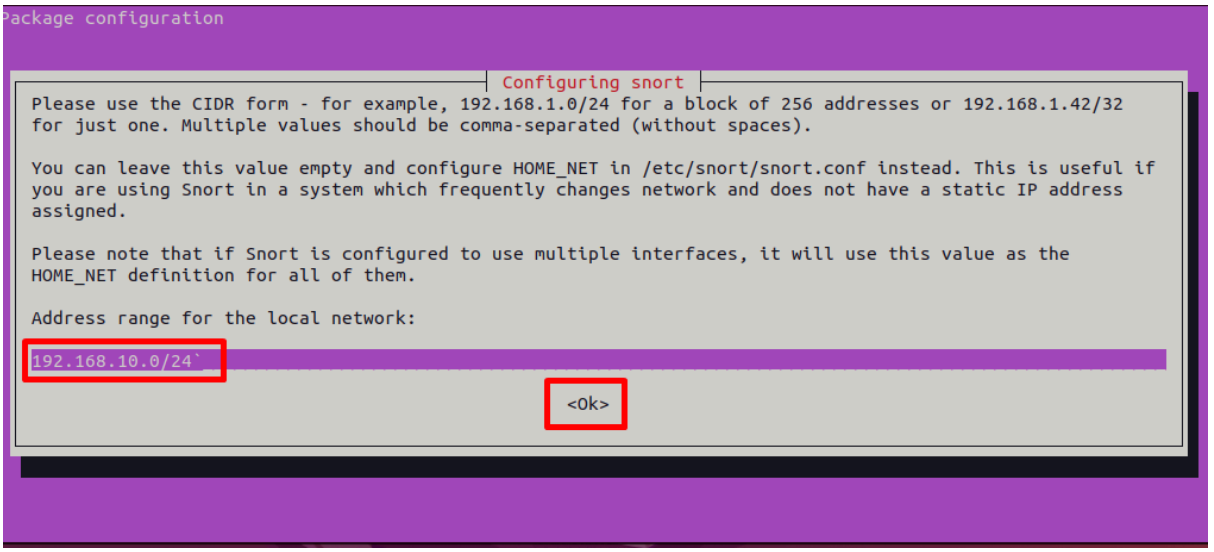
```
snort@snort-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cd:d2:e1 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.158/24 brd 192.168.10.255 scope global dynamic noprefixroute ens33
       valid_lft 341sec preferred_lft 341sec
    inet6 fe80::5f18:edbc:90df:3b02/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
snort@snort-virtual-machine:~$ ip link show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:cd:d2:e1 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
snort@snort-virtual-machine:~$ sudo ip link set ens33  promisc on
snort@snort-virtual-machine:~$ ip link show ens33
2: ens33: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default q
len 1000
    link/ether 00:0c:29:cd:d2:e1 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
snort@snort-virtual-machine:~$
```

- **Install SNORT**

sudo apt-get install snort -y

```
snort@snort-virtual-machine:~$ sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 net-tools oinkmaster
  snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 net-tools oinkmaster snort
  snort-common snort-common-libraries snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 2.554 kB of archives.
After this operation, 11,4 MB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-6 [44,3
kB]
Get:2 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-6 [238 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-common-libraries amd64 2.9.15.1-6build1 [882
 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-rules-default all 2.9.15.1-6build1 [146 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-common all 2.9.15.1-6build1 [49,7 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ubuntu5 [204
```

#Tambahkan Network yang ada pada Laptop/OS kalian

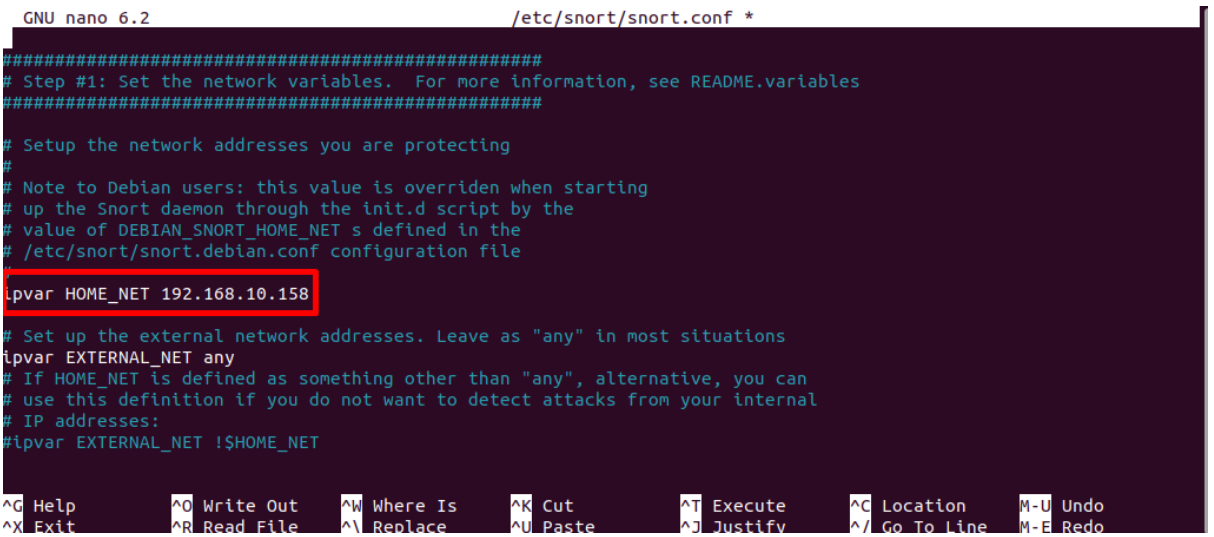


- **Edit Capture Packet IP**

  sudo nano /etc/snort/snort.conf

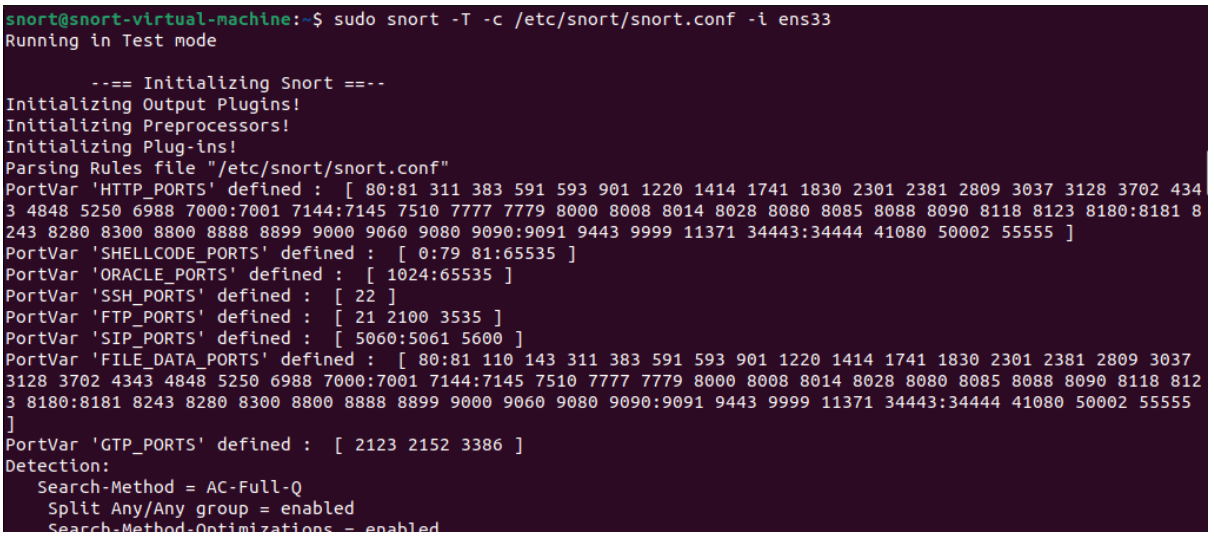
  (Ctrl + /) + (Ctrl + T) -> Navigation “Ipvar HOME_NET”

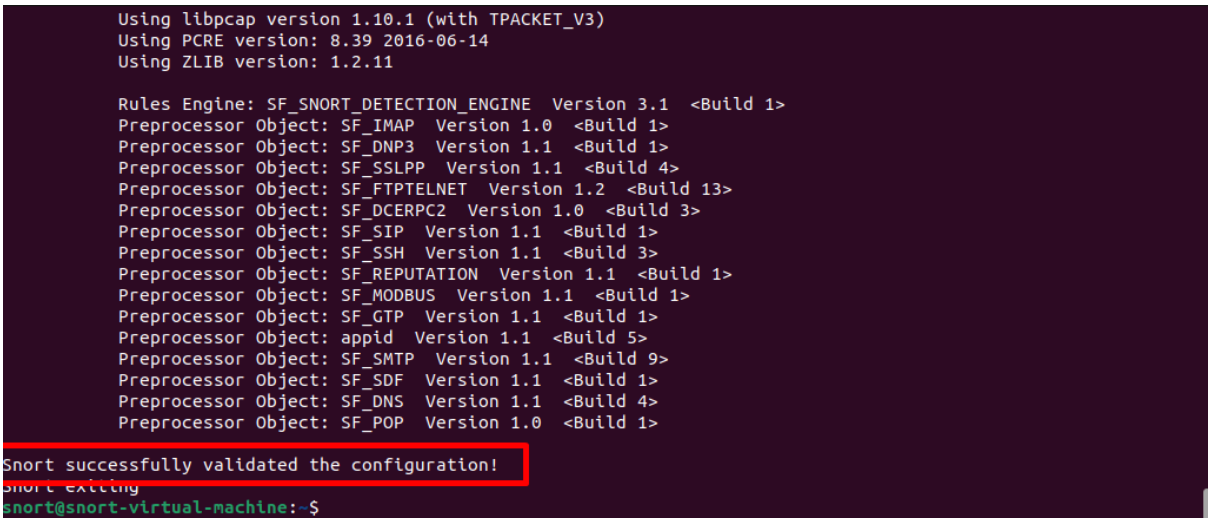
  Edit “ipvar HOME_NET any” to “ipvar HOME_NET 192.168.10.0/24 (your network Ubuntu)



- **Validasi fungsi dari SNORT**

sudo snort -T -c /etc/snort/snort.conf -i ens33

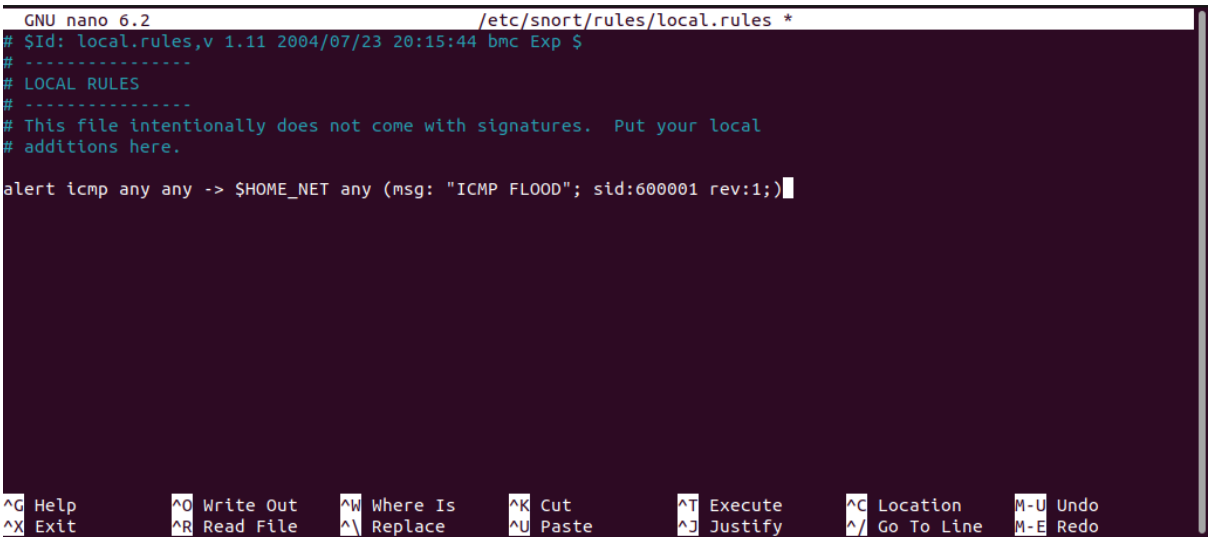




#pastikan Successfull

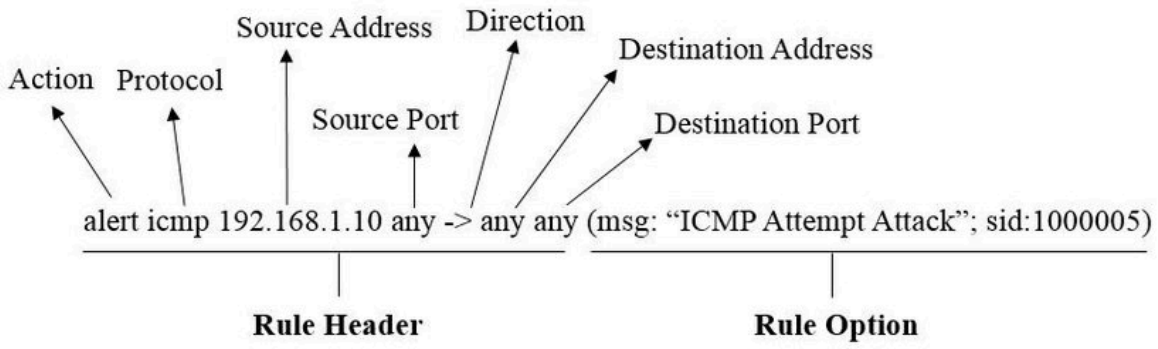
- **Create Rules IDS**
  Kita buat Rules IDS jika ada packet ICMP Flood maka akan diberikan Alert.

  sudo nano /etc/snort/rules/local.rules



Range SID Snort yang umum digunakan:

Range SID	Keterangan
0 - 999,999	SID yang disediakan Snort (default rules).
1,000,000 - 1,999,999	Custom rules buatan user.
2,000,000 - 2,147,483,647	Reserved untuk komunitas atau proyek lain.



- **Test Ping ICMP from Laptop**

  Ping (destination ip ubuntu) -t

  #gunakan IP Snort sebagai destination untuk test IDS yang kita buat

```
2025-05-17  16:08.07  /home/mobaxterm  ping 192.168.10.158 -t

Pinging 192.168.10.158 with 32 bytes of data:
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time=1ms TTL=64
Reply from 192.168.10.158: bytes=32 time=1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64
Reply from 192.168.10.158: bytes=32 time=1ms TTL=64
Reply from 192.168.10.158: bytes=32 time<1ms TTL=64

2025-05-17  16:08.29  /home/mobaxterm
```

- **Run Logg Capture Alert SNORT**

  sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

  #cmd untuk running Alert

```
snort@snort-virtual-machine:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
05/17-16:07:54.095114  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Pr
iority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
05/17-16:08:04.535390  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:04.851554  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Pr
iority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
05/17-16:08:05.547499  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:06.550288  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:07.556074  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:10.378826  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Pr
iority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
05/17-16:08:18.842079  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:19.852833  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:20.832997  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Pr
iority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
05/17-16:08:20.855978  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:21.865191  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:22.871792  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:22.977548  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Pr
iority: 2] {UDP} 0.0.0.0:5678 -> 255.255.255.255:5678
05/17-16:08:23.873512  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:24.881259  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
05/17-16:08:25.887266  [**] [1:600001:1] ICMP FLOOD [**] [Priority: 0] {ICMP} 192.168.10.156 -> 192.168.10.158
```