



# Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System (IDS)* Untuk Mendeteksi Serangan *Distributed Denial Of Service (DDOS)*

**Raihan Fauzi<sup>1</sup>, Yusuf Muhyidin<sup>2</sup>, Dayan Singasatia<sup>3</sup>**

<sup>1,2,3</sup>Teknik Informatika<sup>1</sup> STT Wastukencana Purwakarta, Indonesia

e-mail: [fauziraihan2000@gmail.com](mailto:fauziraihan2000@gmail.com)<sup>1</sup>, [yusufmuhyidin@wastukencana.ac.id](mailto:yusufmuhyidin@wastukencana.ac.id)<sup>2</sup>, [dayan@wastukencana.ac.id](mailto:dayan@wastukencana.ac.id)<sup>3</sup>

## **Abstract**

*Madrasah Aliyah Purwakarta State. is a public high school located in the Purwakarta Regency, Purwakarta District, all activities at this school have used computer networks to support the activities in this school. Madrasah Aliyah Purwakarta State. at this time it has not implemented a computer network security system, because there is no computer network security system implemented at Madrasah Aliyah Negeri Purwakarta, it is still vulnerable to attacks including Ping Attack, Network Scanning and DDOS. Network Development Lyfe Cycle (NDLC) is a method for planning and managing the process of developing a computer network, the NDLC method has 5 stages, namely analysis, design, simulation prototyping, implementation, monitoring, and management. Madrasah Aliyah Purwakarta State. The result of this research is a computer network security system design based on Intrusion Detection System (IDS) using snort and portsentry to detect an attack that enters the computer network of Madrasah Aliyah Negeri Purwakarta such as Ping icmp, nmap (port scan) and DDOS, with get a notification of an attack that enters the computer network, the attack can be prevented by implementing portsentry so that attacks such as Ping icmp, nmap and DDOS will not be able to enter the computer network.*

**Keywords:** Network Security, Intrusion Detection System (IDS), Snort, Portsentry, DDOS

## **Abstrak**

*A Madrasah Aliyah Negeri Purwakarta. adalah sekolah menengah atas negeri yang berada di wilayah Kabupaten Purwakarta Kecamatan Purwakarta, semua aktivitas disekolah ini sudah menggunakan jaringan komputer untuk mendukung sarana kegiatan yang ada disekolah ini. sehingga jaringan komputer menjadi kebutuhan utama di Madrasah Aliyah Negeri Purwakarta dalam menjalankan segala aktivitasnya, jaringan komputer di Madrasah Aliyah Negeri Purwakarta. pada saat ini belum menerapkan system keamanan jaringan komputer, karena tidak adanya system keamanan jaringan komputer yang diterapkan di Madrasah Aliyah Negeri Purwakarta, masih rentan terkena serangan diantaranya Ping Attack, Network Scanning dan DDOS. Network Development Lyfe Cycle (NDLC) merupakan metode untuk merencanakan dan dan mengelola proses pengembangan jaringan komputer, metode NDLC memiliki 5 tahapan yaitu analysis, design, simulation prototyping, implementation, monitoring, dan management, untuk melakukan pengembangan jaringan komputer peneliti melakukan observasi dan wawancara di Madrasah Aliyah Negeri Purwakarta. Hasil dari penelitian ini adalah suatu rancangan system keamanan jaringan komputer berbasis Intrusion Detection System (IDS) menggunakan snort dan portsentry untuk mendeteksi adanya sebuah serangan yang masuk ke dalam jaringan komputer Madrasah Aliyah Negeri Purwakarta seperti Ping icmp, nmap (port scan) dan DDOS, dengan mendapatkan sebuah notifikasi serangan yang masuk ke jaringan komputerm, serangan tersebut dapat dicegah dengan menerapkan portsentry sehingga serangan seperti Ping icmp, nmap dan DDOS tidak akan bisa masuk ke dalam jaringan komputer.*

**Kata kunci:** Keamanan Jaringan Komputer, Intrusion Detection System, Snort, Portsentry DDOS.



## 1. PENDAHULUAN

Teknologi informasi semakin berkembang dengan cepat, teknologi informasi sudah menjadi kebutuhan suatu instansi. Seiring perkembangan jaringan peningkatan layanan yang cepat dan efisien harus selalu diperhatikan, dengan jaringan terstruktur dapat mempermudah dalam melakukan pengaksesan dan perawatan jaringan. Oleh karena itu, perancangan suatu jaringan komputer terkadang tidak sesuai dengan perancangan awal ataupun perancangan yang asal terhubung ke internet yaitu penggunaan *switch unmanageable* akan menyebabkan menurunnya performa dan tingkat keamanan suatu jaringan [1]. Madrasah Aliyah Negeri Purwakarta adalah sekolah menengah atas negeri yang berada di wilayah Kabupaten Purwakarta Kecamatan Purwakarta, semua aktivitas di sekolah ini sudah menggunakan jaringan komputer untuk mendukung sarana kegiatan yang ada di sekolah ini. Sehingga jaringan komputer menjadi kebutuhan utama di Madrasah Aliyah Negeri Purwakarta dalam menjalankan segala aktivitasnya, jaringan komputer di Madrasah Aliyah Negeri Purwakarta, pada saat ini belum menerapkan keamanan jaringan komputer, karena tidak adanya teknik *system* keamanan jaringan komputer yang diterapkan di Madrasah Aliyah Negeri Purwakarta, masih rentan terkena serangan diantaranya *Ping Attack*, *Network Scanning* dan *Distributed Denial Of Service (DDOS)*. *Intrusion Detection System (IDS)* merupakan sebuah sistem yang digunakan sebagai pendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Intrusion tersebut berupa, *Ping Flood*, *Port Scan*, Serangan *Dos/DDOS* dan akses yang tidak dikenal oleh router [2]. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer [3]

## 2. METODOLOGI PENELITIAN

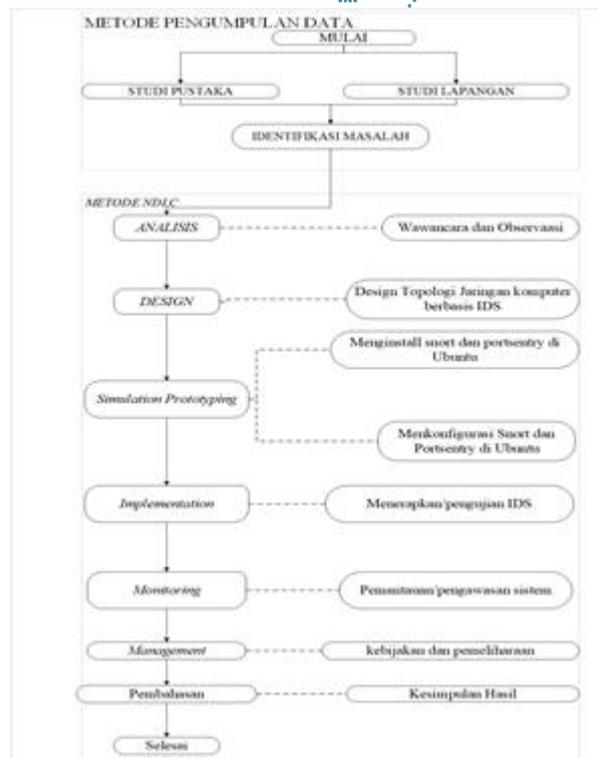
*DDOS attack* merupakan sebuah metode serangan dengan mengirimkan banyak paket ke dalam sebuah jaringan yang menyebabkan perangkat jaringan tidak lagi berjalan sesuai fungsinya dan dibutuhkan sebuah metode untuk mendeteksi kejadian di server secara *real-time* agar dapat dianalisa dan menjadi dasar sebagai alat bukti yaitu dengan menggunakan *Intrusion Detection System (IDS)* [4].

*Snort* adalah teknologi deteksi intursi dan pencegahan open *source*. *Snort* dapat melakukan analisis paket *real-time* dan *logging* di jaringan, analisis protocol dan pencarian konten atau pencocokan adalah fitur yang paling kuat yaitu yang bisa digunakan untuk mendeteksi berbagai serangan *buffer overflow*, *stealth port scan*, *probe smb*, *footprinting*, *DOS* dan *DDOS* [5].

*Portsenry* merupakan sebuah sistem yang diimplementasikan untuk mendeteksi aktivitas serangan oleh *attacker* pada suatu komputer, *portsentry* juga dapat melakukan pencegahan atau memblokir akses terhadap *port* komputer *host* atau server [6].

*Network Development Lyfe Cycle (NDLC)* merupakan metode untuk mengembangkan atau merancang *system* jaringan komputer dan memungkinkan pemantauan terhadap *system* yang sedang dirancang atau dikembangkan agar

dapat diketahui kinerjanya. NDLC juga merupakan metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi Analisa pendistribusian data [7].



**Gambar 1.** Alur Penelitian

## 2.1. Analisis

Pada tahap analisis ini penulis melakukan penelitian di Madrasah Aliyah Negeri Purwakarta. untuk mencari sebuah informasi pada *jaringan komputer* dengan cara melakukan wawancara, survey dan identifikasi masalah terhadap jaringan komputer sekolah Madrasah Aliyah Negeri Purwakarta.

### a) Wawancara

Dengan mencari informasi yang berkaitan dengan pembahasan secara langsung kepada pihak yang berkaitan dengan yang memegang server jaringan MAN Purwakarta mengajukan beberapa pertanyaan yang berkaitan dengan laporan penulisan, serta menghasilkan sebuah percakapan yang dapat memberikan atau menghasilkan informasi.

### b) Studi Pustaka

Studi Pustaka yang dilakukan pada penelitian ini adalah mengumpulkan teori, atau literatur yang relevan mengenai penelitian. Teori teori yang didapat berasal dari jurnal, buku, artikel, website ataupun penelitian sebelumnya yang pernah dilakukan.

c) Identifikasi Masalah

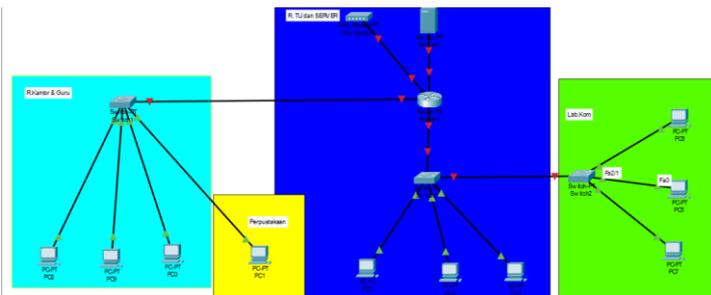
Pada tahap ini peneliti melakukan identifikasi masalah terhadap jaringan komputer MAN Purwakarta dengan bantuan *software kali linux*, dalam identifikasi masalah peneliti melakukan percobaan serangan dengan *ping icmp*, *nmap* (port scan), dan *DDOS*, pada saat melakukan serangan ini berhasil masuk tidak ada *alert* terhadap server, sehingga jaringan komputer masih rentan terhadap serangan *ping icmp*, *nmap* (port scan) dan *DDOS*.

2.2. Design

Pada tahap *Design* ini penulis melakukan penelitian terhadap topologi jaringan komputer yang sudah ada di sekolah Madrasah Aliyah Negeri Purwakarta., untuk membangun *system* keamanan jaringan komputer berbasis *Intrusion Detetction System (IDS)*.

a) Topologi Awal

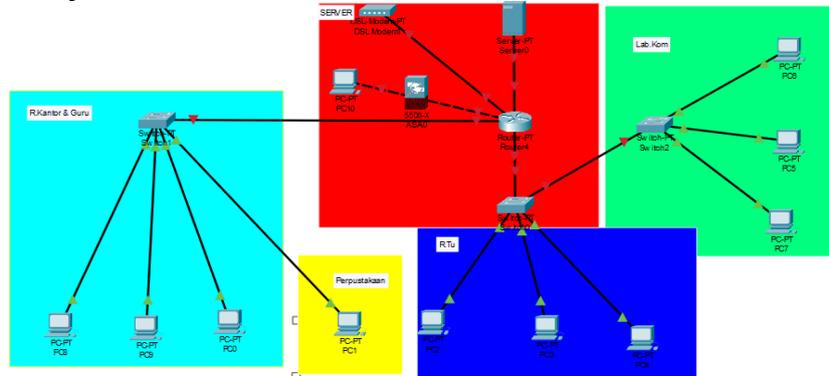
Pada *design* topologi awal ini sistem keamanan jaringan komputer di Madrasah Aliyah Negeri Purwakarta belum menerapkan sistem keamanan jaringan komputer berbasis *IDS*.



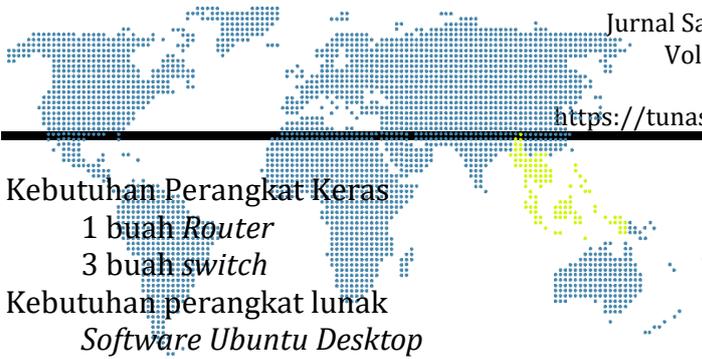
Gambar 2. Topologi awal

b) Topologi Usulan

Pada design usulan topologi jaringan komputer ini penulis mengusulkan penerapan sistem keamanan jaringan komputer dengan berbasis *IDS (Intrusion Detection System)*.



Gambar 3. Topologi usulan



Kebutuhan Perangkat Keras

1 buah *Router*

3 buah *switch*

Kebutuhan perangkat lunak

*Software Ubuntu Desktop*

### 2.3. Simulation Prototyping

Pada tahap *Simulation Prototyping* ini penulis membangun *system* keamanan jaringan komputer berbasis teknik IDS untuk sekolah Madrasah Aliyah Negeri Purwakarta.

#### 2.3.1. Install *Snort*

- a) `apt install snort -y`
- b) `cd /etc/snort/rules`
- c) `nano local.rules` (Masukan Rules konfigurasi *snort*)  
-Ping icmp  
`alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Ada yang Ping"; sid:1000001; rev:1;)`

Nmap (port scan)

`alert tcp any any -> $HOME_NET 21 (msg:"Ada Yang Scanning"; sid:60001; rev:1;)`

`alert tcp any any -> $HOME_NET 22 (msg:"Ada Yang Scanning"; sid:60002; rev:1;)`

DDOS Hping3 dan Loic

`alert tcp any any -> $HOME_NET any (msg:Ada Serangan DDOS; dsize:>1000; sid:10;)`

`alert tcp any any -> $HOME_NET 80 (flags:S; msg:"Ada Serangan DDOS Type:SYN flood"; flow:stateless; sid:3; detection_filter:track by_dst, count 20,seconds 10;)`

- d) `snort -T -c /etc/snort/snort.conf`
- e) `snort -A console -c /etc/snort/snort.conf`

#### 2.3.2. Install *Portsentry*

- a. `apt install portsentry`
- b. `nano /etc/portsentry/portsentry.conf`
  - 1) Ubah Block Tcp&Udp jadi "1"
  - 2) Iptables support for linux`#Kill Route="/sbin/iptables/ -I input -s $TARGETS$ -j DROP" (hapus tanda pagar)`
- c. `service portsentry restart`
- d. `tail -f /var/log/syslog`



## 2.4. Implementation

Pada tahap implementasi penulis melakukan penerapan atau pengujian terhadap *system* keamanan jaringan komputer berbasis IDS untuk sekolah Madrasah Aliyah Negeri Purwakarta, dengan melakukan pengujian atau pengetesan *system* keamanan jaringan komputer berbasis IDS dengan bantuan *Virtual Machine* dan *software Ubuntu Desktop* dan *Kali Linux* dalam simulasi penerapan *system* keamanan jaringan komputer berbasis IDS untuk Madrasah Aliyah Negeri Purwakarta.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Snort

#### a) Ping ICMP

Percobaan serangan dengan melakukan *ping icmp* di kali linux untuk memastikan penyerang dan target serangan bisa saling berkomunikasi.

```
root@rehan: /home/rehan/Downloads
File Actions Edit View Help
root@rehan) - [~/home/rehan/Downloads]
# ping 192.168.43.79
PING 192.168.43.79 (192.168.43.79) 56(84) bytes of data.
64 bytes from 192.168.43.79: icmp_seq=1 ttl=64 time=0.334 ms
64 bytes from 192.168.43.79: icmp_seq=2 ttl=64 time=0.355 ms
64 bytes from 192.168.43.79: icmp_seq=3 ttl=64 time=0.197 ms
64 bytes from 192.168.43.79: icmp_seq=4 ttl=64 time=0.204 ms
64 bytes from 192.168.43.79: icmp_seq=5 ttl=64 time=0.390 ms
64 bytes from 192.168.43.79: icmp_seq=6 ttl=64 time=0.297 ms
64 bytes from 192.168.43.79: icmp_seq=7 ttl=64 time=0.422 ms
64 bytes from 192.168.43.79: icmp_seq=8 ttl=64 time=0.362 ms
64 bytes from 192.168.43.79: icmp_seq=9 ttl=64 time=0.401 ms
```

Gambar 4. Ping ICMP

Pada gambar penyerang melakukan percobaan serangan dapat dilihat ip target 192.168.43.79 dimana penyerang dapat berkomunikasi atau terhubung dengan target setelah melakukan *ping icmp* yang terus *mereply*. Komputer yang sudah diterapkan *Intrusion Detection System (IDS)* di *Ubuntu Desktop* akan mendeteksi adanya percobaan serangan yang akan masuk ke dalam jaringan komputer.

```
07/13-10:24:53.988002 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:53.988002 ** [1:384:5] ICMP PING [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:53.988018 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:54.930553 ** [1:408:5] ICMP Echo Reply [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:54.930553 ** [1:366:7] ICMP PING MIX [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:54.930553 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:54.930553 ** [1:384:5] ICMP PING [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:54.930570 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:54.930570 ** [1:408:5] ICMP Echo Reply [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:55.954424 ** [1:366:7] ICMP PING MIX [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:55.954424 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:55.954424 ** [1:384:5] ICMP PING [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:55.954441 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:55.954441 ** [1:408:5] ICMP Echo Reply [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:56.977757 ** [1:366:7] ICMP PING MIX [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:56.977757 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:56.977757 ** [1:384:5] ICMP PING [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:56.977773 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:56.977773 ** [1:408:5] ICMP Echo Reply [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:24:58.001377 ** [1:366:7] ICMP PING MIX [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:58.001377 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:58.001377 ** [1:384:5] ICMP PING [**] [Classification: Msc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:24:58.001394 ** [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
```

Gambar 5. Snort dapat mendeteksi serangan

Pada gambar diatas IDS dengan *snort* sudah diterapkan, *snort* dapat mendeteksi serangan dan memberitahu administrator jaringan dengan adanya *alert* serangan yang masuk berupa waktu, jenis serangan dan ip penyerang.

### b) Nmap (Port Scanning)

Pada Percobaan selanjutnya akan melakukan scanning terhadap jaringan komputer target.

```
rehan@rehan:~/Downloads$ nmap -Pn 192.168.43.79
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 00:28 EDT
NSE: loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 00:28
Scanning 192.168.43.79 [1 port]
Completed ARP Ping Scan at 00:28, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:28
Completed Parallel DNS resolution of 1 host. at 00:28, 0.00s elapsed
Initiating SYN Stealth Scan at 00:28
Scanning rehan-VirtualBox (192.168.43.79) [1000 ports]
Discovered open port 80/tcp on 192.168.43.79
Completed SYN Stealth Scan at 00:28, 0.06s elapsed (1000 total ports)
Initiating Service scan at 00:28
Scanning 1 service on rehan-VirtualBox (192.168.43.79)
Completed Service scan at 00:28, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.43.79.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Nmap scan report for rehan-VirtualBox (192.168.43.79)
Host is up, received arp-response (0.00016s latency).
Scanned at 2022-07-13 00:28:42 EDT for 65
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:07:21:28 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
```

Gambar 6. Scanning terhadap jaringan komputer target

Pada gambar penyerang berhasil melakukan nmap (port scanning) terhadap jaringan komputer dengan nip target 192.168.43.79.

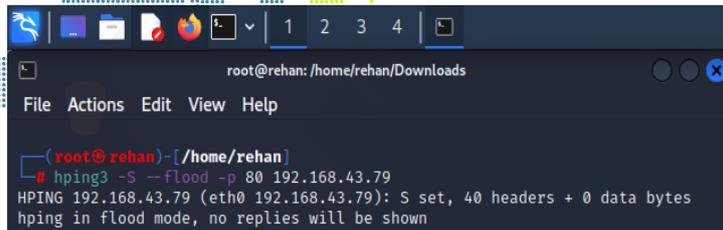
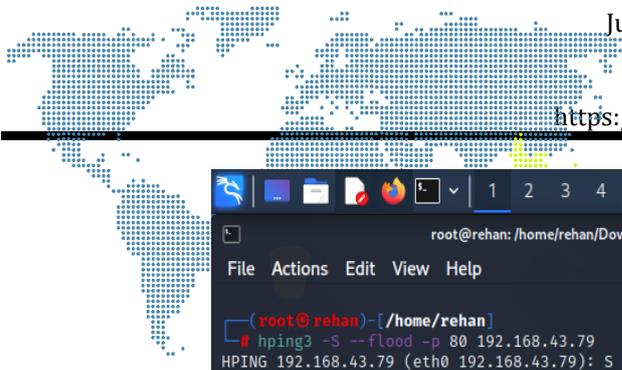
```
07/13-10:28:02.876884 [**] [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:28:02.876884 [**] [1:499:4] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:28:03.899473 [**] [1:480:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:03.899473 [**] [1:366:7] ICMP PING 'NIX [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:03.899473 [**] [1:480:5] ICMP PING speedera [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:03.899473 [**] [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:03.899473 [**] [1:499:4] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:28:03.899473 [**] [1:480:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:28:04.923261 [**] [1:366:7] ICMP PING 'NIX [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:04.923261 [**] [1:480:5] ICMP PING speedera [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:04.923261 [**] [1:1000001:1] Ada Yang Ping [**] [Priority: 0] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:04.923261 [**] [1:499:4] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:04.923261 [**] [1:366:7] ICMP PING 'NIX [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.226 -> 192.168.43.79
07/13-10:28:04.923261 [**] [1:480:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.43.79 -> 192.168.43.226
07/13-10:28:07.889449 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.43.226 -> 192.168.43.226
07/13-10:28:10.892013 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.43.226 -> 192.168.43.226
07/13-10:28:12.804033 [**] [1:60000:1] Ada Yang Scanning [**] [Priority: 0] [TCP] 192.168.43.226 -> 192.168.43.79:22
07/13-10:28:12.804223 [**] [1:60000:1] Ada Yang Scanning [**] [Priority: 0] [TCP] 192.168.43.226 -> 192.168.43.79:21
07/13-10:28:12.807680 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.43.226 -> 192.168.43.226
07/13-10:28:12.811809 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.43.226 -> 192.168.43.226
```

Gambar 7. nmap (port scanning)

Pada gambar diatas dikomputer yang sudah diterapkan *snort* dapat mendeteksi saat kegiatan nmap (*port scanning*) ke jaringan komputer dengan *alert* waktu, jenis serangan dan ip penyerang

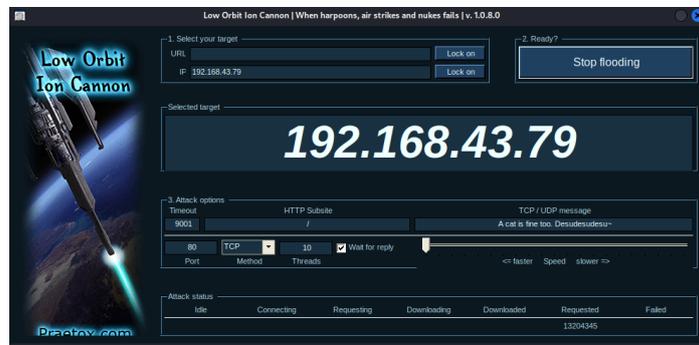
### c) Distributed Denial Of Service (DDOS)

Pada Percobaan selanjutnya akan melakukan serangan dengan DDOS Hping3 dan Loic terhadap target.



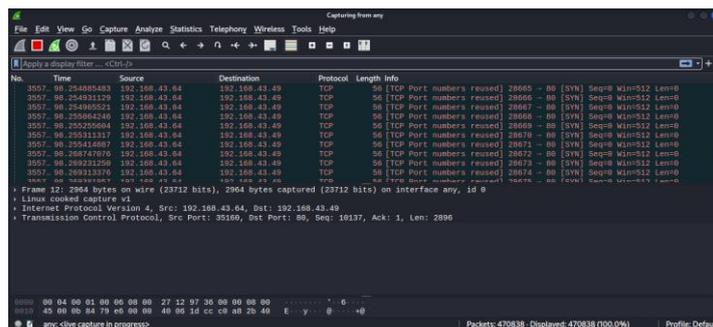
Gambar 8. DDOS Hping3 dan Loic terhadap target

Pada serangan DDOS dengan Hping3 ini -S adalah socket -flood adalah flooding untuk memenuhi *traffic* jaringan target -p port yang akan dituju adalah port 80 dengan ip target 192.168.43.79.



Gambar 9. Serangan DDOS dengan Hping3

Pada serangan DDOS dengan LOIC ini metode tcp untuk memenuhi *traffic* jaringan target -p port yang akan dituju adalah port 80 dan paket yang terkirim 13204345 (Requested) dengan ip target 192.168.43.79.



Gambar 10. Serangan DDOS dengan LOIC

Sebelum portsentry diterapkan di jaringan komputer serangan DDOS masih bisa di lakukan dengan mengirimkan atau membanjiri jaringan komputer dengan pengiriman paket SYN attack yang akan mengakibatkan perlambatan dalam pelayanan. Pada komputer target yang sudah diterapkan IDS akan mencoba untuk mendeteksi serangan yang masuk.



```
root@rehan-VirtualBox: /etc/snort/rules
root@rehan-VirtualBox: /etc/snort/rules
27/13:10:40:47.488227 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 216.239.38.120:443 -> 192.168.43.79:54972
27/13:10:40:47.705080 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 216.239.38.120:443 -> 192.168.43.79:54972
27/13:10:40:47.755314 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 216.239.38.120:443 -> 192.168.43.79:54972
27/13:10:40:47.849989 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:48.060883 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:48.063515 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:48.063515 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:48.147489 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 52.45.252.32:443 -> 192.168.43.79:51326
27/13:10:40:48.193866 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:48.312121 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:49.371283 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 103.145.227.94:443 -> 192.168.43.79:47888
27/13:10:40:50.218864 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:50.260883 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:50.425520 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 74.125.200.95:443 -> 192.168.43.79:52340
27/13:10:40:51.364380 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 216.239.38.120:443 -> 192.168.43.79:54972
27/13:10:40:52.049910 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 216.239.38.120:443 -> 192.168.43.79:54972
27/13:10:40:52.049910 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:52.049913 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:52.090855 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:52.090879 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:52.187919 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
27/13:10:40:53.207158 *** [1:10:0] Ada Serangan DDoS *** [Priority: 0] [TCP] 31.13.95.1443 -> 192.168.43.79:60864
```

Gambar 11. Penerapan snort

Pada gambar dikomputer yang sudah diterangkan *snort* dapat mendeteksi saat ada serangan DDOS Hping3 dan LOIC ke jaringan komputer dengan *alert* waktu,jenis serangan dan ip penyerang.

### 3.2. Portsentry

#### a) Ping Icmp

Selanjutnya akan melakukan percobaan *ping icmp* terhadap target

```
root@rehan: /home/rehan
File Actions Edit View Help
root@rehan) - [~/home/rehan]
# ping 192.168.43.79
PING 192.168.43.79 (192.168.43.79) 56(84) bytes of data:
From 192.168.43.226 icmp_seq=1 Destination Host Unreachable
From 192.168.43.226 icmp_seq=2 Destination Host Unreachable
From 192.168.43.226 icmp_seq=3 Destination Host Unreachable
From 192.168.43.226 icmp_seq=4 Destination Host Unreachable
From 192.168.43.226 icmp_seq=5 Destination Host Unreachable
From 192.168.43.226 icmp_seq=6 Destination Host Unreachable
From 192.168.43.226 icmp_seq=7 Destination Host Unreachable
From 192.168.43.226 icmp_seq=8 Destination Host Unreachable
From 192.168.43.226 icmp_seq=9 Destination Host Unreachable
From 192.168.43.226 icmp_seq=10 Destination Host Unreachable
From 192.168.43.226 icmp_seq=11 Destination Host Unreachable
From 192.168.43.226 icmp_seq=12 Destination Host Unreachable
From 192.168.43.226 icmp_seq=13 Destination Host Unreachable
```

Gambar 12. Ping Icmp

Sesudah *portsentry* diterapkan di jaringan komputer target saat ada *ping icmp* sudah tidak bisa dilakukan dengan pengiriman paket icmp terus menerus dikarenakan sudah diblokir atau ditutup aksesnya oleh *portsentry*.

#### b) Nmap (Port Scanning)

Pada Percobaan selanjutnya akan melakukan scanning terhadap jaringan komputer target.

```
root@rehan: /home/rehan
File Actions Edit View Help
root@rehan) - [~/home/rehan]
# nmap -sS -sV -v -v -Pn 192.168.43.79
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 00:16 EDT
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 00:16
Scanning 192.168.43.79 [1 port]
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 50.00% done; ETC: 00:16 (0:00:01 remaining)
Completed ARP Ping Scan at 00:16, 1.46s elapsed (1 total hosts)
Nmap scan report for 192.168.43.79 [host down, received no-response]
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (0 hosts up) scanned in 1.68 seconds
Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

Gambar 13.Nmap (Port Scanning)



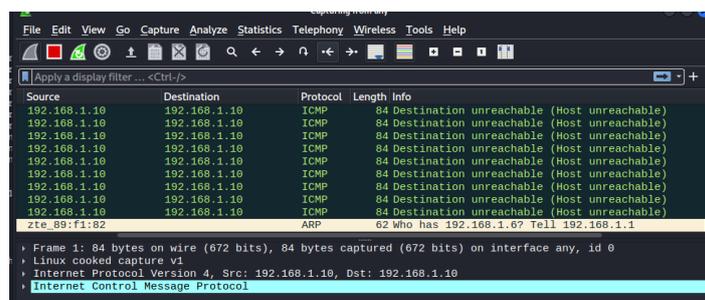
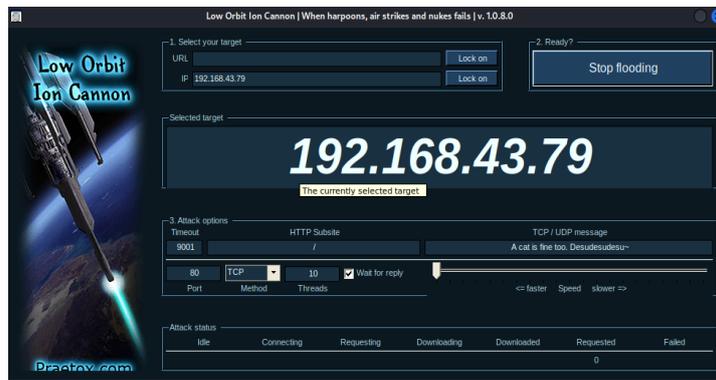
Sesudah *portsentry* diterapkan saat ada aktivitas *nmap* (port scanning) tidak bisa dilakukan karena sudah diblokir secara otomatis oleh *portsentry*, sehingga attacker tidak mendapatkan informasi port yang tersedia.

### c) *Distributed Denial of Service (DDOS)*

Pada Percobaan selanjutnya akan melakukan serangan dengan DDOS Hping3 dan Loic terhadap target.

```
root@rehan: /home/rehan/Downloads
File Actions Edit View Help

(root@rehan) - [ /home/rehan ]
# hping3 -S --flood -p 80 192.168.43.79
HPING 192.168.43.79 (eth0 192.168.43.79): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



Gambar 14. DDOS

Pada gambar serangan DDOS dengan Hping3 dan LOIC sudah tidak bisa masuk terhadap jaringan komputer target dikarena sudah tutup aksesnya oleh *portsentry* dan tidak ada paket yang terkirim.

### 3.3. Monitoring

Pada tahap monitoring ini penulis melakukan pengawasan atau pemantauan terhadap sistem keamanan jaringan komputer berbasis IDS agar sesuai dengan tujuan di awal yaitu untuk bisa mendeteksi adanya serangan seperti *ping*, *nmap* (*Scanning*) dan DDOS.

### 3.4. Management

Pada tahap ini penulis akan melakukan kebijakan dan perawatan *system* keamanan jaringan komputer berbasis IDS sehingga dapat berjalan dengan baik sistem keamanan yang sudah dirancang.

### 3.5. Hasil Grafik Penerapan *Snort*

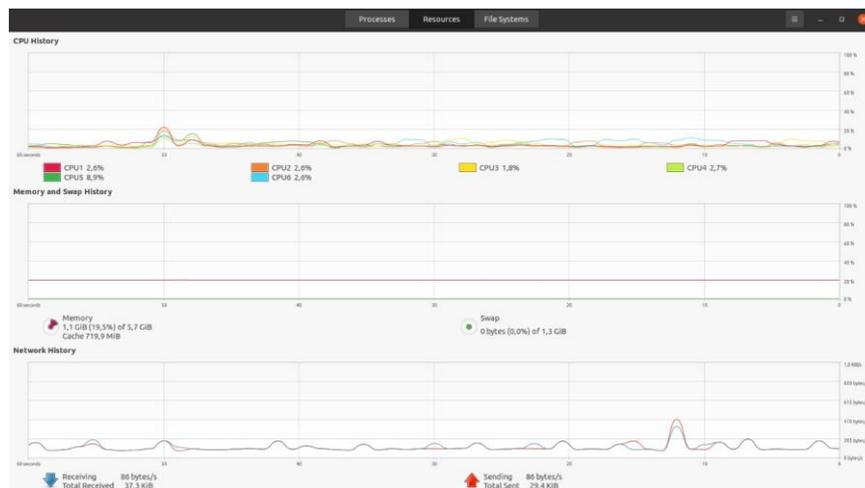
Sebelum *Ping Icmp*



Gambar 15. Sebelum Ping Icmp

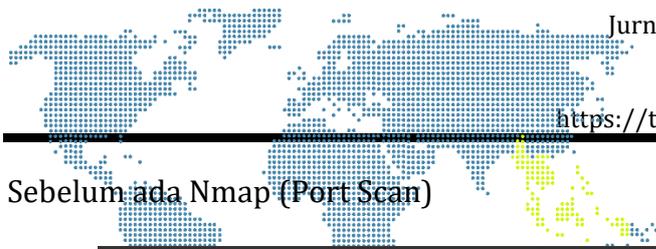
Pada grafik diatas sebelum adanya serangan dengan melakukan *ping attack* grafik *network history* hanya mencapai bytes 205 bytes/s dan pemakaian CPU hanya 20% dan memory 20 %.

Sesudah ada *Ping Icmp*



Gambar 16. Sesudah ada Ping Icmp

Pada grafik serangan dengan *Ping icmp*, pada grafik *network history* dapat dilihat bahwa mengalami kenaikan yang sangat tinggi dalam *traffic* jaringan sampai 418,0 bytes/s, serta untuk pengguna memory naik 20% dan penggunaan Cpu 20%.



### Sebelum ada Nmap (Port Scan)



**Gambar 17.** Sebelum ada Nmap (Port Scan)

Pada grafik diatas sebelum adanya serangan dengan melakukan *ping attack* grafik *network history* hanya mencapai bytes 205,0 bytes/s dan pemakaian CPU hanya 20% dan memory 20 %.

### Sesudah Ada Nmap (Port Scan)



**Gambar 18.** Sesudah ada Nmap (Port Scan)

Pada grafik serangan dengan nmap,pada grafik *network history* dapat dilihat bahwa mengalami kenaikan yang sangat tinggi dalam *traffic* jaringan sampai 48.0 kib/s,serta untuk penggunaan memory naik 40% dan penggunaan Cpu 20%.



Sebelum ada DDOS



Gambar 19. Sebelum ada DDOS

Pada grafik diatas sebelum adanya serangan dengan melakukan *ping attack* grafik *network history* hanya mencapai 205 bytes/s dan pemakaian CPU hanya 20% dan memory 20%.

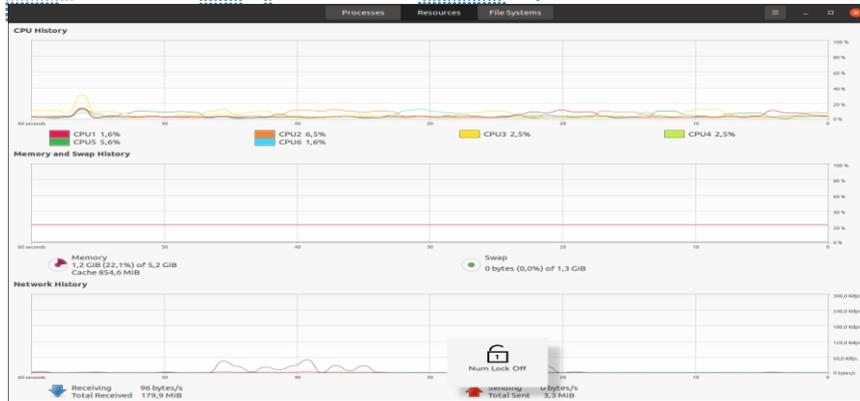
Sesudah ada DDOS



Gambar 19. Sesudah ada DDOS

Pada grafik diatas serangan dengan DDOS Hping3 dan Loic, pada grafik *network history* dapat dilihat bahwa mengalami kenaikan yang sangat tinggi dalam *traffic* jaringan sampai 80.0 MB/s, serta untuk penggunaan memory naik 40% dan penggunaan Cpu 60%.

### 3.6. Hasil Grafik Penerapan *Portsentry* Setelah *Portsentry* diterapkan



**Gambar 20.** Sesudah *Portsentry* diterapkan

Pada grafik penulis telah menerapkan *portsentry* untuk memblokir atau menutup akses serangan yang akan terjadi terhadap jaringan komputer, sehingga penyerang tidak dapat melakukan serangan dengan *ping icmp, nmap* (port scan) dan ddos terhadap jaringan komputer, sehingga jaringan komputer yang diterapkan *portsentry* sudah memblokir atau menutup secara otomatis penyerang saat akan melakukan serangan *ping icmp, nmap* (port scan) dan DDOS.

### 3.7. Tabel Ringkasan Hasil Penerapan IDS *Snort*

a) Sebelum diterapkan IDS *Portsentry*

**Tabel 1.** Ringkasan Hasil Pengujian DDOS dengan (IDS) *Snort*

Pengujian	Sebelum	Sesudah
<i>Ping (ICMP)</i>	205 bytes/s	418 bytes/s
<i>Nmap</i>	205 bytes/s	48,0 Kib/s
DDOS	205 bytes/s	80. Mb/s

Dari hasil penerapan *intrusion Detection System* dengan menggunakan *snort* untuk jaringan komputer, hasil yang didapatkan dari penerapan *snort, snort* hanya mampu mendeteksi adanya serangan seperti *Ping (ICMP), Nmap* dan *DDOS* yang masuk ke dalam jaringan komputer dengan memberikan sebuah *alert* atau informasi bahwa ada serangan yang masuk dengan informasi, tanggal dan waktu, type serangan, *snort* tidak dapat menindak lanjuti penyerang dikarenakan *snort* hanya mendeteksi sebuah serangan yang masuk.

b) Sesudah diterapkan *portsentry*

**Tabel 2.** Ringkasan Hasil Pengujian DDOS dengan *Portsentry*

Pengujian	Sebelum	Sesudah
<i>Ping (ICMP)</i>	418 bytes/s	205 bytes/s
<i>Nmap</i>	48,0 Kib/s	205 bytes/s
DDOS	80,0 Mb/s	205 bytes/s

Dari hasil penerapan *intrusion Detection System* dengan menggunakan *portsentry* untuk jaringan komputer, hasil yang didapatkan dari penerapan *portsentry*, *portsentry* bisa mencegah adanya serangan seperti *Ping (ICMP) Nmap*, dan *DDOS* yang masuk ke dalam jaringan komputer dengan memblokir ip penyerang secara otomatis.

#### 4. SIMPULAN

Berdasarkan hasil pengujian yang dilakukan oleh peneliti dapat disimpulkan bahwa *snort* dapat diimplementasikan sebagai salah satu Teknik keamanan jaringan (*IDS*) pada sistem operasi ubuntu 20.04 LTS untuk mendeteksi serangan berupa *Ping attack*, *nmap (port scanning)* dan *DDOS*, serangan *ping*, *nmap (port scan)* dan *DDOS* yang dilakukan dimana serangan tersebut dapat dicegah dengan menerapkan *portsentry* sehingga serangan seperti *Ping attack*, *nmap* dan *DDOS* tidak akan bisa masuk ke dalam jaringan komputer.

#### DAFTAR PUSTAKA

- [1] P. T. Samudera and I. Rahayu, "" Rancangan Dan Konfigurasi Jaringan Pada," vol. 1, no. 1, pp. 597–603, 2021.
- [2] A. R. Machdi, "Analisa dan Implementasi Sistem Kemananan Jaringan Intrusion Detection System ( IDS ) Berbasis Mikrotik," vol. 1, no. 1, pp. 16–21, 2021.
- [3] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.
- [4] M. Syani, "Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps)," *J. Inkofar*, vol. 1, no. 1, pp. 13–20, 2020, doi: 10.46846/jurnalinkofar.v1i1.155.
- [5] R. S. Putra, R. Mayasari, and N. B. A. Karna, "Implementasi Dan Analisis Keamanan Jaringan Virtual HIPS Snort Pada Layanan Web Server Dengan Penyerangan DOS DAN DDOS," *e-Proceeding Eng.*, vol. 5, no. 3, pp. 4958–4965, 2018.
- [6] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasis Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.
- [7] U. A. Ahmad, R. E. Saputra, and P. Y. Pangestu, "Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optic Dengan Metode Network Development Life Cycle ( Ndlc ) Design Of Computer Network Infrastructure Using Optical Fiber With Network Development Life Cycle (NDLC) Method," vol. 8, no. 6, pp. 12066–12079, 2021.