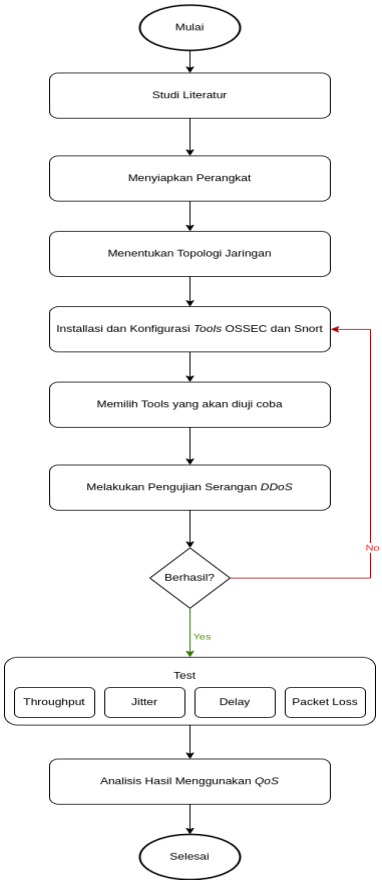
BAB III
METODE PENELITIAN

3.1 Objek dan Subjek Penelitian

Objek penelitian dari penelitian ini yaitu perbandingan performansi dari *tools* OSSEC dan Snort yang meliputi pendeteksian dan pencegahan menggunakan *Intrusion Detection and Prevention System (IDPS)* yang diimplementasikan pada sebuah laptop yang menjadi *server* yang telah dikonfigurasi. Dan untuk subjek penelitiannya adalah *tools* OSSEC dan Snort. Sumber data yang diperoleh berasal dari hasil uji coba *tools* OSSEC dan Snort di server *Intrusion Detection and Prevention System (IDPS)* dengan pengujian serangan *Distributed Denial of Service (DDoS)* dengan menggunakan *Quality of Service (*QoS*).*

3.2 Diagram Alir Penelitian

Penelitian ini dilakukan secara sistematis yang dimulai dari studi literatur terkait dengan teori penelitian yang dilakukan. Setelah membaca teorinya, dilanjutkan dengan menyiapkan semua perangkat lunak dan keras yang dibutuhkan pada PC server, PC *client*, dan PC *attacker*. Kemudian, dilanjutkan dengan menentukan topologi jaringan yang tepat. Setelah dirancang topologi jaringan yang tepat, penulis melanjutkan dengan melakukan instalasi dan konfigurasi *tools IDPS* OSSEC dan Snort. Setelah berhasil melakukan instalasi dan konfigurasi pada *tools IDPS* OSSEC dan Snort. Selanjutnya dilakukan pemilihan *tools* untuk dilakukan pengujian serangan dan jika tidak berhasil akan dilakukan pengecekan konfigurasi kembali dan jika berhasil akan dilanjutkan ke tahap analisis hasil dari data yang telah didapatkan dari pengujian menggunakan parameter QoS. Berikut pemaparan alur diagram yang dirancang pada penelitian ini :



Gambar 3. 1 Diagram Alir Penelitian

3.2.1 Studi Literatur

Setelah ditemukan masalah terkait penelitian ini, peneliti akan melakukan studi literatur sebagai landasan pengetahuan dasar dalam melakukan analisa, perancangan, implementasi, dan pengujian untuk mendukung penelitian yang akan dilakukan. Referensi yang diambil berasal dari buku, jurnal, *website*, dan penelitian yang sejenis dengan penelitian yang dilakukan peneliti.

3.2.2 Menyiapkan Perangkat

Setelah melakukan studi literatur, penulis akan menyiapkan perangkat yang dibutuhkan. Dimulai dari menentukan kebutuhan

hardware dan *software.* Berikut tabel kebutuhan *hardware dan software :*

Tabel 3. 1 Kebutuhan *hardware*

No	Perangkat	Unit	Keterangan
1	Laptop	1	Sebagai *server*
2	Komputer	1	Sebagai *client*
3	Komputer	10	Sebagai penyerang
4	Mikrotik	1	Sebagai penyedia jaringan *private*
5	Kabel LAN *(straight over)*	1	Sebagai penghubung jaringan LAN

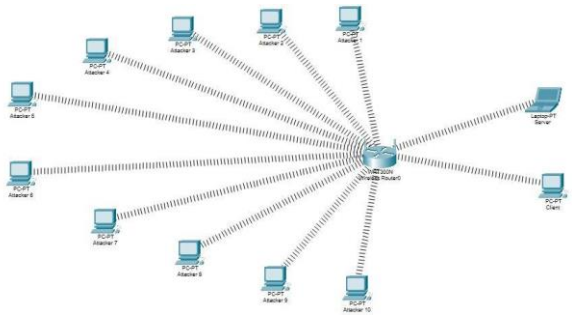
Tabel 3. 2 Kebutuhan *software*

No	Pengguna	Perangkat Lunak	Keterangan
1	PC *Server*	*Ubuntu version 20.04*	Sistem operasi server
		OSSEC	*Tools IDPS*
		Snort	*Tools IDPS*
2	PC *Client*	*Windows*	Sistem operasi *client*
		Wireshark	*Tools* untuk melakukan *capture* data yang melewati suatu jaringan
3	PC Penyerang	*Ubuntu version* 20.04	Sistem operasi penyerang
		Hping3	*Tools* untuk melakukan serangan *UDP, TCP, ICMP Flood*

3.2.3 Topologi Jaringan

Sebelum melakukan penginstalan *tools,* akan dilakukan perancangan topologi jaringan. Penelitian ini menggunakan sistem jaringan *Local Area Network (LAN).* Jaringan pada setiap PC ini didapatkan dari *wireless router.* Pada topologi jaringan ini, penulis menggunakan 10 PC yang berperan sebagai *attacker* dimana di PC tersebut sudah terinstal *tools* untuk melakukan serangan *DDoS* yaitu HPing3. Dan pada penelitian ini juga menggunakan 1 laptop sebagai server dimana di server tersebut terdapat *tools* yang akan diuji coba yaitu Snort dan OSSEC. Selain itu, juga digunakan 1 PC yang berperan sebagai *client* yang bertugas memantau jaringan *Local Area*

Network (LAN) yang telah dibuat. Topologi jaringan penelitian ini ditunjukkan pada Gambar 3.2.



Gambar 3. 2 Gambar topologi jaringan

3.2.4 Instalasi dan Konfigurasi Tools (OSSEC DAN SNORT)

A. Instalasi dan Konfigurasi OSSEC

1. Instalasi OSSEC

Langkah pertama yang dilakukan pada saat instalasi OSSEC adalah melakukan *update* dan *upgrade* sistem dengan tujuan semua berjalan dengan lancar nantinya tidak ada ada yang rusak saat proses penginstalan karena belum *update* dan *upgrade*. Setelah itu dilanjutkan dengan menginstal *library* yang dibutuhkan OSSEC. Kemudian dilanjutkan dengan melakukan instalasi OSSEC. Berikut perintah penginstalan OSSEC dibawah ini.

Instalasi *library*
$sudo su #apt-get update -y && apt-get upgrade -y #sudo apt install -y git php php-cli php-common libapache2-mod-php apache2-utils sendmail inotify-tools apache2 build-essential gcc make wget tar zlib1g-dev lib pcre2-dev libpcre3-dev unzip libz-dev libssl-dev lib pcre2-dev libevent-dev build-essential libsystemd-dev #systemctl enable apache2 #systemctl start apache2

```
#aenmod rewrite
#sudo systemctl restart apache2
#./install.sh
```

Instalasi OSSEC

```
$sudo su
#wget https://github.com/ OSSEC/ OSSEC-
hids/archive/3.7.0.tar.gz
#tar -xvzf3.7.0.tar.gz
```

2. Konfigurasi OSSEC

Setelah selesai penginstalan, dilanjutkan dengan melakukan *setting* konfigurasi pada OSSEC. Berikut tahapan konfigurasi OSSEC.

Konfigurasi OSSEC

```
#cd /var/ OSSEC/etc
#sudo nano OSSEC.conf
```

Setelah membuka direktori /var/OSSEC/etc, maka dilanjutkan dengan melakukan konfigurasi pada *file OSSEC.conf* seperti pada perintah dibawah ini.

```
<ossec_config>
  <global>
    <email_notification>no</email_notification>
  </global>

  <!-- Only DDoS Rules & add custom decoder
(network_decoder.xml) -->
  <rules>
    <decoder>etc/decoder.xml</decoder>
    <include>local_rules.xml</include>
  </rules>

  <syscheck>
```

```
   <!-- Frequency that syscheck is executed - default to every
22 hours -->
   <frequency>79200</frequency>

   <!-- Directories to check  (perform all possible
verifications) -->
   <directories
check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
   <directories
check_all="yes">/bin,/sbin,/boot</directories>

   <!-- Files/directories to ignore -->
   <ignore>/etc/mtab</ignore>
   <ignore>/etc/mnttab</ignore>
   <ignore>/etc/hosts.deny</ignore>
   <ignore>/etc/mail/statistics</ignore>
   <ignore>/etc/random-seed</ignore>
   <ignore>/etc/adjtime</ignore>
   <ignore>/etc/httpd/logs</ignore>
   <ignore>/etc/utmpx</ignore>
   <ignore>/etc/wtmpx</ignore>
   <ignore>/etc/cups/certs</ignore>
   <ignore>/etc/dumpdates</ignore>
   <ignore>/etc/svc/volatile</ignore>

   <!-- Windows files to ignore -->
   <ignore>C:\WINDOWS/System32/LogFiles</ignore>
   <ignore>C:\WINDOWS/Debug</ignore>
   <ignore>C:\WINDOWS/WindowsUpdate.log</ignore>
   <ignore>C:\WINDOWS/iis6.log</ignore>
   <ignore>C:\WINDOWS/system32/wbem/Logs</ignore>

<ignore>C:\WINDOWS/system32/wbem/Repository</ignor
e>
   <ignore>C:\WINDOWS/Prefetch</ignore>

<ignore>C:\WINDOWS/PCHEALTH/HELPCTR/DataColl<
/ignore>
   <ignore>C:\WINDOWS/SoftwareDistribution</ignore>
   <ignore>C:\WINDOWS/Temp</ignore>
   <ignore>C:\WINDOWS/system32/config</ignore>
   <ignore>C:\WINDOWS/system32/spool</ignore>
   <ignore>C:\WINDOWS/system32/CatRoot</ignore>
 </syscheck>
```

```
<!-- Frequency that syscheck is executed - default to every
22 hours -->
   <frequency>79200</frequency>

   <!-- Directories to check  (perform all possible
verifications) -->
   <directories
check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
   <directories
check_all="yes">/bin,/sbin,/boot</directories>

   <!-- Files/directories to ignore -->
   <ignore>/etc/mtab</ignore>
   <ignore>/etc/mnttab</ignore>
   <ignore>/etc/hosts.deny</ignore>
   <ignore>/etc/mail/statistics</ignore>
   <ignore>/etc/random-seed</ignore>
   <ignore>/etc/adjtime</ignore>
   <ignore>/etc/httpd/logs</ignore>
   <ignore>/etc/utmpx</ignore>
   <ignore>/etc/wtmpx</ignore>
   <ignore>/etc/cups/certs</ignore>
   <ignore>/etc/dumpdates</ignore>
   <ignore>/etc/svc/volatile</ignore>

   <!-- Windows files to ignore -->
   <ignore>C:\WINDOWS/System32/LogFiles</ignore>
   <ignore>C:\WINDOWS/Debug</ignore>
   <ignore>C:\WINDOWS/WindowsUpdate.log</ignore>
   <ignore>C:\WINDOWS/iis6.log</ignore>
   <ignore>C:\WINDOWS/system32/wbem/Logs</ignore>

<ignore>C:\WINDOWS/system32/wbem/Repository</ignor
e>
   <ignore>C:\WINDOWS/Prefetch</ignore>

<ignore>C:\WINDOWS/PCHEALTH/HELPCTR/DataColl<
/ignore>
   <ignore>C:\WINDOWS/SoftwareDistribution</ignore>
   <ignore>C:\WINDOWS/Temp</ignore>
   <ignore>C:\WINDOWS/system32/config</ignore>
   <ignore>C:\WINDOWS/system32/spool</ignore>
   <ignore>C:\WINDOWS/system32/CatRoot</ignore>
 </syscheck>
```

```
  <rootcheck>

<rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit
_files>

<rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</ro
otkit_trojans>

<system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</s
ystem_audit>

<system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.tx
t</system_audit>

<system_audit>/var/ossec/etc/shared/cis_rhel_linux_rcl.txt</
system_audit>

<system_audit>/var/ossec/etc/shared/cis_rhel5_linux_rcl.txt
</system_audit>
  </rootcheck>

  <active-response>
    <disabled>yes</disabled>
  </active-response>

  <remote>
    <connection>syslog</connection>
  </remote>

  <remote>
    <connection>secure</connection>
  </remote>

  <alerts>
    <log_alert_level>10</log_alert_level>
  </alerts>

  <!-- Files to monitor (localfiles) -->
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/iptables.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
```

```
  <location>/var/log/iplog</location>
 </localfile>
 <localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
 </localfile>

 <localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
 </localfile>

 <localfile>
  <log_format>syslog</log_format>
  <location>/var/log/dpkg.log</location>
 </localfile>

 <localfile>
  <log_format>command</log_format>
  <command>df -P</command>
 </localfile>

 <localfile>
  <log_format>full_command</log_format>
  <command>netstat -tan |grep LISTEN |egrep -v
'(127.0.0.1| ::1)' | sort</command>
 </localfile>

 <localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
 </localfile>
</ossec_config>
```

3. Instalasi OSSEC WUI

Tahap berikutnya adalah melakukan penginstalan OSSEC-WUI dan setelah selesai dilanjutkan dengan pengkonfigurasian OSSEC-WUI. OSSEC WUI terletak pada /var/www/html dan dapat dijalankan pada *port* 8000. Pada tahap terakhir melakukan *restart* OSSEC-WUI. Berikut perintah penginstalan OSSEC-WUI dibawah ini.

Instalasi OSSEC WUI
#git clone https://github.com/ OSSEC/ OSSEC-WUI.git #cd /var/www/html/ OSSEC-WUI # ./setup.sh

4. Konfigurasi OSSEC WUI

Setelah dilakukan penginstalan dilanjutkan dengan pengkonfigurasian pada OSSEC WUI seperti pada perintah dibawah ini.

Konfigurasi OSSEC WUI
#cd /etc/apache2/sites-enabled #sudo nano 000-default.conf #cd /etc/apache2 #sudo nano ports.conf #systemctl restart apache

B. Instalasi dan Konfigurasi Snort

1. Instalasi Snort

Langkah pertama yang dilakukan adalah melakukan *update* dan *upgrade.* Kemudian dilanjutkan dengan menginstal *library* yang dibutuhkan Snort. Selanjutnya, melakukan instalasi Snort. Berikut perintahnya dibawah ini.

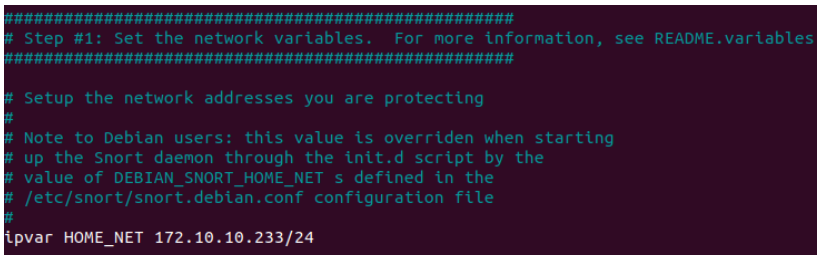
Instalasi Snort
$sudo su #apt-get update -y && apt-get upgrade -y #apt-get install openssh-server ethtool build-essential lib pcap-dev lib pcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev autoconf #apt-get install Snort #Snort -V

2. Konfigurasi Snort

Setelah proses penginstalan selesai dilakukan, dilanjutkan dengan pengkonfigurasian pada *file snort.conf* yang terletak pada direktori /etc/snort. Berikut perintahnya dibawah ini.

Konfigurasi Snort
#cd /etc/snort #sudo nano snort.conf

Berikut tampilan *snort.conf* pada Gambar 3.3 dimana pada langkah pertama dilakukan pengubahan *IP address* pada HOME_NET dari *any* menjadi *IP address* pada server, yaitu 172.10.10.233/24 seperti pada gambar dibawah ini.



Gambar 3. 3 Konfigurasi IP Address Snort

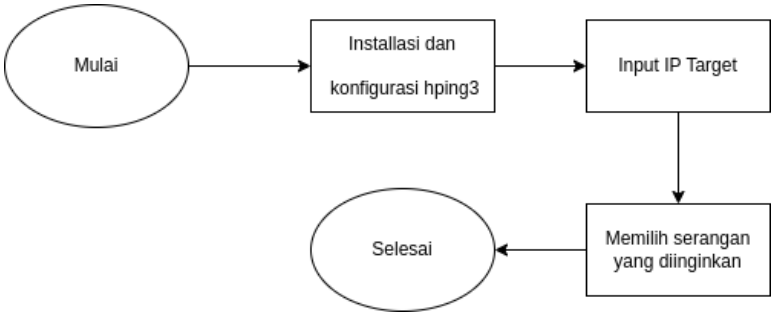
Setelah dilakukan pengkonfigurasian pada *file* snort*.conf*, dilanjutkan dengan melakukan pengkonfigurasian pada *file local.rules* dimana *file ini* nantinya akan memuat pendeteksian dan pencegahan berupa *drop* paket dari serangan *ICMP*, *UDP*, dan *TCP Flood.* Berikut perintahnya dibawah ini.

Konfigurasi Rules Snort
#cd /etc/snort/rules #sudo nano local.rules

Pada Gambar 3.4 ini, merupakan tampilan dari *local.rules* yang telah dibuat untuk menampilkan nantinya jika ada serangan yang masuk berupa *alert.*

Gambar 3. 4 Rules Snort

3.2.5 Melakukan Pengujian Serangan



Gambar 3. 5 Diagram Alur *DDoS Attack*

Serangan yang dilakukan adalah *DDoS* dengan menggunakan *tools* HPing3. Langkah pertama yang dilakukan adalah membuka terminal dan dilanjutkan dengan melakukan instalasi HPing3 dengan mengetikkan perintah sudo apt-get install hping3 pada terminal. Setelah terinstal, dilanjutkan dengan pemilihan target serangan yang akan dilakukan, seperti *ICMP*, *TCP*, dan *UDP*. Kemudian setelah memilih serangan tekan enter pada keyboard dan serangan akan dimulai. Dan untuk memberhentikan serangan tekan Ctrl +C pada keyboard. Berikut perintahnya dibawah ini.

```
#ICMP Flood →sudo hping3 172.10.10.233 --icmp --Flood
#TCP Flood → sudo hping3 172.10.10.233 -S -p 80 --Flood
#UDP Flood → sudo hping3 172.10.10.233 --udp -p 80 --Flood
```

3.2.6 Analisis Hasil

Analisis data pada penelitian ini adalah menggunakan metode *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.

2. *Delay*

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

3. *Jitter*

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

4. *Packet loss*

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