BAB III
METODOLOGI PENELITIAN

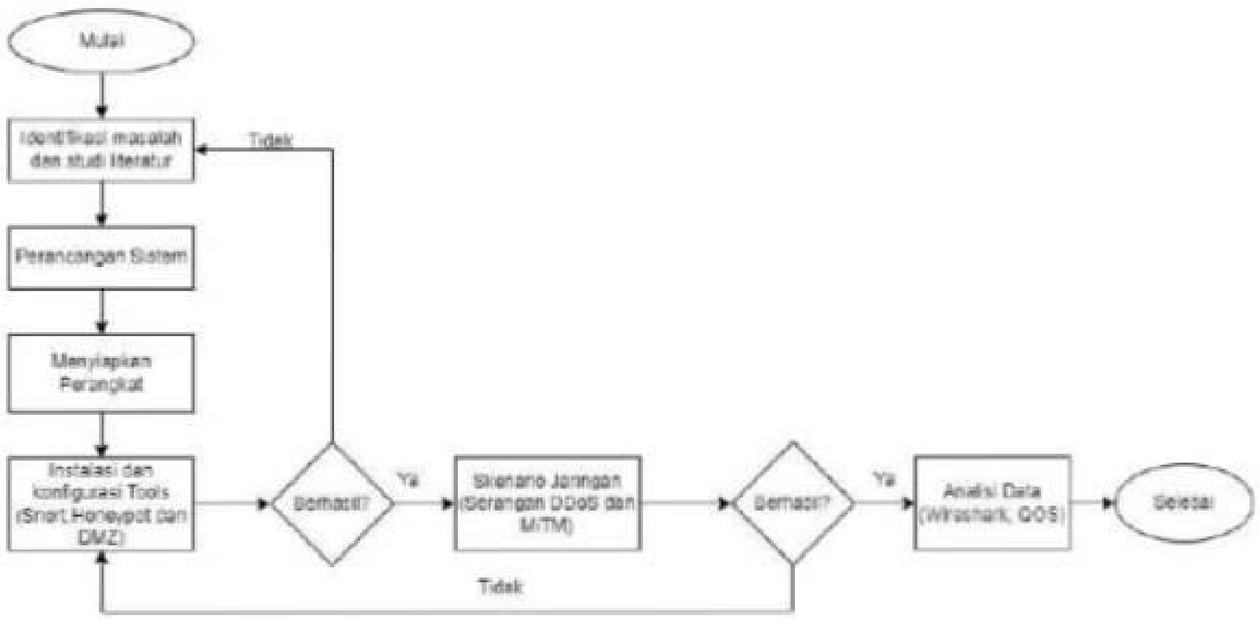
3.1 OBJEK DAN SUBJEK PENELITIAN

Dalam penelitian ini, objek yang dikaji adalah anailisis keamanan sistem jaringan menggunakan *(IDPS)* snort dan honeypot cowrie yang diimplementasikan pada server yang telah dikonfigurasi IDPS. Sedangkan subjek pada penelitian ini adalah tools DMZ,cowrie dan snort.Sumber data yang diperoleh dari hasil uji coba dengan tools server IDPS dengan pengujian menggunakan QOS.

3.2 DIAGRAM DAN ALUR PENELITIAN

Pada penelitian ini, flowchart penelitian diimplementasikan secara sistematis dalam beberapa langkah. Dari mana memulai identifikasi masalah dan penelitian literatur, yang nantinya akan dilanjutkan dalam perancangan sistem.Sistem yang terencana dan dirancang tentunya membutuhkan beberapa perangkat, seperti : Software dan hardware yang digunakan untuk menginstal dan mengkonfigurasi DMZ, Snort dan Honeypot Cowrie. Jika sistem berhasil diinstal dan dikonfigurasi, maka akan terus dilakukan upaya serangan yaitu DDoS dan Man-in-the-Middle (MiTM). Namun, jika penginstalan dan pengaturan sistem gagal, tema dan sistem akan dijalankan kembali. Selain itu, serangan dilakukan di lain waktu dengan menganalisis hasil akurasi menggunakan metode QOS dan menganalisis hasil jaringan ketika tidak ada serangan atau terjadi serangan.

Adapun pemaparan alur diagram yang dirancang pada penelitian ini yang tedapat pada Gambar 3.1.

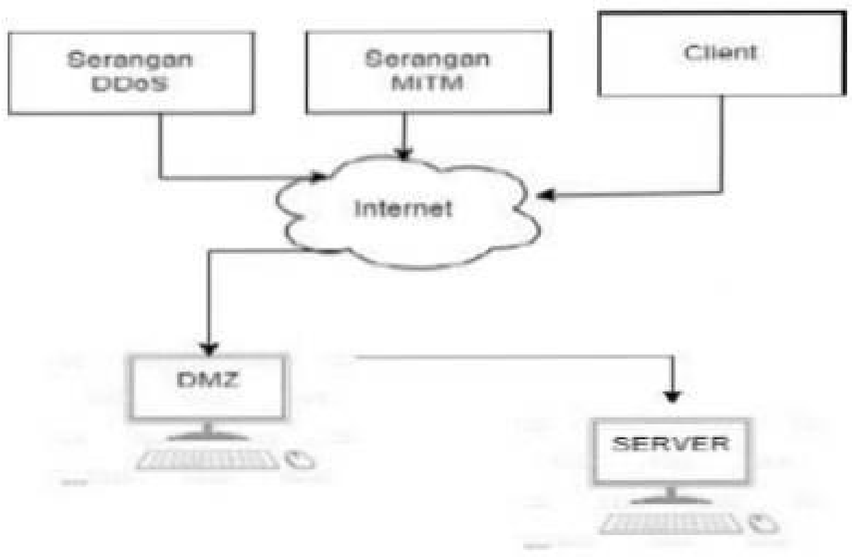


Gambar 3.1 Alur Penelitian

3.2.1 IDENTIFIKASI MASALAH DAN STUDI LITERATUR

Dalam jaringan komputer, misalnya jaringan WLAN, dimungkinkan untuk memberikan informasi dengan cepat di jaringan lokal. Namun, selalu ada celah yang dapat merusak sistem yang dibuat oleh administrator jaringan, yang terutama bertanggung jawab atas keamanan sistem jaringan komputer. Jika terjadi pembobolan, administrator sistem tidak selalu siap sedia. Artinya, pencurian tidak dapat dideteksi, dicegah, atau diprediksi. Oleh karena itu, penulis mengumpulkan referensi-referensi yang diperlukan sebagai dasar tahapan penelitian, dan referensi yang digunakan penulis adalah jurnal-jurnal sebelumnya yang masih berkaitan dengan penelitian ini. Selain jurnal-jurnal sebelumnya, penulis menggunakan e-book untuk melengkapi informasi tentang metode yang digunakan.

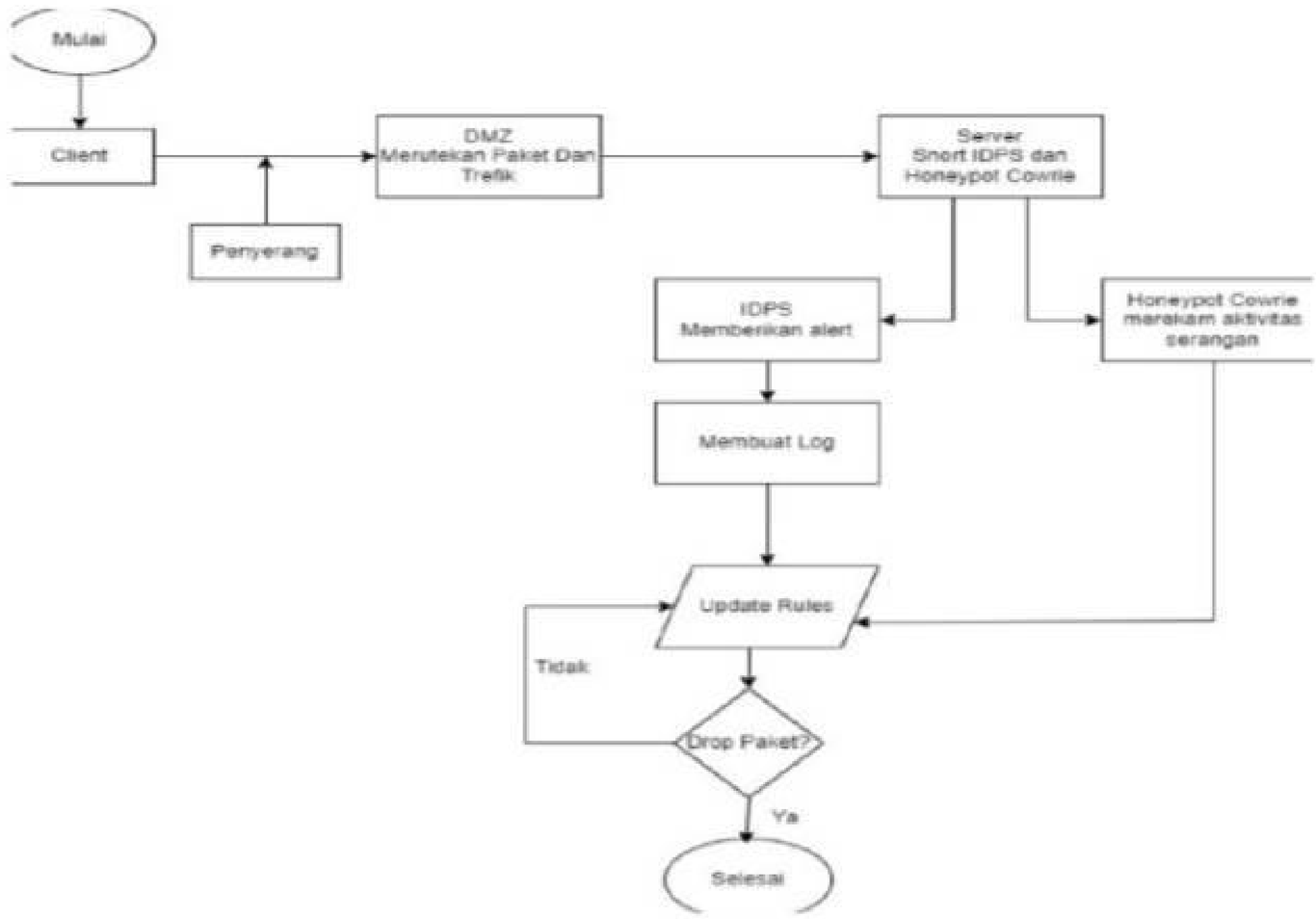
3.2.2 PERANCANGAN SISTEM



Gambar 3. 2 Topologi Perancangan Sistem

Berdasarkan Gambar 3.2 pengujian sistem terhadap serangan ini dirancang dengan simulsi dengan tiga PC. PC pertama sebagai router yang didalamnya terdapat DMZ, fungsi dari DMZ ini adalah untuk melindungi server dari serangan secara penuh.PC kedua digunakan untuk server yang didalamnya terdapat honeypot cowrie dan snort.Honeypot cowrie bertugas untuk merekam semua aktivitas penyerang dan mengumpulkan informasi yang berharga tentang serangan yang masuk.Snort (IDPS) bertugas untuk meenganalisi lalu lintas jaringan dan mendeteksi pola serang yang tidak normal. Snort dapat memantau dan mengidentifikasi aliran paket jaringan yang mencurigakan, seperti peningkatan lalu lintas yang tidak wajar, dan memberikan peringatan kepada administrator jaringan untuk mengambil tindakan yang sesuai.

Pada tahap pengujian skenario, sistem ini menggambarkan alur kerja sistem sehingga dapat mencegah serangan, yang dapat dijelaskan pada gambar di bawah ini:



Gambar 3.3 Alur Kerja Sistem

Berdasarkan gambar 3.3 dapat dijelaskan bahwa attcker akan menyerang menggunakan serang DDoS dan MiTM, pada tahap ini apabila

attacker berhasil menembus *firewall* maka attacker akan masuk ke sistem palsu yang telah di buat oleh *honeypot* dan aktivitas penyerang akan direkam oleh honeypot cowrie. Didalam *snort* akan bekerja yaitu mendeteksi *attacker* dan apabila dia tidak terdeteksi maka akan mendeteksi ulang, dan jika terdeteksi maka attacker akan di blok.

3.2.3 ANALISA KEBUTUHAN SISTEM

Saat menganalisis persyaratan sistem, sistem jaringan harus dapat berfungsi dengan baik, yang menjelaskan berbagai persyaratan yang mencakup persyaratan sistem pada tabel dibawah ini:

No.	Pengguna	Perangkat Lunak	Keterangan
1.	PC Router	Ubuntu Dekstop v20.04 Iptables v1.8.4	Sistem Operasi PC Router Aplikasi *firewall* yang dikonfigurasi sebagai DMZ *network*
2.	PC Server	Ubuntu Dekstop v20.04 Snort v2.9.7.8 Honeypot Cowrie v2.2.0	Sistem operasi PC server Tools IDPS yang bertugas memberikan peringan, memblokir dan membuat rules Mengamati log yang dihasilkan oleh Cowrie dan Snort secara teratur untuk mendeteksi aktivitas mencurigakan atau serangan terhadap DMZ
3	PC	Ubuntu v20.04	Sistem operasi penyerang

	Penyerang	LOIC Attercap Hping3	*Tools* DDoS *attack* (TCP dan UDP) *Tools* MiTM *attack* *Tools* DDoS *attack* (ICMP)
4.	Client	Windows 10	Sistem operasi client

Tabel 3.1 Kebutuhan sistem

3.2.4 INSTALASI DAN KONFIGURASI SISTEM

1). Instalasi dan konfigurasi DMZ

Untuk melakukan konfigurasi DMZ yang awal yang harus diperhatikan yaitu memiliki infrastruktur jaringan yang dapat memungkinkan implementasi DMZ dan memiliki router dan firewall yang dapat mendukung konfigurasi DMZ.Dan sebelum melakukan konfigurasi pastikan IP address pada interface yang akan dijadikan DMZ.Tahap pertama, pastikan bahwa kedua antarmuka sebuah jaringan diaktifkan, perintah yang digunakan untuk memeriksa antarmuka yaitu *ip a* perhatikan antarmuka yang terhubung ke internet. Opsi lain adalah menginstal iptables dan membuat file di */etc/network/if-up.d/* seperti iptabless-dmz # *nano /etc/network/if-up.d/iptables-dmz* lalu file tersebut akan disimpan dan keluar dan lalu ubah kepemilikan file dmz .sh Jika kepemilikan file telah berubah, jalankan dmz.sh dengan sudo *./etc/network/if-up.d/dmz.sh*. Batasi paket masuk dan cegah serangan pada komputer Anda dengan mengaktifkan mode penerusan dengan perintah *sudo nano /etc/sysctl.conf*. Kemudian, terapkan aturan inti di file *sysctl.conf* dan perbarui sesuai dengan perintah *sudo sysctl -p /etc/sysctl. conf* .Agar dapat terhubung ke internet dan menggunakan NAT dan WAN jika perlu *tools resolver* dengan menggunakan perintah *sudo apt install resolvconf* ketika melakukan konfigurasi resolver tersebut dengan menggunakan perintah *sudo nano /etc/resolvconf/resolv.conf.d/head*. Untuk tahap terakhir pada konfigurasi DMZ yaitu dengan melakukan update resolver dengan

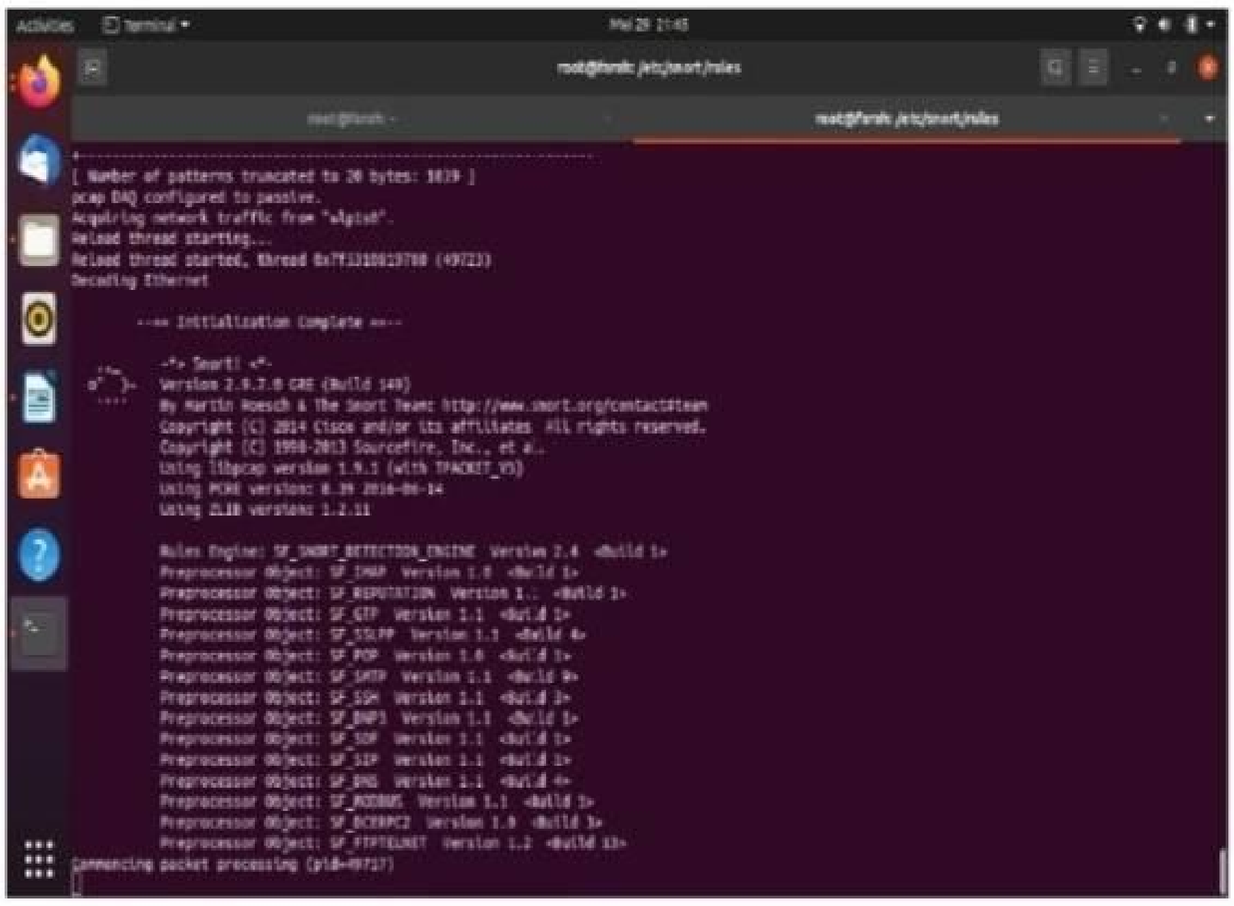
menggunakan perintah *sudo resolvconf -u.*

2) Melakukan penginstallan *tool Snort* pada Ubuntu

Tahap instalasi Snort mulai memperbarui dan memperbarui sistem Ubuntu 20.04. Setelah memperbarui dan meningkatkan, langkah selanjutnya adalah menginstal dependensi yang diperlukan *(package* dan *library)* untuk Snort. Setelah dependensi diinstal, lanjutkan untuk mengunduh dan menginstal Snort. Lihat tabel di bawah untuk petunjuk instalasi rinci untuk Snort.Script yang digunakan untuk mengintsall paket-paket tersebut adalah:

```
sudo apt install -y gcc libpcre3-dev zlib1g-
dev libluajit-5.1-dev libpcap-dev membukasl
libssl-dev libnghttp2-dev libdumbnet-dev bison
flex libdnet autoconf libtool
```

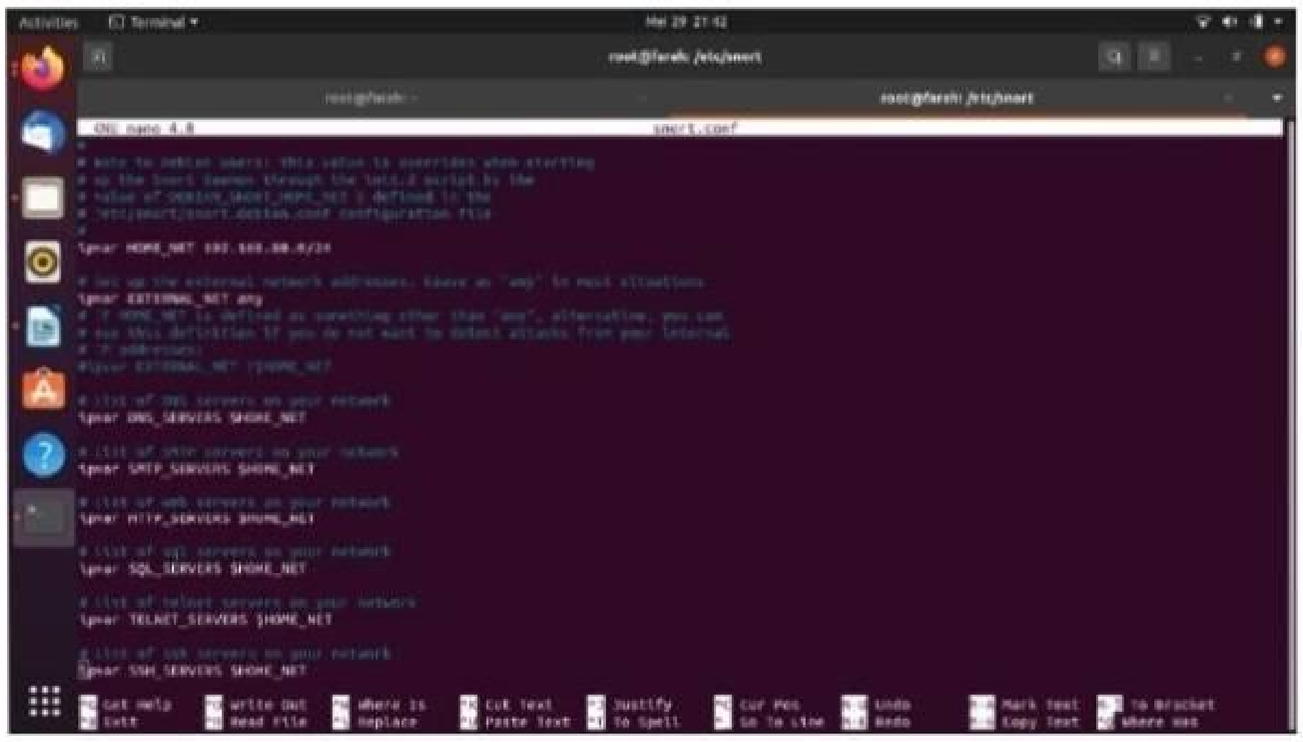
Instalasi Snort juga bisa dilakukan dengan menggunakan perintah apt-get isnatll snort atau bisa juga dilakukan dengan mengunduh program pada sistus (www.snort.org) Setelah snort berhasil diinstall maka lakukan pengecekan pada konfigurasi yang telah dilakukan seperti berikut ini:



Gambar 3.4 Penginstalan Snort Complete

a). Melakukan konfigurasi Snort.conf

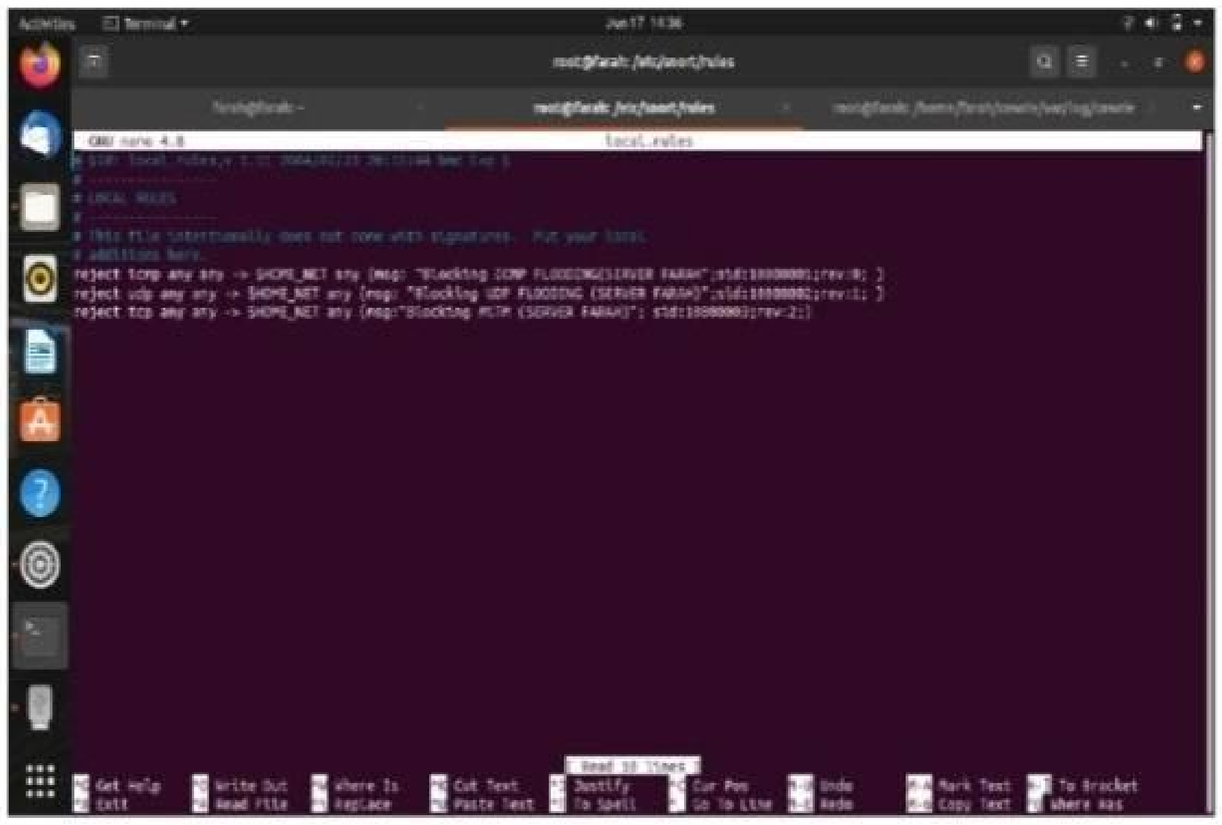
Untuk melakukan konfigurasi Snort.conf dapat membuka File konfigurasi Snort terletak di file /etc/snort/snort.conf di dalam file snort.conf. Pengaturan pertama adalah menyimpan aturan di direktori dan mengkonfigurasi jaringan. Di Snort.conf Anda dapat menentukan alamat jaringan dengan memberikan alamat IP host, yaitu 192.168.88.0/24, dan nama alamat grup, yaitu HOME_NET. Di file Snort.conf Anda dapat membuat aturan atau perintah untuk mendapatkan alamat email, menemukan antarmuka yang akan digunakan dan menjalankan fungsi IDPS. penetapan alamat IP dapat dilihat dibawah ini:



Gambar 3.5 Konfigurasi Snort.conf

b). Melakukan konfigurasi file rules

Simpan aturan yang ditentukan pada langkah ini disimpan dalam direktori bernama RULE_PATH. Selanjutnya, aktifkan file local.rules, dimana file ini dapat menambahkan aturan yang memungkinkan Snort mengeluarkan peringatan ketika mendeteksi serangan. Untuk penulisan ini, peneliti menggunakan aturan untuk mendeteksi dan memblokir serangan ICMP,UDP dan MiTM yang masuk kedalam server yang ditujukan pada gambar dibawah ini:



Gambar 3.6 Konfigurasi File Rules

3) Instalasi dan konfigurasi Honeypot Cowrie

Pada instalasi honeypot cowrie terdapat beberapa tahapan, yang pertama mengintsall dependensi dengan menggunaka perintah

```
root@cowrie:~# apt update
root@cowrie:~# apt-get install git python-virtualenv libssl-dev libffi-dev build-essential
libpython-dev python2.7-minimal authbind
root@cowrie:~# adduser --disabled-password cowrie
Adding user `cowrie' ...
Adding new group `cowrie' (1000) ...
Adding new user `cowrie' (1000) with group `cowrie' ...
Creating home directory `/home/cowrie' ...
Copying files from `/etc/skel' ...
Changing the user information for cowrie
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root@cowrie1:~# su - cowrie
cowrie@cowrie1:~$
```

Gambar 3.7 Penginstalan Depedensi Cowrie

Selanjutnya, ambil for cowrie menggunakan git

```
cowrie@cowrie1:~$ git clone http://github.com/micheloosterhof/cowrie
Cloning into 'cowrie'...
remote: Counting objects: 9340, done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 9340 (delta 3), reused 2 (delta 0), pack-reused 9330
Receiving objects: 100% (9340/9340), 7.43 MiB | 2.32 MiB/s, done.
Resolving deltas: 100% (6415/6415), done.
Checking connectivity... done.
cowrie@cowrie1:~$
```

Gambar 3.8 Mengambil cowrie di Github

Selanjutnya membuat virtual untuk menjalankan python dan cowrie

```
cowrie@cowrie1:~$ cd cowrie
cowrie@cowrie:~/cowrie$ virtualenv cowrie-env
Running virtualenv with interpreter /usr/bin/python2
New python executable in /home/cowrie/cowrie/cowrie-env/bin/python2
Also creating executable in /home/cowrie/cowrie/cowrie-env/bin/python
Installing setuptools, pkg_resources, pip, wheel...done.
cowrie@cowrie1:~$
```

Gambar 3.9 Menjalankan Python

langkah selanjutnya, aktifkan lingkungan virtual python, dan instal pyhton cowrie perlu dijalankan

```
cowrie@cowrie1:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env)  cowrie@cowrie1:~/cowrie$ pip install --upgrade pip
Requirement already up-to-date: pip in ./cowrie-env/lib/python2.7/site-packages
(cowrie-env) cowrie@cowrie1:~/cowrie$ pip install --upgrade -r requirements.txt
Collecting twisted>=17.1.0 (from -r requirements.txt (line 1))
  Downloading Twisted-17.9.0.tar.bz2 (3.0MB)
    100% |????????????????????????????????| 3.0MB 403kB/s
Collecting cryptography>=0.9.1 (from -r requirements.txt (line 2))
  Downloading cryptography-2.2-cp27-cp27mu-manylinux1_x86_64.whl (2.2MB)
    100% |????????????????????????????????| 2.2MB 544kB/s
```

Gambar 3. 10 Mengaktifkan Lingkungan virtual python

Selanjutnya, untuk mengonfigurasi cowrie, dan memulai

```
cp cowrie.cfg.dist cowrie.cfg
```

Gambar 3.11 Mengkonfigurasi cowrie

Terakhir jalankan perintah dibawah ini

```
cowrie@cowrie:~/cowrie$ bin/cowrie start
Using default Python virtual environment "/home/cowrie/cowrie/cowrie-env"
Starting cowrie: [twistd   --umask 0022 --pidfile var/run/cowrie.pid --logger
cowrie.python.logfile.logger cowrie ]...

cowrie@cowrie:~/cowrie$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Gambar 3.12 Menjalankan cowrie

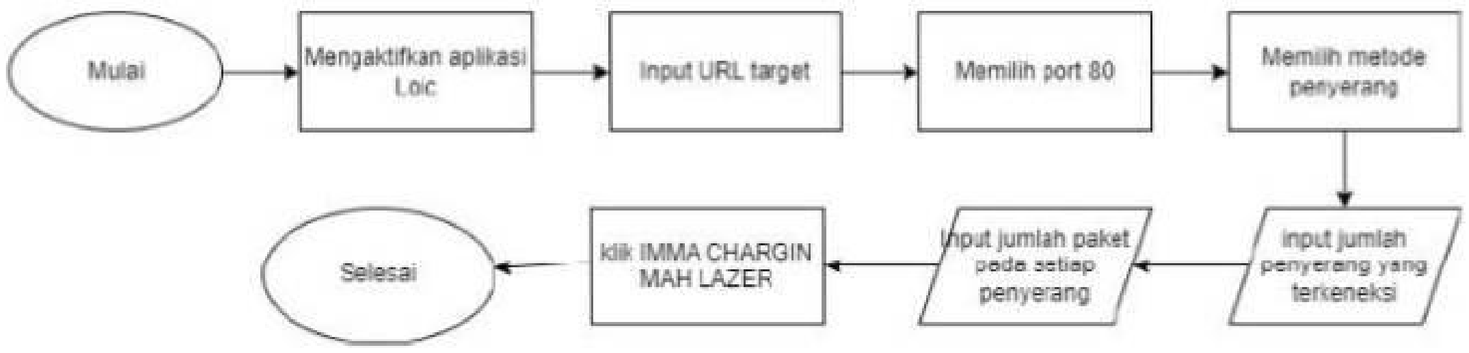
3.2.5 SKENARIO PENGUJIAN SISTEM

Untuk pengujian sistem, dijelaskan cara kerja sistem yang dapat merekam aktivitas penyerang dan memberikan peringatan dan memblokir terdapat serangan.Setiap pengguna dan penyerang memiliki skenario dan alur yang berbeda. Ketika client dan penyerang mengakses server, maka keduamnya akan melewati DMZ yang bertugas untuk merutekakan paket dan juga trafik yang lewat. Setelah itu honeypot akan merekam aktivitas penyerang dan IDPS akan melakukan tugasnya melakukan allow dan block terhadap paket dan trafik yang tidak sesuai dengan signature based.Sehingga IDPS dapat mengupdate rules untuk mendapatkan drop paket yang dilakukan penyerang.

3.2.6 SKENARIO PENGUJIAN SERANGAN

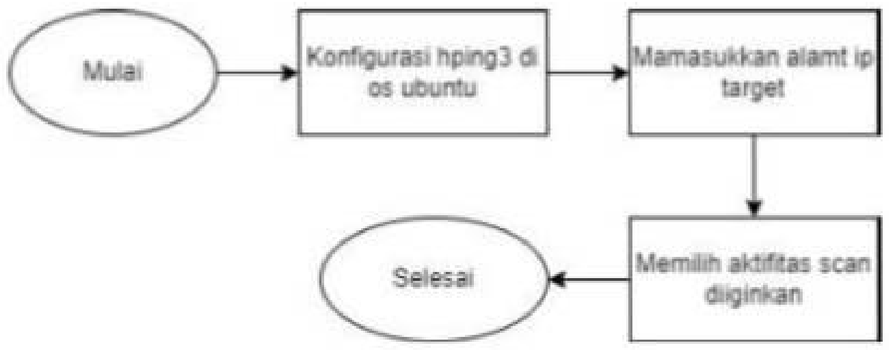
Untuk tahap skenario pengujian serangan terdapat skenario yang dilakukan pada penelitian ini, diantaranya sebagai berikut:

1. Skenario Serangan *Distributed Denial Of Service* (DDoS)



Gambar 3. 13 skrnario pengujian serangan DDoS

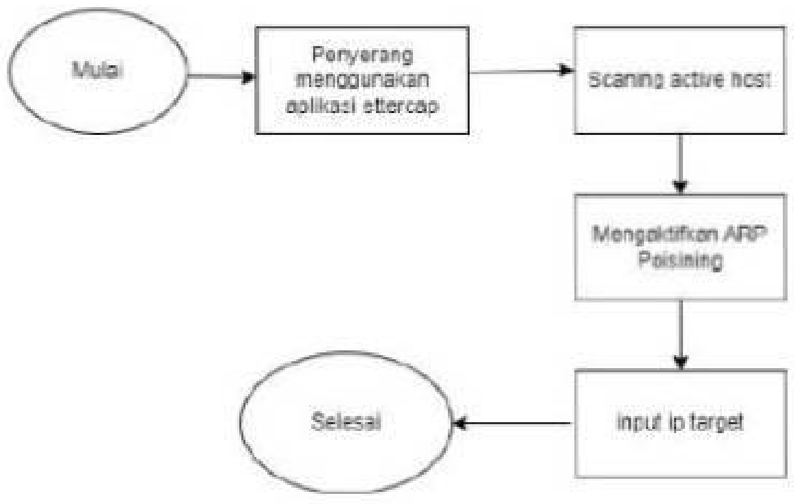
Penyerangan DDoS dilakukan dengan menggunakan 2 tools yaitu LOIC dan Hping3.Untuk serangan LOIC yang pertama dilakukan yaitu mengaktifkan aplikasi LOIC dengan langkah awal memaasukkan IP 192.168.88.254 sebagai target penyerangan.Selanjutnya memilih port 80 lalu memilih metode penyerangan UDP, berikut penyerang menentukan banyaknya user pada kolom threads serta menentukan banyaknya threads pada setiap user. Tahapan Terakhir yaitu memulia serangan dengan mengklik IMMA CHARGIN MAH LAZER.



Gambar 3. 14 Skenario Pengujian Serangan Hping3

Untuk serangan Hping3 yang pertama dilakukan menginstall Hping3 dan menjalankan perintah serangan dengan memberikan perintah #ICMP Flood hping3 -1 -p 80 –flood -d 1450 192.168.88.253 lalu tekan enter dan penyerang akan melakukan serangannya.

2. Skenario Serangan *Man In The Middle* (MiTM)



Gambar 3.15 Skenario Pengujian Serangan MiTM

Serangan MITM ini menggunakan aplikasi Ettercap, diaman fungsi dari ettercap yaitu untuk melakukan snifing packet. Kemudaian melakukan scaning pada host yang aktif dan dilanjutkan memilih target penyerang dan mengaktifkan ARP poisining, selnjutnya penyerang mengimput IP sebagai target.ARP ini yang akan melakukan protokol yang akan bertugas untuk menerjemahkan peralamat dari IP addres menjadi MAC Address.

3.3 TEKNIK PENGUMPULAN DATA

Dalam penelitian ini, teknik pengumpulan data dilakukan dengan melakukan observasi. Observasi yang dilakukan adalah dengan cara melakukan pengujian serangan secara langsung terhadap DDOS dan MiTM. Dari hasil pengujian serangan tersebut, data yang dikumpulkan antara lain seperti akurasi dan deteksi pencegahan yang diperoleh dari log pada setiap tools. Berdasarkan skenario pengujian, serta penggunaan resource pada komputer server. Pengumpulan data dihasilkan dari 10 kali percobaan dengan setiap percobaan selama 1 menit pada tools SNORT dan *honeypot cowrie*.

3.4 ANALISIS DATA

Dalam penelitian ini, penulis membuat analisis menggunakan metode (QOS) *Quality Of Service* untuk setiap pengujian seistem dari serangan DDoS dan MiTM. Implementasi QoS membantu memastikan bahwa pengambilan data Snort dan Honeypot terfokus pada serangan yang sedang berlangsung dan memungkinkan pemantauan yang efektif tanpa terganggu oleh lalu lintas normal atau lalu lintas yang tidak relevan.Kualitas jaringan internet dapat ditentukan berdasarkan nilai QOS sesuai yang ditetapkan oleh TIPHON. *Telecommunications and Internet Protocol Over Networks* (TIPHON) merupakan sebuah standarisasi yang dikeluarkan oleh *European Telecommunication Standards Institute* (ETSI) yang dijadikan sebagai standar untuk penilaian *Quality Of Service*. Dimana dalam pengukuranya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut [23]. Dengan memberikan prioritas dan mengelola alokasi sumber daya jaringan, QoS memainkan peran penting dalam

memfasilitasi analisis dan pengambilan data yang akurat dalam skenario serangan DDoS dan MITM dengan menggunakan aplikasi Wireshark. Dalam Metode pengambilan data snort dan honeypot cowrie dapat diukur menggunakan parameter yaitu throughput, delay, jitter, packet loss dan packet delivery ratio.

1. Throughput

Throughput adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

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

Tabel 3.2 Standar Kualitas *Throughput*

2. Delay

Delay adalah waktu tunda atau waktu penundaan yang terjadi saat data dikirim dari sumber ke tujuan melalui jaringan. Pengukuran *Delay* berdasarkan nilai QOS sesuai yang ditetapkan TIPHON. yang dikeluarkan oleh *European Telecommunication Standards Institute* (ETSI)

Kategori Latency	Nilai Delay (ms)	Indeks
Sangat baik	<150	4
Baik	<250	3
Cukup Baik	<350	2
Buruk	<450	1

Tabel 3.3 Standar Quality Delay

3. Jitter

Pengukuran *Jitter* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) yang dikeluarkan oleh *European Telecommunication Standards Institute* (ETSI)Dimana dalam pengukuranya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut.

Kategori Jitter	Nilai Jitter (ms)	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

Tabel 3.4 Standar Kualitas *Jitter*

4. Packet Loss

Pengukuran *Packet Loss* berdasarkan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) yang dikeluarkan oleh *European Telecommunication Standards Institute* (ETSI).Dimana dalam pengukuranya terdapat beberapa kategori untuk menentukan kualitas jaringan tersebut.

Kategori Degredasi	Nilai Packet Loss (%)	Indeks
Sangat baik	0-2%	4
Baik	3-14%	3
Cukup Baik	15-24%	2
Buruk	>25%	1

Tabel 3.5 Standar Kualitas *Packet Loss*