

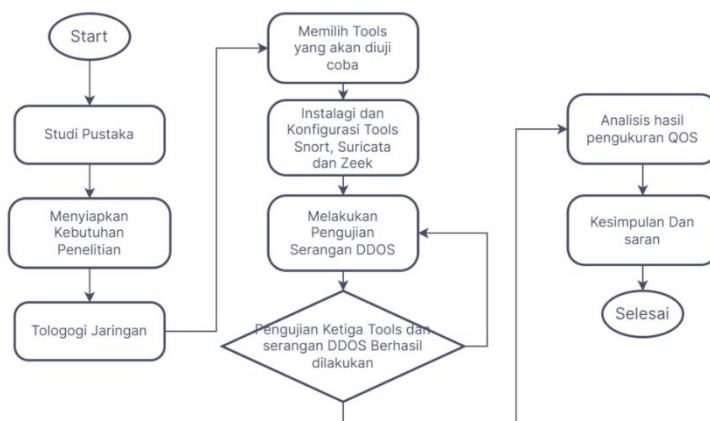
BAB III METODE PENELITIAN

1.1 OBJEK DAN SUBJEK PENELITIAN

Dalam penelitian ini, objek yang dikaji yaitu perbandingan performansi dari ketiga tools yaitu snort, suricata dan Zeek yang meliputi akurasi deteksi dan pencegahan ketiga tools *Intrusion Prevention System (IPS)* yang diimplementasikan pada satu laptop yang sama dimana laptop tersebut merupakan *server* yang dikonfigurasi sebagai *Network IPS* dari setiap tools IPS yang diuji. Sedangkan subjek pada penelitian ini adalah tools Snort, Suricata dan Zeek. Sumber data yang diperoleh berasal dari hasil uji coba ketiga tools di-*server* IPS dengan pengujian serangan menggunakan QOS (*Quality Of Service*).

1.2 DIAGRAM ALUR PENELITIAN

Alur dalam penelitian ini dimulai dari tahapan studi pustaka, menyiapkan kebutuhan penelitian, konfigurasi topologi, menentukan tools yang akan diuji coba, instalasi dan konfigurasi tools (Snort, Suricata dan Zeek), melakukan pengujian serangan, dan yang terakhir yaitu menganalisis hasil pengujian serangan dari keempat tools tersebut (Snort, Suricata dan Zeek) seperti pada diagram alur sebagai berikut:



Gambar 3.1 Diagram Alur Penelitian

1.2.1 STUDI PUSTAKA

Pada tahap awal yaitu studi pustaka sebagai landasan pengetahuan dasar dalam melakukan analisa, perancangan, implementasi dan pengujian untuk mendukung penelitian yang akan dilakukan. Teori-teori pada studi pustaka ini didapatkan dan bersumber dari buku, jurnal, *website* dan penelitian sejenis.

1.2.2 PERANGKAT

Dalam penelitian ini, perangkat-perangkat yang dibutuhkan terdiri dari perangkat

keras (*hardware*) dan perangkat lunak (*software*), yaitu:

- a. Perangkat Keras (*hardware*)
 1. Satu unit Laptop sebagai server *Intrusion Prevention System* (IPS) dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
 2. Sepuluh unit PC sebagai *attacker* (Penyerang) dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
 3. Satu unit PC sebagai *client* dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
 4. Satu buah Mikrotik.
- b. Perangkat Lunak (*software*)

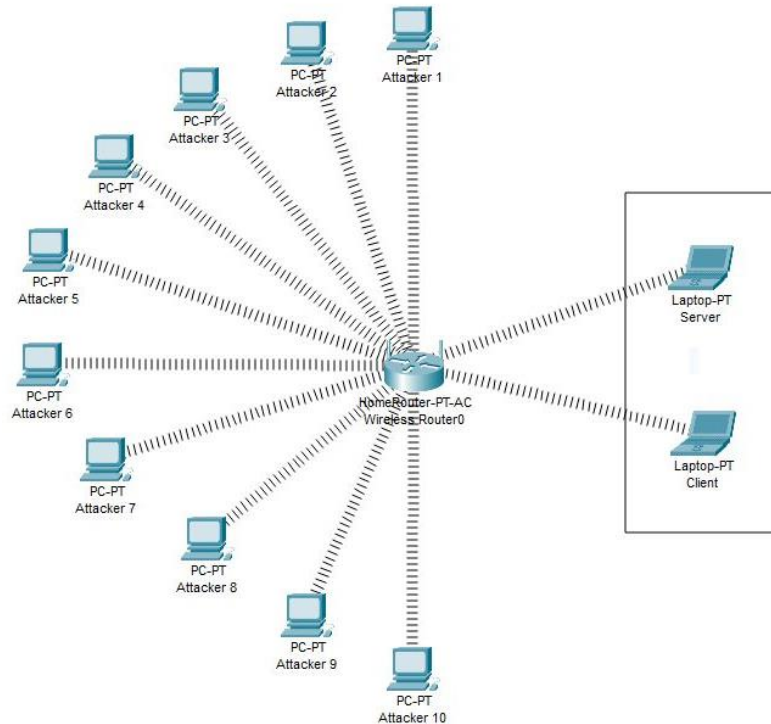
Tabel 3.1 Perangkat Lunak (*Software*)

No	Nama	Deskripsi
1	Linux Ubuntu 22.04	Sistem Operasi untuk Server IPS dan <i>attacker SYN flooding</i> dan <i>ICMP Flood</i> (Hping3).
2	Windows 10	Sistem Operasi untuk web <i>client</i> .
3	Snort	<i>Tool</i> yang digunakan untuk mendeteksi serangan dari PC <i>attacker</i> .
4	Suricata	<i>Tool</i> yang digunakan untuk mendeteksi serangan dari PC <i>attacker</i> .
5	Zeek	<i>Tool</i> yang digunakan untuk mendeteksi serangan dari PC <i>attacker</i> .
6	Hping3	<i>Tool</i> yang digunakan untuk melakukan serangan <i>SYN flood</i> dan <i>ICMP Flood</i> ke PC server.

1.2.3 TOPOLOGI JARINGAN

Topologi jaringan pada penelitian ini terdiri dari banyak laptop. Pertama, Laptop 1 sebagai web server untuk menginstal Snort, Suricata dan Zeek sebagai IPS pada OS Linux Ubuntu 22.04. Kemudian, 10 komputer digunakan sebagai PC penyerang yang sudah terpasang alat untuk melakukan serangan DDOS, yaitu HPing3. Selain itu, laptop lain berfungsi sebagai *web client* yang digunakan penulis untuk menganalisis perhitungan QOS menggunakan wireshark dengan mengakses web server. Sistem jaringan ini diimplementasikan dalam jaringan area lokal (LAN). Topologi jaringan pada

penelitian ini ditunjukkan pada Gambar 3.2.



Gambar 3.2 Topologi Jaringan

1.2.4 INSTALASI DAN KONFIGURASI TOOLS (SNORT, SURICATA DAN ZEEK)

Pada tahap ini, peneliti akan memilih satu persatu *tools* yaitu Snort, Suricata dan Zeek untuk dilakukan instalasi beserta konfigurasinya dan untuk dilakukan pengujian terhadap serangan dan analisisnya ditahap selanjutnya. Tahap ini akan diulang hingga semua *tools* sudah di instalasi.

A. Instalasi dan Konfigurasi Pada Snort

1. Instalasi Snort

Pada tahap instalasi Snort, diawali dengan melakukan *update* dan *upgrade* sistem Ubuntu 22.04. Setelah melakukan *update* dan *upgrade* maka tahap berikutnya melakukan instalasi *dependencies* (*package* dan *library*) yang dibutuhkan oleh Snort. Jika *dependencies* telah terinstall, maka dilanjutkan dengan mengunduh dan melakukan instalasi Snort. Bisa dilihat pada tabel dibawah ini.

Tabel 3.2 Instalasi Snort

```

1  $sudo su
2  #apt-get update -y
3  #apt-get upgrade -y
4  #apt-get install openssh-server ethtool build-
essential libpcap-dev libpcre3-dev libdumbnet-dev
bison flex zlib1g-dev liblzma-dev openssl libssl-dev
autoconf
5  #mkdir Snort-Installation-Files
6  #cd Snort-Installation-Files
7  #wget http://luajit.org/download/LuaJIT-2.0.5.tar.gz
8  #tar xzf LuaJIT-2.0.5.tar.gz
9  #cd LuaJIT-2.0.5
10 #make && make install
11 #cd ..
12 #wget https://www.snort.org/downloads/snort/daq-
2.0.7.tar.gz
13 #tar -zxvf daq-2.0.7.tar.gz
14 #cd daq-2.0.7
15 #apt-get install libnetfilter-queue-dev libnetfilter-
queueuel libnfnetlink-dev libnfnetlink0 -y
16 #autoreconf -f -i
17 #./configure --enable-nfq=yes && make && make install
18 #cd ..
19 #wget https://www.snort.org/downloads/snort/snort-
2.9.16.tar.gz
20 #tar -xvzf snort-2.9.16.tar.gz
21 #cd snort-2.9.16
22 #./configure --enable-sourcefire && make && make
install
23 #ldconfig
24 #ln -s /usr/local/bin/snort /usr/sbin/snort
24 #snort -V

```

2. Konfigurasi Snort

Setelah tahap instalasi Snort berhasil dilakukan, maka tahap berikutnya adalah melakukan konfigurasi Snort agar dapat berjalan dan berfungsi sebagai Snort dengan mode *Network-IPS*. Berikut merupakan tahapan dari konfigurasi Snort.

Tabel 3.3 Konfigurasi Snort

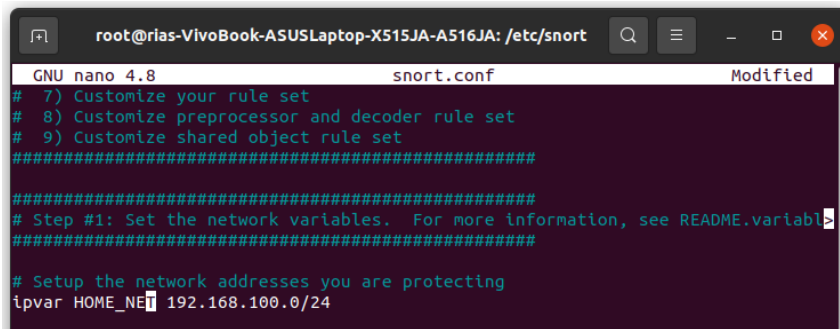
```

# Create the Snort directories:
1  #sudo mkdir /etc/snort
2  #sudo mkdir /etc/snort/rules
3  #sudo mkdir /etc/snort/rules/iplists
4  #sudo mkdir /etc/snort/preproc_rules
5  #sudo mkdir /usr/local/lib/snort_dynamicrules
6  #sudo mkdir /etc/snort/so_rules
#Creating our logging directories:
7  #sudo mkdir /var/log/snort
8  #sudo mkdir /var/log/snort/archived_logs
# Create some files that stores rules and ip lists:
9  #sudo touch /etc/snort/rules/iplists/black_list.rules
10 #sudo touch /etc/snort/rules/iplists/white_list.rules
11 #sudo touch /etc/snort/rules/local.rules
12 #sudo touch /etc/snort/sid-msg.map
# Copy Snort Config Files:
13 #cd home/riias/Snort-Installation-Files/snort-
2.9.16/etc/
14 #sudo cp *.conf* /etc/snort
13 #sudo cp *.map /etc/snort
14 #sudo cp *.dtd /etc/snort
15 #cd home/riias/Snort-Installation-Files/snort-
2.9.16/src/dynamic-
preprocessors/build/usr/local/lib/snort_dynamicprepro-
cessor/sudo cp *
/usr/local/lib/snort_dynamicpreprocessor/
# Comment All Rules Snort Configuration:
16 #sudo sed -i "s/include \$RULE\ PATH/#include
\$RULE\_PATH/" /etc/snort/snort.conf
# Verifikasi Konfigurasi
17 #ldconfig

```

Berikutnya, setelah konfigurasi pada tabel diatas selesai dilakukan maka tahap

berikutnya adalah melakukan konfigurasi *file* Snort yaitu *snort.conf* seperti pada beberapa gambar dibawah ini.



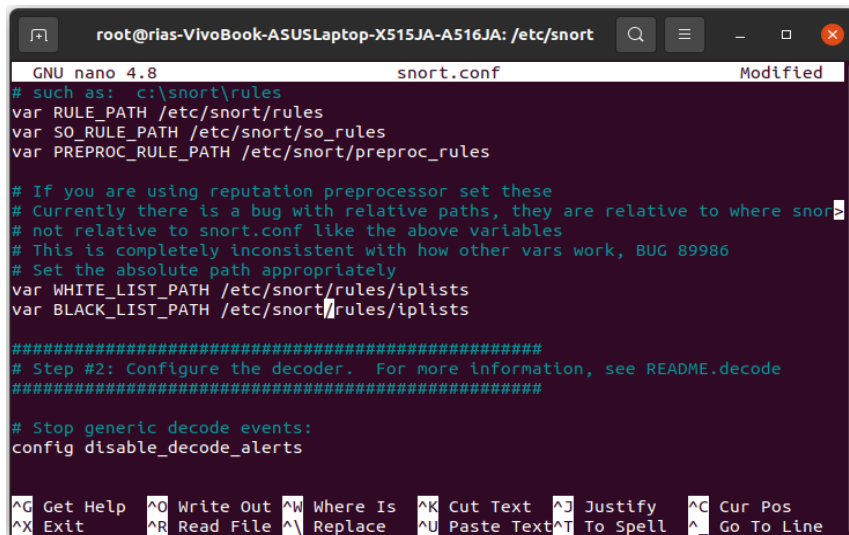
```
root@rias-VivoBook-ASUSLaptop-X515JA-A516JA: /etc/snort
GNU nano 4.8 snort.conf Modified
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####

#####
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.100.0/24
```

Gambar 3.3 Konfigurasi IP Address HOME_NET Snort

Pada *file snort.conf* di *line 45*, IP *address* pada HOME_NET diubah menjadi 192.168.100.0/24. HOME_NET merupakan alamat jaringan yang akan dilindungi oleh Snort IPS. Penggunaan IP *address* tersebut bertujuan untuk menjadikan Snort berjalan sebagai mode IPS dikarenakan IP *address* tersebut merupakan IP *address network*.



```
root@rias-VivoBook-ASUSLaptop-X515JA-A516JA: /etc/snort
GNU nano 4.8 snort.conf Modified
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists

#####
# Step #2: Configure the decoder. For more information, see README.decoder
#####

# Stop generic decode events:
config disable_decode_alerts
```

Gambar 3.4 Konfigurasi Direktori Snort

Berikutnya, melakukan konfigurasi beberapa *direktori* yang diperlukan oleh Snort seperti pada *line 104 – 106* dan *line 113-114* menjadi seperti pada Gambar 3.4.

```

root@rias-VivoBook-ASUSLaptop-X515JA-A516JA: /etc/snort
GNU nano 4.8 snort.conf Modified
# Configure maximum number of flowbit references. For more information, see README.Flowbit
# config flowbits_size: 64

# Configure ports to ignore
# config ignore_ports: tcp 21 6667:6671 1356
# config ignore_ports: udp 1:17 53

# Configure active response for non inline operation. For more information, see README.act
# config response: eth0 attempts 2

# Configure DAQ related options for inline operation. For more information, see README.daq
#
config daq: nfq
config daq_dir: /usr/local/lib/daq
config daq_mode: inline
config daq_var: queue=0
#
# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ

^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos
^X Exit          ^R Read File   ^A Replace    ^U Paste Text ^T To Spell   ^_ Go To Line

```

Gambar 3.5 Konfigurasi DAQ Snort

Setelah itu, melakukan konfigurasi DAQ (*Data Acquisition*) yang akan digunakan oleh Snort diantaranya jenis DAQ yang digunakan yaitu *nfq*, direktori DAQ, mode yang digunakan adalah *inline* dan variabel DAQ *queue=0* seperti pada gambar 3.5.

```

root@rias-VivoBook-ASUSLaptop-X515JA-A516JA: /etc/snort
GNU nano 4.8 snort.conf Modified
include reference.config

#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/local.rules

```

Gambar 3.6 Konfigurasi Lokasi Rule Snort

Kemudian, konfigurasi terakhir yang dilakukan adalah menentukan lokasi untuk *rules* yang akan digunakan oleh Snort. Untuk menentukan lokasi *rules* yang akan digunakan, dapat dilakukan dengan menghapus tanda # pada lokasi *rules* yang akan digunakan, dimana pada Gambar 3.6 lokasi file yang digunakan adalah *local.rules*.

3. Melakukan Konfigurasi Rules Snort

```

*local.rules
/etc/snort/rules
drop icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Flood Attempt";
classtype:icmp-event; threshold: type threshold, track by_src, count
50, seconds 1; sid:1000001; rev:1;)

drop tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "SYN Flood Attempt";
flow:stateless; flags:S,12; threshold: type both, track by_dst, count
20, seconds 1; sid:1000002; rev:1)

```

Gambar 3.7 Rules Snort

Pada Gambar 3.7 merupakan *rules* Snort yang digunakan untuk melakukan deteksi dan pencegahan yang berupa *drop* paket dari serangan ICMP *Flood* dan SYN *Flood*. Keterangan lengkap dari *rules* pada gambar diatas adalah sebagai berikut:

- 1) Drop: melakukan blok dan log paket.
 - 2) icmp/tcp : protokol yang digunakan.
 - 3) \$EXTERNAL_NET : variabel IP *address* yang berisi selain IP *address* pada \$HOME_NET.
 - 4) any : semua port *number* yang digunakan.
 - 5) -> : arah jalannya lalu lintas jaringan, dimana bagian sebelah kiri dari tanda merupakan sumber paket, sedangkan untuk bagian sebelah kanan dari tanda merupakan tujuan paket.
 - 6) \$HOME_NET : variabel IP *address* yang berisi alamat dari jaringan yang dilindungi.
 - 7) msg : pesan yang ditampilkan ketika *rules* tersebut memenuhi kondisi yang telah ditentukan.
 - 8) classtype : merupakan *keyword* untuk mengkategorikan *rules* dalam mendeteksi jenis serangan.
 - 9) flow : *keyword* yang digunakan untuk memeriksa arah jalannya paket.
 - 10) flag : *keyword* yang digunakan untuk memeriksa *flag* tertentu dari paket yang menggunakan protokol TCP
 - 11) threshold : *keyword* yang digunakan untuk mengatur batasan tertentu agar *rule* dapat berjalan.
 - 12) sid : *keyword* yang digunakan untuk memberikan identitas unik dari setiap *rules*.
 - 13) rev : *keyword* yang digunakan untuk memberikan identitas unik dari setiap revisi *rules*.
4. Menjalankan perintah uji coba serangan (pada laptop penyerang)

```
#ICMP Flood hping3 -1 -p 80 --flood -d 1450 192.168.100.154 -V  
#TCP SYN Flood hping3 -S -p 80 -flood -d 192.168.100.154 -V
```

B. Instalasi dan Konfigurasi Suricata

1. Instalasi Suricata

Pada tahap instalasi Suricata memiliki tahap yang sama dengan proses instalasi Snort, yaitu diawali dengan melakukan *update* dan *upgrade* sistem Ubuntu 22.04. Setelah melakukan *update* dan *upgrade* maka tahap berikutnya melakukan instalasi *dependencies* (*package* dan *library*) yang dibutuhkan oleh Suricata. Jika *dependencies* telah terinstall, maka dilanjutkan dengan mengunduh dan melakukan instalasi Suricata. Untuk tahapan instalasi Suricata secara rinci, dapat dilihat pada tabel dibawah ini.

Tabel 3.4 Instalasi Suricata

```
1 $sudo su
2 #apt-get update -y
3 #apt-get upgrade -y
4 #apt-get install libpcre3-dbg libpcre3-dev autoconf
  automake libtool libpcap-dev libnet1-dev libyaml-dev
  libjansson4 libcap-ng-dev libmagic-dev libjansson-dev
  zlib1g-dev
5 #add-apt-repository ppa:oisf/suricata-stable
6 #apt-get update -y
7 #apt-get install suricata suricata-dbg -y
```

2. Konfigurasi Suricata

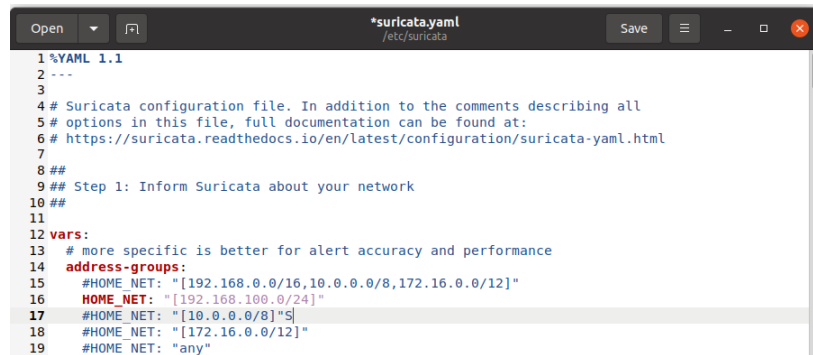
Setelah tahap instalasi Suricata berhasil dilakukan, maka tahap berikutnya adalah

Tabel 3.5 Konfigurasi Suricata

```
1 #cd /etc/suricata
2 #gedit suricata.yaml
  ---Tambahkan # pada baris 15 HOME_NET:
  "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]" menjadi
3 #HOME NET:
  "[192.168.0.0/16,10.
  0.0.0/8,172.16.0.0/1
  2]"
  ---Hapus # pada
  baris 16 dan edit
  menjadi HOME_NET:
  "[192.168.200.0/24]"
  ---Ctrl + F, ketik
  rule-files
  ---Tambahkan hapus -
  suricata.rules
  menjadi -
  local.rules
  ---Di atasnya
  dibagian default-
  rule-path di ganti
  menjadi
  /etc/suricata/rules
4 #cd rules
5 #gedit local.rules
6 #suricata -c
  /etc/suricata/surica
  ta.yaml -q 0
7 #tail -f
  /var/log/suricata/fa
  st.log
```


melakukan konfigurasi Suricata agar dapat berjalan dan berfungsi sebagai Suricata dengan mode *Network-IPS*. Berikut merupakan tahapan dari konfigurasi Suricata.

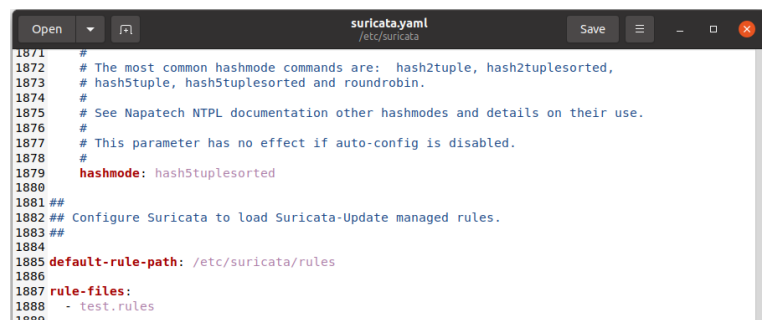
Berikutnya, setelah konfigurasi pada tabel diatas selesai dilakukan maka tahap berikutnya adalah melakukan konfigurasi file suricata yaitu *suricata yml* seperti pada gambar dibawah ini.



```
1 %YAML 1.1
2 ---
3
4 # Suricata configuration file. In addition to the comments describing all
5 # options in this file, full documentation can be found at:
6 # https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html
7
8 ##
9 ## Step 1: Inform Suricata about your network
10 ##
11
12 vars:
13 # more specific is better for alert accuracy and performance
14 address-groups:
15 #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
16 HOME_NET: "[192.168.100.0/24]"
17 #HOME_NET: "[10.0.0.0/8]"
18 #HOME_NET: "[172.16.0.0/12]"
19 #HOME_NET: "any"
```

Gambar 3.8 Gambar Konfigurasi IP Address HOME_NET Suricata

Pada file *suricata.yaml* di *line 15*, IP *address* pada HOME_NET diubah menjadi 192.168.100.0/24. HOME_NET merupakan alamat jaringan yang akan dilindungi oleh Suricata IPS. Penggunaan IP *address* tersebut bertujuan untuk menjadikan Suricata berjalan sebagai mode NIPS dikarenakan IP *address* tersebut merupakan IP *address network*.



```
1871 #
1872 # The most common hashmode commands are: hash2tuple, hash2tuplesorted,
1873 # hash5tuple, hash5tuplesorted and roundrobin.
1874 #
1875 # See Napatech NTPL documentation other hashmodes and details on their use.
1876 #
1877 # This parameter has no effect if auto-config is disabled.
1878 #
1879 hashmode: hash5tuplesorted
1880
1881 ##
1882 ## Configure Suricata to load Suricata-Update managed rules.
1883 ##
1884
1885 default-rule-path: /etc/suricata/rules
1886
1887 rule-files:
1888 - test.rules
1889
```

Gambar 3.9 Konfigurasi File Rules Suricata

Berikutnya melakukan konfigurasi untuk menentukan *file rules* yang akan digunakan oleh Suricata. Untuk menentukan *file rules* yang akan digunakan, dapat dilakukan dengan mencantumkan nama *file rules* yang digunakan pada bagian *rules-files* seperti pada Gambar 3.8.

C. Instalasi dan Konfigurasi Zeek

1. Instalasi Suricata

Pada tahap instalasi Zeek memiliki tahap yang sama dengan proses instalasi Snort dan Suricata, yaitu diawali dengan melakukan instalasi *dependencies* (*package* dan *library*) yang dibutuhkan oleh Zeek. Jika *dependencies* telah terinstall, maka dilanjutkan dengan mengunduh dan melakukan instalasi Zeek. Untuk tahapan instalasi Zeek secara rinci, dapat dilihat pada tabel dibawah ini.

```
1 $sudo su
2 #mkdir Zeek-Installation-Files
3 #cd Zeek-Installation-Files
4 #apt-get install git cmake make gcc g++ flex bison
  libpcap-dev libssl-dev python-dev swig zlib1g-dev
5 #wget https://download.zeek.org/zeek-3.0.5.tar.gz
6 #tar -xvzf zeek-3.0.5.tar.gz
7 #cd zeek-3.0.5
8 #./configure
9 #make
10 #make install
```

Tabel 3.6 instalasi Zeek

2. Konfigurasi Zeek

Setelah tahap instalasi Zeek berhasil dilakukan, maka tahap berikutnya adalah melakukan konfigurasi Zeek, berikut merupakan tahapan dari konfigurasi Zeek.

```
1 #cd /usr/local/zeek/etc
2 #nano node.cfg
3 #Ganti pada bagian interface menjadi
  interface=wlo1
4 #nano zeekctl.cfg
  #Hapus isi pada bagian MailTo menjadi MailTo =
  #Jalankan Zeek
5 #zeekctl
6 #install
7 #deploy
8 #status
```

Tabel 3.7 Konfigurasi Zeek

Pada tahap konfigurasi Zeek bagian *line* kedua dari tabel diatas merupakan konfigurasi untuk menentukan *interface* yang akan dilakukan *scanning* oleh Zeek, dimana pada konfigurasi tersebut menggunakan enp1s0 sebagai *interface* yang akan *discanning* dikarenakan jaringan pada *interface* tersebut merupakan jaringan yang digunakan oleh laptop target.

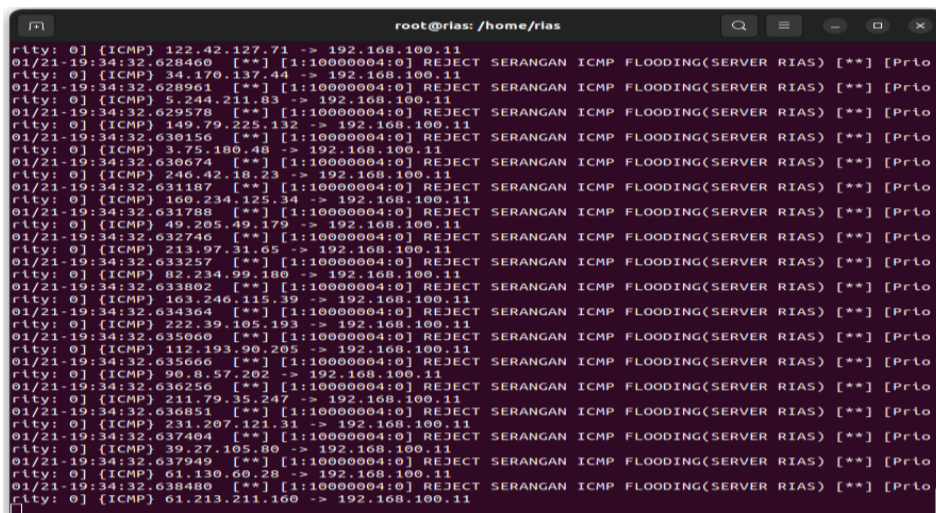
1.2.5 MELAKUKAN PENGUJIAN SERANGAN

Dalam melakukan pengujian terhadap server yang telah dikonfigurasi ke dalam *rules Intrusion Prevention System* (IPS). Pengujian ini dilakukan dengan memberikan serangan *Distributed Denial of Service* (DDOS) melalui PC penyerang ke PC server, dengan menggunakan tiga *tools* yaitu Snort, Suricata dan Zeek. penyerangan ini

dilakukan dengan *tools* yang berbeda. Serangan pertama akan dilakukan pada PC server yang telah diaktifkan oleh *tool* Snort dengan perintah IPS, kemudian setelah serangan berhasil akan terlihat apakah *tool* Snort dapat menampilkan peringatan pada PC server atau tidak. Setelah mengetahui hasil pengujian serangan tersebut menggunakan *tool* Snort, dilakukan pengujian dengan langkah yang sama dengan menggunakan *tool* Suricata dan Zeek pada PC server.

1. Pengujian serangan ICMP Flood

Dalam skenario serangan ICMP Flood, penyerang menggunakan *tool* hping3 untuk melakukan serangan. Setelah penyerang menyelesaikan *Scanning*, maka, IPS Snort, Suricata dan Zeek akan mendeteksi dan memblokir sesuai aturan yang ditetapkan. Pengujian ini dilakukan dengan menggunakan dua skenario, yang dimana skenario pertama adalah penyerang melakukan serangan ICMP Flood di server tetapi IPS Snort, Suricata dan Zeek dinonaktifkan, dan skenario kedua adalah penyerang melakukan serangan ICMP Flood, tetapi IPS Snort, Suricata dan Zeek diaktifkan, sehingga dapat terlihat perbandingannya. Hasil pengujian *Quality of Service* (QOS) dengan IPS Snort, Suricata dan Zeek dinonaktifkan dan dengan IPS Snort, Suricata dan Zeek diaktifkan.



```
root@rias: /home/rias
rftv: 0] [ICMP] 122.42.127.71 -> 192.168.100.11
01/21-19:34:32.628460 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 34.170.137.49 -> 192.168.100.11
01/21-19:34:32.628961 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 5.244.211.83 -> 192.168.100.11
01/21-19:34:32.629578 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 149.79.225.132 -> 192.168.100.11
01/21-19:34:32.630156 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 3.75.180.48 -> 192.168.100.11
01/21-19:34:32.630674 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 246.42.18.23 -> 192.168.100.11
01/21-19:34:32.631187 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 160.234.125.34 -> 192.168.100.11
01/21-19:34:32.631788 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 49.205.49.179 -> 192.168.100.11
01/21-19:34:32.632746 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 213.97.31.65 -> 192.168.100.11
01/21-19:34:32.633257 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 82.234.99.180 -> 192.168.100.11
01/21-19:34:32.633802 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 163.246.115.39 -> 192.168.100.11
01/21-19:34:32.634364 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 222.39.105.193 -> 192.168.100.11
01/21-19:34:32.635060 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 112.393.90.205 -> 192.168.100.11
01/21-19:34:32.635666 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 90.8.57.202 -> 192.168.100.11
01/21-19:34:32.636256 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 211.79.35.247 -> 192.168.100.11
01/21-19:34:32.636851 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 231.207.121.31 -> 192.168.100.11
01/21-19:34:32.637404 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 39.27.105.80 -> 192.168.100.11
01/21-19:34:32.637949 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 61.130.60.28 -> 192.168.100.11
01/21-19:34:32.638480 [**] [1:10000004:0] REJECT SERANGAN ICMP FLOODING(SERVER RIAS) [**] [Prto
rftv: 0] [ICMP] 61.213.211.160 -> 192.168.100.11
```

Gambar 3.10 Alert ICMP Flood pada IPS Snort

Pada Gambar 3.10 ini Peringatan yang ditampilkan saat menerima serangan ICMP Flood, berdasarkan dengan konfigurasi di `/etc/snort/rules/local.rules`. Peringatan snort juga dapat dilihat dengan menjalankan perintah `snort -A console -c /etc/snort/snort.conf`.

```

event] [Priority: 3] [ICMP] 9.158.36.38:8 -> 192.168.100.11:0
01/21/2023-19:38:11.268522 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 46.137.135.180:8 -> 192.168.100.11:0
01/21/2023-19:38:11.269300 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 178.47.186.42:8 -> 192.168.100.11:0
01/21/2023-19:38:11.269831 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 84.5.27.112:8 -> 192.168.100.11:0
01/21/2023-19:38:11.270936 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 44.227.151.70:8 -> 192.168.100.11:0
01/21/2023-19:38:11.270386 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 15.36.22.15:8 -> 192.168.100.11:0
01/21/2023-19:38:11.272041 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 130.45.40.241:8 -> 192.168.100.11:0
01/21/2023-19:38:11.271489 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 253.63.143.117:8 -> 192.168.100.11:0
01/21/2023-19:38:11.278972 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 94.228.222.125:8 -> 192.168.100.11:0
01/21/2023-19:38:11.279489 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 42.135.111.135:8 -> 192.168.100.11:0
01/21/2023-19:38:11.280024 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 91.197.198.233:8 -> 192.168.100.11:0
01/21/2023-19:38:11.280550 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 26.133.11.208:8 -> 192.168.100.11:0
01/21/2023-19:38:11.281109 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 153.173.146.237:8 -> 192.168.100.11:0
01/21/2023-19:38:11.281660 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 166.40.144.100:8 -> 192.168.100.11:0
01/21/2023-19:38:11.282212 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 24.250.33.164:8 -> 192.168.100.11:0
01/21/2023-19:38:11.282059 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 135.243.50.87:8 -> 192.168.100.11:0
01/21/2023-19:38:11.283415 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 19.15.91.233:8 -> 192.168.100.11:0
01/21/2023-19:38:11.283965 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 184.25.156.245:8 -> 192.168.100.11:0
01/21/2023-19:38:11.284516 [wDrop] [**] [1:100000:1] ICMP SURICATA REJECT [**] [Classification: Generic ICMP
event] [Priority: 3] [ICMP] 108.132.193.99:8 -> 192.168.100.11:0

```

Gambar 3.11 Alert ICMP Flood pada IPS Suricata

Pada Gambar 3.11 Suricata dapat menampilkan peringatan ketika serangan ICMP Flood mencoba masuk kedalam server. Alert yang berjalan di Suricata mengikuti konfigurasi yang sudah diatur di direktori /etc/suricata/rules/local.rules. Alert yang muncul pada Suricata dapat dilihat dengan menjalankan perintah tail -f /var/log/suricata/fast.log.

```

root@rias: /home/rias/zeek/checked/icmp
0
1674393394.726236 192.168.100.11 3 111.59.147.07 3 - 1 56 00
1674393394.726281 192.168.100.11 3 218.05.89.130 3 - 1 56 00
1674393394.726291 192.168.100.11 3 21.134.53.181 3 - 1 56 00
1674393374.872638 61.98.139.45 8 192.168.100.11 0 1 28 128
1674393394.726825 98.80.232.231 8 192.168.100.11 0 1 28 128
1674393377.492707 235.192.156.192 8 192.168.100.11 0 1 28 00
1674393394.726830 204.237.206.121 8 192.168.100.11 0 1 28 128
1674393381.724882 208.186.45.165 8 192.168.100.11 0 1 28 128
1674393394.726994 193.64.95.153 8 192.168.100.11 0 1 28 128
1674393404.279180 3.94.158.180 8 192.168.100.11 0 1 28 128
1674393394.753986 194.50.24.195 8 192.168.100.11 0 1 28 128
1674393394.755887 74.163.57.17 8 192.168.100.11 0 1 28 128
1674393377.935005 155.124.129.61 8 192.168.100.11 0 1 28 128
1674393396.244811 68.227.78.29 8 192.168.100.11 0 1 28 128
1674393382.581383 192.168.100.11 3 40.229.181.251 3 - 1 56 00
1674393374.387115 192.168.100.11 3 230.251.61.161 3 - 1 56 00
1674393394.756171 145.2.205.20 8 192.168.100.11 0 1 28 128
1674393405.892396 192.168.100.11 3 62.247.107.156 3 - 1 56 00
1674393394.757298 192.168.100.11 3 146.4.97.63 3 - 1 56 00
1674393394.757465 192.168.100.11 3 68.179.134.32 3 - 1 56 00
1674393382.540744 192.168.100.11 3 104.63.46.201 3 - 1 56 00
1674393394.757513 192.168.100.11 3 103.204.252.247 3 - 1 56 00
1674393394.757535 192.168.100.11 3 69.91.66.84 3 - 1 56 00
1674393399.834253 192.168.100.11 3 94.192.246.78 3 - 1 56 00
1674393394.757559 192.168.100.11 3 51.65.107.218 3 - 1 56 00
1674393406.954540 192.168.100.11 3 167.189.197.15 3 - 1 56 00
1674393394.757582 192.168.100.11 3 97.39.26.144 3 - 1 56 00
1674393409.281897 56.165.195.87 8 192.168.100.11 0 1 28 128
1674393406.836879 149.180.131.225 8 192.168.100.11 0 1 28 128
1674393394.757606 192.168.100.11 3 226.252.134.252 3 - 1 56 00
1674393398.955664 192.168.100.11 3 230.230.173.195 3 - 1 56 00
1674393394.757627 192.168.100.11 3 214.57.27.139 3 - 1 56 00
1674393394.757673 192.168.100.11 3 24.251.243.20 3 - 1 56 00
1674393404.879499 192.168.100.11 3 153.3.49.59 3 - 1 56 00
1674393394.757699 192.168.100.11 3 119.129.224.214 3 - 1 56 00
1674393406.830108 134.246.92.195 8 192.168.100.11 0 1 28 128
1674393394.757721 192.168.100.11 3 129.153.214.126 3 - 1 56 00
1674393378.406766 121.78.186.108 8 192.168.100.11 0 1 28 128
1674393394.757708 192.168.100.11 3 170.136.173.53 3 - 1 56 00
1674393398.699843 154.251.264.57 8 192.168.100.11 0 1 28 128
1674393394.757812 192.168.100.11 3 128.105.219.150 3 - 1 56 00
1674393394.757858 192.168.100.11 3 224.27.203.119 3 - 1 56 00
1674393406.907610 192.168.100.11 3 75.95.141.57 3 - 1 56 00
1674393394.758047 192.168.100.11 3 172.234.26.238 3 - 1 56 00
1674393394.758071 192.168.100.11 3 39.103.203.204 3 - 1 56 00
1674393394.758094 192.168.100.11 3 63.125.209.115 3 - 1 56 00
1674393394.758116 192.168.100.11 3 38.178.137.196 3 - 1 56 00
1674393377.294408 192.168.100.11 3 174.163.231.174 3 - 1 56 00
1674393379.564983 186.197.34.208 8 192.168.100.11 0 1 28 128
1674393394.758191 192.168.100.11 3 237.204.224.254 3 - 1 56 00

```

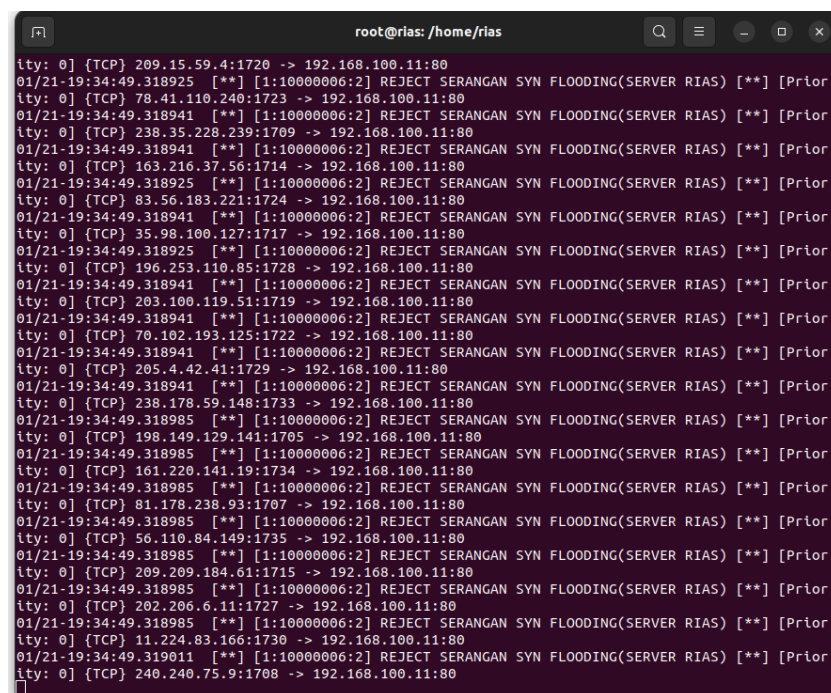
Gambar 3.12 Alert ICMP Flood pada IPS Zeek

Pada Gambar 3.12 Zeek memiliki layar peringatan saat serangan ICMP Flood mencoba masuk kedalam server. Peringatan yang ditampilkan di Zeek mematuhi aturan yang sesuai dengan rules Zeek. Untuk menampilkan peringatan, server harus menjalankan perintah zeek-cut ts id.orig_h id.orig_p id.resp_h id.resp_p protoconn_state history orig_pkts orig_ip_bytes resp_pkts

resp_ip_bytes < conn.log.

2. Pengujian Serangan SYN Flood

pada Saat mencoba serangan SYN Flood, penyerang menggunakan alat Hping3 yang diunduh dan diinstal di Ubuntu 22.04. Cara kerja serangan ini adalah dengan mengirimkan sebanyak mungkin paket SYN ke server target atau teknik ini disebut *flooding* dimana penyerang membanjiri server dengan paket SYN. Serangan ini diuji menggunakan dua skenario, skenario pertama adalah penyerang mengirim paket SYN Flood ke server tetapi IPS Snort, Suricata dan Zeek tidak aktif, dan skenario kedua adalah penyerang melakukan serangan SYN Flood yang terdeteksi oleh Snort, Suricata dan Zeek.



```
root@riias: /home/riias
ity: 0] {TCP} 209.15.59.4:1720 -> 192.168.100.11:80
01/21-19:34:49.318925  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 78.41.110.240:1723 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 238.35.228.239:1709 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 163.216.37.56:1714 -> 192.168.100.11:80
01/21-19:34:49.318925  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 83.56.183.221:1724 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 35.98.100.127:1717 -> 192.168.100.11:80
01/21-19:34:49.318925  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 196.253.110.85:1728 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 203.100.119.51:1719 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 70.102.193.125:1722 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 205.4.42.41:1729 -> 192.168.100.11:80
01/21-19:34:49.318941  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 238.178.59.148:1733 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 198.149.129.141:1705 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 161.220.141.19:1734 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 81.178.238.93:1707 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 56.110.84.149:1735 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 209.209.184.61:1715 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 202.206.6.11:1727 -> 192.168.100.11:80
01/21-19:34:49.318985  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 11.224.83.166:1730 -> 192.168.100.11:80
01/21-19:34:49.319011  [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] {TCP} 240.240.75.9:1708 -> 192.168.100.11:80
```

Gambar 3.13 Alert SYN Flood pada IPS Snort

Pada Gambar 3.13 terlihat Snort dapat menampilkan peringatan saat menerima *signature* yang sesuai dengan aturan atau perintah *rules* yaitu serangan SYN Flood terdeteksi, yang berarti Snort dapat mengirimkan peringatan ketika serangan SYN Flood terjadi di server dengan pesan di notifikasi. seperti yang dipersyaratkan oleh *rules*.

```

root@rias: /home/rias
ity: 0] [TCP] 209.15.59.4:1720 -> 192.168.100.11:80
01/21-19:34:49.318925 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 78.41.110.240:1723 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 238.35.228.239:1709 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 163.216.37.56:1714 -> 192.168.100.11:80
01/21-19:34:49.318925 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 83.56.183.221:1724 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 35.98.100.127:1717 -> 192.168.100.11:80
01/21-19:34:49.318925 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 196.253.110.85:1728 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 203.100.119.51:1719 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 70.102.193.125:1722 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 205.4.42.41:1729 -> 192.168.100.11:80
01/21-19:34:49.318941 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 238.178.59.148:1733 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 198.149.129.141:1705 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 161.220.141.19:1734 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 81.178.238.93:1707 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 56.110.84.149:1735 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 209.209.184.61:1715 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 202.206.6.11:1727 -> 192.168.100.11:80
01/21-19:34:49.318985 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 11.224.83.166:1730 -> 192.168.100.11:80
01/21-19:34:49.319011 [**] [1:10000006:2] REJECT SERANGAN SYN FLOODING(SERVER RIAS) [**] [Prior
ity: 0] [TCP] 240.240.75.9:1708 -> 192.168.100.11:80

```

Gambar 3.14 *Alert SYN Flood* pada IPS Suricata

Pada Gambar 3.14 terdapat tampilan *alert* pada saat ada serangan SYN *flooding* masuk kedalam server. *Alert* yang diberikan pada Suricata sesuai dengan rules. Untuk melihat *alert* maka server harus menjalankan perintah untuk melihat log aktivitas pada terminal dengan perintah `tail -f /var/log/suricata/fast.log`.

```

root@rias: /opt/zeek/etc
root@rias: /home/rias/zeek/checked/fyn
root@rias: /home/rias/zeek/checked/fyn
1674393019.193701 53.195.160.61 8 192.168.100.11 0 - 1 28 1 28
1674393019.194239 36.14.00.124 8 192.168.100.11 0 - 1 28 1 28
1674393019.198040 287.239.24.92 8 192.168.100.11 0 - 1 28 1 28
1674393023.050933 17.230.17.224 8 192.168.100.11 0 - 1 28 0 0
1674393038.548402 56.24.45.24 8 192.168.100.11 0 - 1 28 0 0
1674393035.623032 253.114.123.182 49988 192.168.100.11 80 r 1 40 0 40
1674393038.092383 192.168.100.11 3 214.46.134.210 3 - 1 56 0 0
1674393024.427651 200.53.27.37 8 192.168.100.11 0 - 1 28 1 28
1674393019.197479 63.65.166.235 8 192.168.100.11 0 - 1 28 1 28
1674393022.068973 192.168.100.11 3 159.14.161.219 3 - 1 28 0 0
1674393022.999222 174.75.62.220 8 192.168.100.11 0 - 1 28 0 0
1674393019.199129 46.19.21.291 8 192.168.100.11 0 - 1 28 0 0
1674393037.082809 194.82.154.121 8 192.168.100.11 0 - 1 28 0 0
1674393032.022031 102.151.13.47 8 192.168.100.11 0 - 1 28 0 0
1674393023.383318 152.125.178.240 8 192.168.100.11 0 - 1 28 1 28
1674393030.938906 156.155.284.219 8 192.168.100.11 0 - 1 28 0 0
1674393024.428499 167.129.198.53 8 192.168.100.11 0 - 1 28 2 28
1674393014.060239 192.168.100.11 3 74.155.288.8 3 - 1 56 0 0
1674393019.224938 251.862.157.180 5 192.168.100.11 0 - 1 28 1 28
1674393017.534554 173.46.198.3 8 192.168.100.11 0 - 1 28 1 28
1674393023.792744 118.13.60.6 8 192.168.100.11 0 - 1 28 0 0
1674393021.946904 192.168.100.11 3 53.50.43.124 3 - 1 56 0 0
1674393033.051855 121.131.17.138 8 192.168.100.11 0 - 1 28 1 28
1674393017.026416 17.27.01.53 8 192.168.100.11 0 - 1 28 0 0
1674393021.087604 40.131.131.240 8 192.168.100.11 0 - 1 28 0 0
1674393027.185677 121.190.56.129 8 192.168.100.11 0 - 1 28 1 28
1674393017.428659 39.198.56.190 8 192.168.100.11 0 - 1 28 0 0
1674393017.428659 192.168.100.11 3 8.92.107.138 3 - 1 56 0 0
1674393019.224938 143.90.17.118 8 192.168.100.11 0 - 1 28 1 28
1674393019.224938 234.161.208.02 8 192.168.100.11 0 - 1 28 0 0
1674393019.066042 201.195.129.45 8 192.168.100.11 0 - 1 28 1 28
1674393035.080935 196.185.88.183 28924 r 1 40 1 40
1674393019.225245 165.234.98.61 8 192.168.100.11 0 - 1 28 1 28
1674393019.225707 153.175.149.254 8 192.168.100.11 0 - 1 28 1 28
1674393022.716717 57.121.21.54 8 192.168.100.11 0 - 1 28 0 0
1674393019.226320 128.98.26.107 8 192.168.100.11 0 - 1 28 1 28
1674393024.302977 126.201.15.104 8 192.168.100.11 0 - 1 28 1 28
1674393019.090925 84.40.22.103 41547 192.168.100.11 80 - 1 40 0 0
1674393020.422293 187.226.198.167 8 192.168.100.11 0 - 1 28 0 0
1674393019.226320 44.187.150.113 8 192.168.100.11 0 - 1 28 0 0
1674393019.229337 235.95.174.44 8 192.168.100.11 0 - 1 28 0 0
1674393019.229886 92.139.200.45 8 192.168.100.11 0 - 1 28 1 28
1674393019.230474 119.58.95.109 8 192.168.100.11 0 - 1 28 1 28
1674393018.045559 39.198.50.152 8 192.168.100.11 0 - 1 28 1 28
1674393019.230998 47.235.138.149 8 192.168.100.11 0 - 1 28 1 28
1674393017.4195117 108.118.204.174 8 192.168.100.11 0 - 1 28 1 28
1674393016.012163 56.158.253.62 8 192.168.100.11 0 - 1 28 1 28
1674393019.232095 53.86.27.121 8 192.168.100.11 0 - 1 28 1 28
1674393019.016123 162.214.208.3 8 192.168.100.11 0 - 1 28 1 28
1674393027.418049 192.168.100.11 3 103.32.210.184 3 - 1 56 0 0
1674393019.283308 192.168.100.11 3 280.243.210.705 3 - 1 40 0 0
1674393018.249762 234.44.04.27 7037 192.168.100.11 80 - 1 40 0 0

```

Gambar 3.15 *Alert SYN Flood* pada IPS Zeek

Pada Gambar 3.15 terlihat Zeek dapat menampilkan peringatan saat menerima *signature* yang sesuai dengan *rules* saat mendeteksi serangan SYN *Flood*, yang berarti Zeek dapat mengirimkan peringatan ketika serangan SYN *Flood* terjadi di server.

1.2.6 ANALISI HASIL

Dalam tahap penelitian ini, penulis membuat analisis perbandingan atau komparatif

dari ketiga *tools* IPS yaitu Snort, Suricata dan Zeek untuk mendeteksi serangan *Distributed Denial of Service* (Ddos) dengan menggunakan aplikasi analisis jaringan, yaitu Wireshark. Dalam Metode perbandingan ini yang akan dikukur adalah *Quality of Service* (QoS). Parameter QoS yang diukur yaitu *throughput*, *delay*, *jitter* dan *packet loss*.

1. *Throughput*

Pengukuran *throughput* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON). Dimana dalam pengukurannya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut.

Table 3.8 Standar Kualitas *Throughput*

Kategori <i>Throughput</i>	Nilai <i>Throughput</i> (bps)	Indeks
Sangat Baik	100	4
Baik	75	3
Cukup Baik	50	2
Buruk	<25	1

(Sumber : TIPHON 1999-2006) [22]

2. *Delay*

Pengukuran *delay* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON). Dimana dalam pengukurannya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut.

Tabel 3.9 Standar Kualitas *Delay*

Kategori <i>Latency</i>	Nilai <i>Delay (ms)</i>	Indeks
Sangat Baik	<150 ms	4
Baik	150 ms s/d 300 ms	3
Cukup Baik	300 s/d 450 ms	2
Buruk	>450 ms	1

(Sumber : TIPHON 1999-2006) [22]

3. *Jitter*

Pengukuran *jitter* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON). Dimana dalam pengukurannya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut

Tabel 3.10 Standar Kualitas *Jitter*

Kategori <i>Jitter</i>	<i>Peak Jitter (ms)</i>	Indeks
Sangat Baik	0 ms	4
Baik	1 s/d 75 ms	3
Cukup Baik	76 s/d 125 ms	2
Buruk	>225 ms	1

(Sumber :TIPHON 1999-2006) [22]

4. *Packet Loss*

Pengukuran *jitter* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON). Dimana dalam pengukurannya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut.

Tabel 3.11 Standar Kualitas *Packet Loss*

<u>Kategori</u> <i>Degradasi</i>	Nilai <i>Packet Loss (%)</i>	<u>Indeks</u>
<u>Sangat Baik</u>	0 – 2%	4
<u>Baik</u>	3 - 14%	3
<u>Cukup Baik</u>	15 - 24%	2
<u>Buruk</u>	>25%	1

(Sumber : TIPHON 1999-2006) [22]