BAB IV
ANALISIS DAN PERANCANGAN

Pada bab ini, peneliti akan menguraikan analisis dan perancangan yang dibutuhkan. Berikut dijelaska analisis kebutuhan sistem dan perancangan sistem dengan lebih lengkap.

4.1 Analisis Kebutuhan System

4.1.1 Analisis Kebutuhan System

Dalam melakukan penelitian ini diperlukan *hardware* dengan metode virtualisasi sebagai berikut :

1. Satu buah Raspberry PI untuk sebagai IDS, dengan spesifikasi :
   Processor : Raspberry PI 3
   RAM : 256 MB
   Hardisk : 16 GB
   Network Adapter : 1 buah
2. Satu buah komputer sebagai attacker, dengan spesifikasi :
   Processor : Core i7
   RAM : 16 GB
   Hardisk : 8 GB
   Network Adapter : 1 buah

4.1.2 Analisis Kebutuhan Software

Software – software yang diperlukan dalam penelitian ini adalah sebagai berikut :

Sistem Operasi :

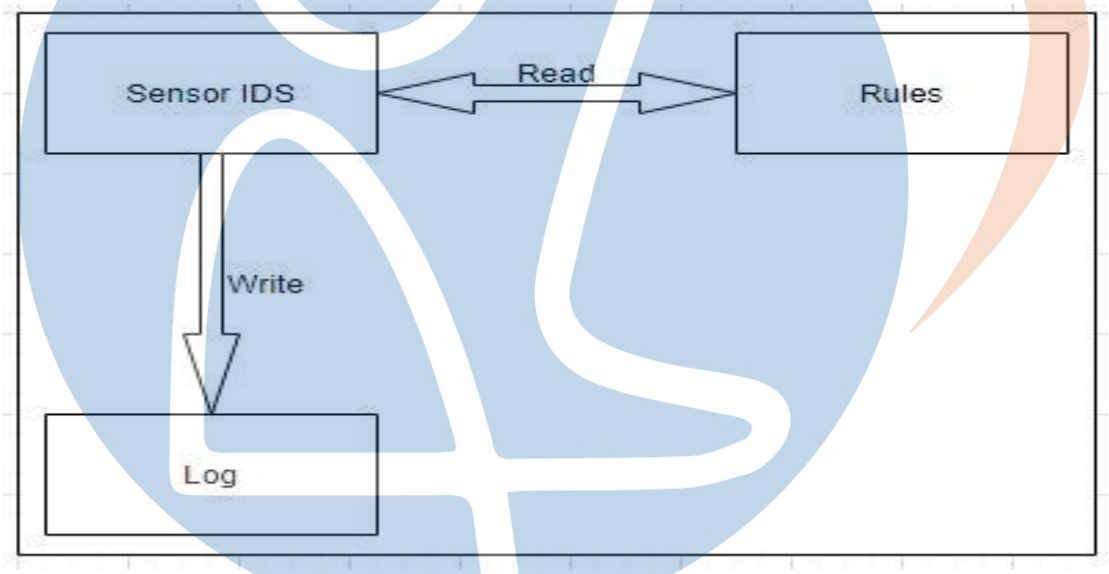
IDS : Ubuntu Server Versi 20.04
Attacker : Ubuntu Versi 20.04
Perangkat Lunak
IDS
Suricata Versi : 6.0.6

Snort Versi	: 2.9.7.0
Fail2ban Versi	: 0.11.1-1
Attacker	: Nmap, DDoS, Brute Force

4.2 Perancangan System

4.2.1 Perancangan Arsitektur System

Arsitektur sistem yang akan dibangun dapat dilihat pada gambar berikut ini.

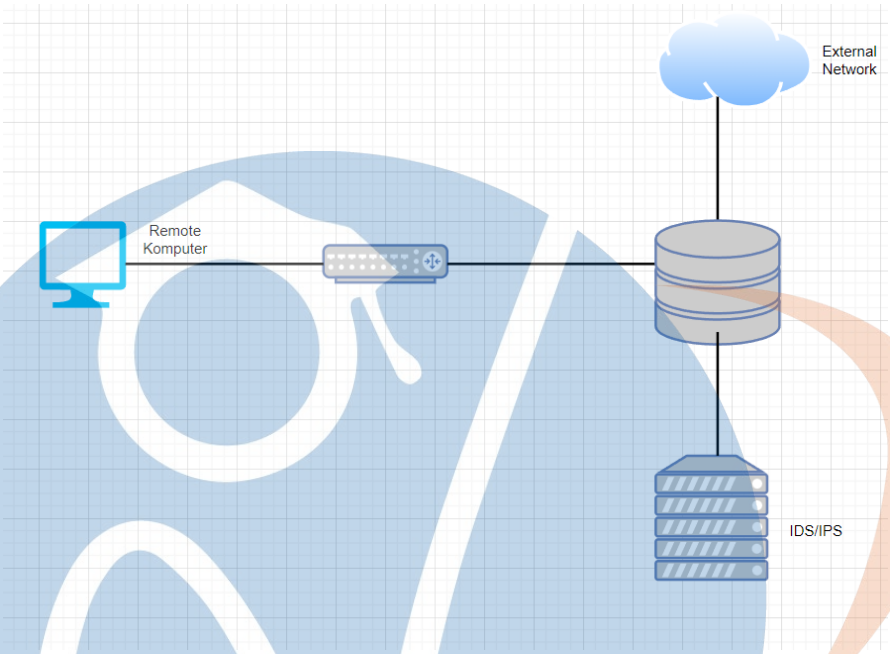


Gambar 13 Perancangan Arsitektur System

Sesuai rancangan Arsitektur Sistem Sensor IDS akan membaca Rules yang berisikan sejumlah pola serangan yang telah ditentukan sesuai dengan traffic ancaman. Pada IDS yang membaca aturan pola pada rules yang menjadi pedoman untuk mendeteksi dan menganalisa lalu lintas jaringan apakah terdapat sebuah serangan atau tidak. Ketika terjadi serangan IDS akan mencatatnya didalam log.

4.2.2 Perancangan Topologi Jaringan

Topologi jaringan yang digunakan pada penilitian ini dapat dilihat pada gambar berikut ini.

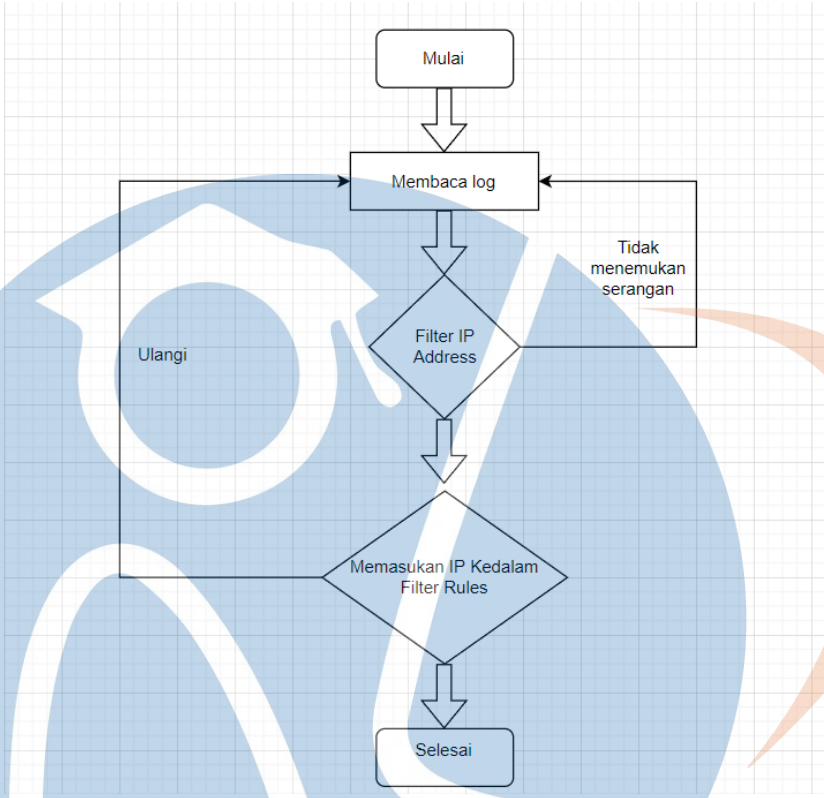


Gambar 14 Rancangan Topologi jaringan

Pada gambar diatas Remote Komputer, Remote Komputer menggunakan alamat IP 192.168.1.109 dengan subnet 255.255.255.0 pada enp0s3. IDS menggunakan alamat IP 192.168.1.120 dengan subnet 255.255.255.0 pada eth0 dan dengan menggunakan bridge ethernet. Perintah PING dilakukan antar computer untuk mengetahui jaringan sudah terhubung.

Komputer yang bertindak sebagai IDS akan akan *verifikasi traffic* lalu lintas data yang mengakses kedalam jaringan server dan apabila ditemukan traffic yang sesuai dengan *rules*(pola *traffic*) yang berada didalam IDS maka akan langsung terbaca oleh IDS dan diteruskan ke USER bahwa *traffic* yang tidak sesuai.

4.2.3 **P**erancangan Script Trigger Firewall



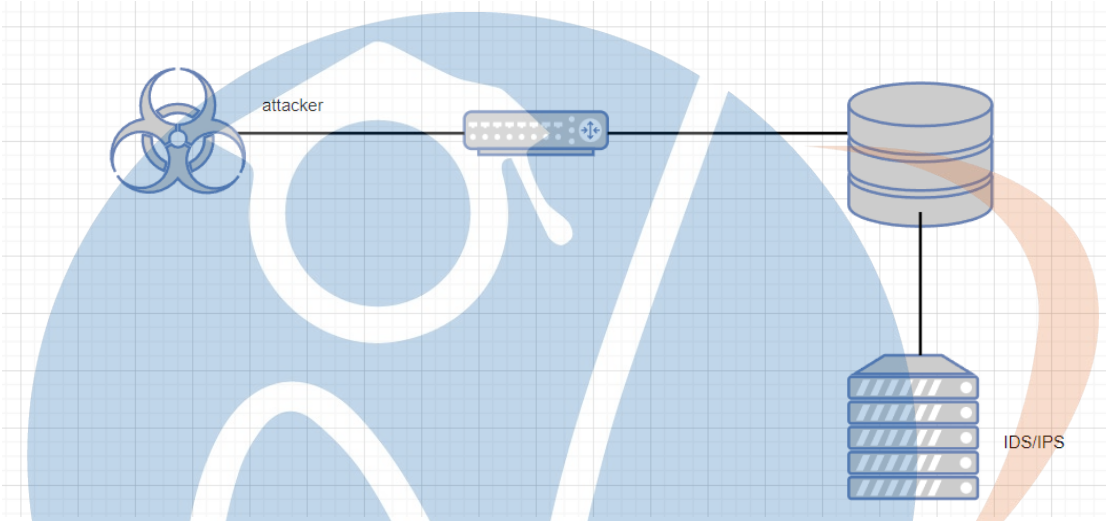
Gambar 15 Scrip Trigger Firewall

Program diatas ini digunakan untuk *trigger firewall*, jadi setiap serangan yang dideteksi oleh IDS akan masuk kedalam log yang ada didalam IDS(*fast.log*). Program akan membaca log tersebut dan membandingkan dengan daftar *IP Address* yang ada didalam program, apakah *IP Address* tersebut sama dengan daftar *IP Address* tersebut, jika sama program akan memulai membaca program kembali dan apabila berbeda maka program akan memasukan *IP Address* penyerang yang nantinya program akan melakukan trigger kepada computer untuk memasukan *IP Address* tersebut kedalam *Filter Rules* yang berada di *Firewall*.

4.3 Skenario Pengujian System

Skenario pengujian yang akan dibagi menjadi tiga skenario.

Topologi dan Skenario pengujian yang akan dijalankan adalah sebagai berikut;



Gambar 16 Skenario Pengujian System

1. Skenario Pertama

   Seorang *attacker* melakukan serangan menggunakan *Scanning port* dengan menggunakan *tools nmap* yang bertujuan untuk menetukan port yang terbuka, *sistem operasi* yang digunakan dan mengetahui alamat *mac address* dari target sisi *attacker* melakukan *scanning port* menggunakan *tools nmap* dengan perintah berikut:

   # nmap -A 192.168.1.120

   # nmap -sS -p- 192.168.1.120

2. Skenario kedua

   Seorang *attacker* melakukan serangan menggunakan *Distribute of service (DOS)* dengan menggunakan *tools hping3* yang bertujuan untuk menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai computer tersebut tidak dapat

menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut dengan cara membanjiri lalu lintas jaringan dengan banyak data. Dari sisi *attacker* melakukan DOS yang bertujuan untuk membanjiri lalu lintas data sehingga layanan server tidak dapat berjalan dengan perintah berikut:

```
#    hping3
hping3> hping3 -S -p 22 --flood --rand-source 192.168.1.120
```

3. Skenario ketiga

   Seorang *attacker* melakukan serangan menggunakan *Brute Force* dengan menggunakan tools *hydra* yang bertujuan untuk mendapatkan sebuah username dan password yang dimiliki oleh komputer tersebut sampai *attacker* ini mendapatkan username dan password komputer dengan menjalankan perintah berikut :

   ```
   # hydra -L user.txt -P pass.txt 192.168.1.120 -t 4 ssh -V
   ```