Penanggulangan Serangan LOIC Terhadap Web Server

Countermeasures for LOIC Attacks Against Web Servers

Molavi Arman[1], Nur Rachmat[2]
[1]Manajemen Informatika, [2]Informatika, Universitas Multi Data Palembang
E-mail: [1]molavi.arman@mdp.ac.id, [2]nur.rachmat@mdp.ac.id

Abstrak

Ketersediaan layanan yang selalu siap secara *realtime* merupakan hal yang selalu diupayakan untuk menunjang kelancaran layanan dalam menggunakan web server sebagai media utama dalam memberikan dan menunjang interface bagi semua kebutuhan pengguna. Kendala utama karena layanan *web server* melalui jalur internet maka sering terjadi kendala teknis yang diakibatkan gangguan serangan DoS LOIC yang melumpuhkan kinerja web server, cpu, dan komponen lainnya yang menguras sumber daya komputer server. Hal seperti ini perlu ditanggulangi sehingga layanan web server tetap tersedia bagi pengguna tanpa kendala. Begitu pula serangan yang menggali informasi dari komputer server seperti aktifitas *port scanning* yang menghasilkan informasi berupa jenis web server, jenis sistem operasi yang digunakan dan informasi penting lainnya. Untuk itu diperlukan upaya penanggulangan dengan menggunakan *firewall iptables* guna meminimalisir gangguan tersebut.

Kata kunci: *DoS, LOIC, Port Scaning, Iptables*

Abstract

The availability of services that are always ready in real-time is something that is always strived to support the smooth running of services in using a web server as the main medium in providing and preparing interfaces for all user needs. The main obstacle is that because web server services go through the internet, technical problems often occur due to interference with DoS LOIC attacks which cripple the performance of web servers, CPUs, and other components that drain server computer resources. Things like this need to be addressed so that web server services are still available to users without problems. Likewise, attacks that dig up information from server computers such as port scanning activities produce information in the form of the type of web server, the type of operating system used, and other important information. For this reason, countermeasures are needed by using an iptables firewall to minimize these disturbances.

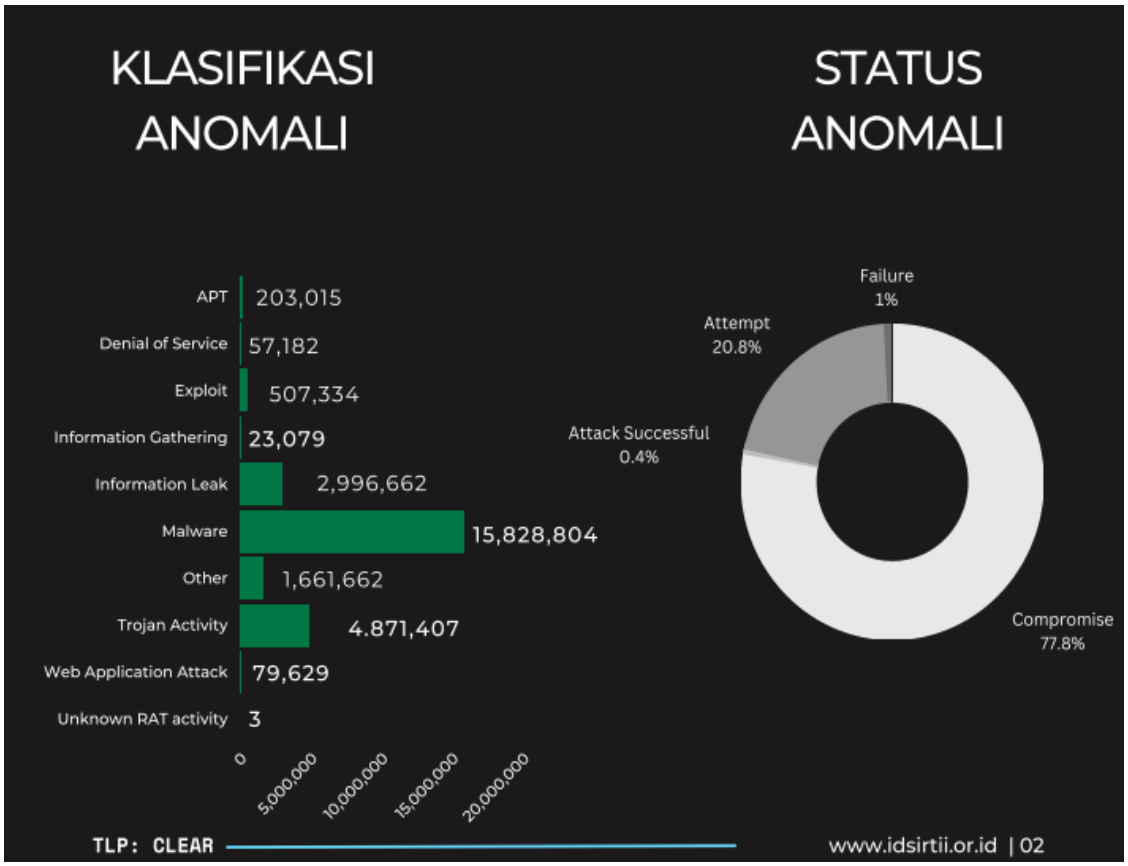
Keywords: DoS, LOIC, Port Scaning, Iptables

1. PENDAHULUAN

Keamanan jaringan menjadi hal yang wajib dipertimbangkan mengingat banyaknya kejadian kebocoran data pada instansi pemerintahan maupun swasta. Untuk melindungi data yang berharga dan informasi yang penting diperlukan perlindungan keamanan jaringan komputer. Teori keamanan data biasanya menggunakan teori kriptografi, integritas dan ketersediaan data, strategi keamanan lainnya serta perlindungan traffic jaringan data itu sendiri. Perlindungan jaringan komputer bisa dimulai dari anti scanning sehingga orang lain tidak berpikir dengan dugaan-dugaan tertentu.

Metode keamanan yang sudah cukup popular seperti IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Firewall, Network Security, Network Security Bases of Knowledge untuk menghambat terjadinya penyerangan atau penyusupan terhadap suatu sistem. Ada banyak cara yang bisa digunakan tergantung kebutuhan.

Berdasarkan informasi yang rilis dari instansi IDSIRTII pada laporan bulan Desember tahun 2022, salah satu jenis serangan siber yaitu Denial of Service yang mencapai 57.182 serangan [1] seperti yang ditampilkan pada gambar 1.



Gambar 1. Grafik Anomali

Pada penelitian [2] membahas evaluasi Snort Intrusion Detection System (IDS) dalam hal kinerja dan deteksi paket data yang diidentifikasi sebagai serangan DoS. Pekerjaan ini menjelaskan aspek yang terlibat dalam membangun sistem keamanan jaringan kampus dan kemudian mengevaluasi risiko dan ancaman keamanan jaringan kampus, terutama menganalisis serangan DoS dan DDoS, dan mengedepankan pendekatan baru untuk solusi keamanan jaringan. Tujuannya adalah untuk menganalisis keunggulan fungsional dari solusi yang diberikan, penyebaran dan konfigurasi *open source* berdasarkan sistem deteksi intrusi Snort. Metrik evaluasi didefinisikan menggunakan Snort yaitu perbandingan antara aturan dasar dengan yang baru, bandwidth yang tersedia, pemuatan CPU dan penggunaan memori.

Dalam penelitian [3] membahas metode pembelajaran machine learning yang dapat mendeteksi paket data yang masuk terinfeksi atau tidak. Algoritma pembelajaran mesin yang digunakan untuk mendeteksi perilaku anomali dari lalu lintas data antara lain Naive Bayes, K-Nearest

eighbor (KNN) dan Support Vector Machine (SVM). Ketiga algoritma ini dibandingkan dan KNN mendapatkan hasil yang lebih baik dalam mendeteksi paket yang terinfeksi daripada dua algoritma lainnya.

Dalam penelitian [4] mengusulkan sistem pertahanan otonom yang menggabungkan tepi komputasi dengan jaringan saraf convolutional neural network (CNN) untuk mengenali apakah server data di IoT mendapat serangan DDoS dan mengidentifikasi mode serangannya. Akurasi

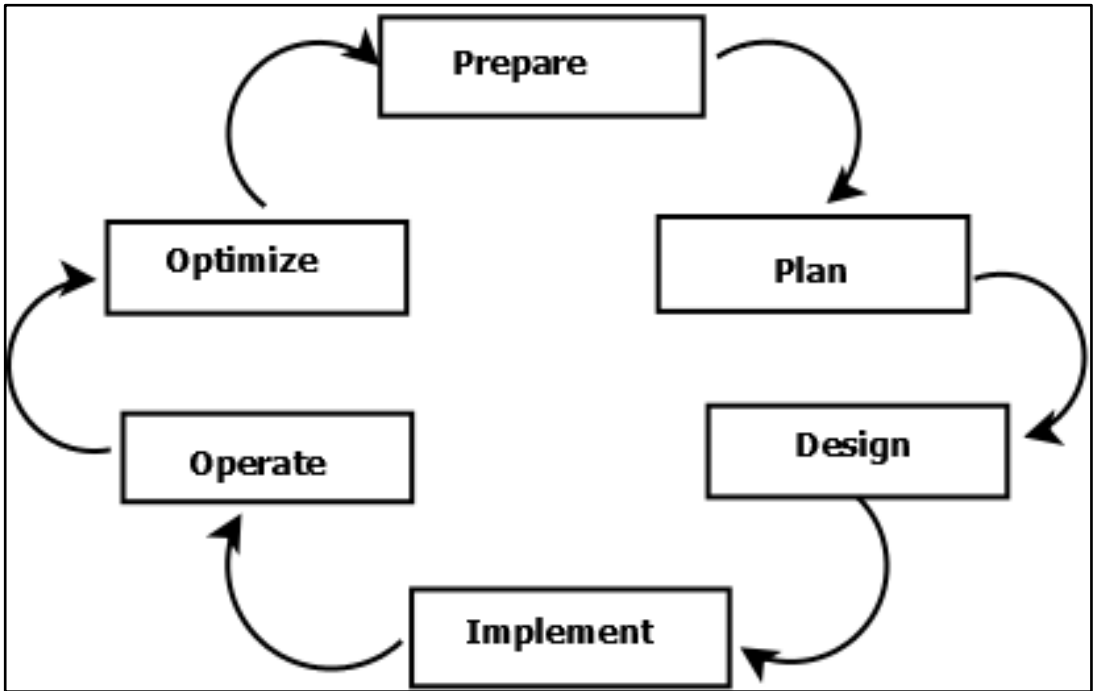
dari CNN terlatih dua dimensi mencapai 99,5% untuk lalu lintas paket dan 99,8% untuk pelatihan fitur paket. Hasil percobaan menunjukkan bahwa server data pada sistem yang diusulkan dapat secara efektif membedakan perbedaan antara serangan DDoS dan transmisi normal untuk mengurangi dampak serangan DDoS pada penyimpanan data IoT saat sedang diserang. Penelitian tersebut menggunakan algoritma CNN untuk memilah *traffic* yang berasal dari DDoS dan yang normal.

Pada penelitian diatas membahas pendeteksian dan pertahanan dari serangan DoS dan DDoS dengan berbagai metode yang digunakan. Salah satu protokol yang dapat diamankan dari serangan DoS yaitu HTTP. Dalam penelitian ini pengamanan HTTP menggunakan *IPTables* untuk meminimalisir serangan tersebut. Percobaan serangan ke server dapat menggunakan *Low Orbit Ion Cannon* (LOIC) yang mampu menghambat protokol HTTP bekerja pada komputer server, untuk itu diperlukan cara untuk mempertahankan komputer server yang memiliki layanan HTTP dari serangan DoS maupun DDoS sekaligus melakukan pemblokiran akses penyerang ke server.

2. METODE PENELITIAN

2.1. Metode Penelitian

Membuat desain jaringan yang memenuhi kebutuhan konsumen dan target organisasi mengamanatkan identifikasi tujuan teknis, dan batasan. Cisco telah merampingkan siklus hidup jaringan menjadi enam fase: *prepare, plan, design, implement, operate,* dan *optimize* (PPDIOO) [11].



Gambar 2. Pendekatan Siklus Hidup Jaringan PPDIOO

Prepare, sebagai analisa kebutuhan yang diperlukan adalah mencari jurnal penelitian sebagai acuan. Kemudian dilanjutkan dengan kebutuhan *hardware* yang terdiri dari 1 PC yang digunakan untuk membuat virtualisasi dengan *virtualbox*, laptop yang digunakan utuk melakukan penyerangan terhadap komputer *virtualbox*, *i* digunakan untuk konsentrator menghubungkan komputer, kabel UTP sebagai media penghubung perangkat yang melalui

switch, dan *cramping tools* sebagai alat untuk merakit kabel jaringan.

Plan, sebagai tahapan rencana yang melakukan analisis terhadap penelitian yang akan diarahkan kearah mana, yaitu percobaan-percobaan yang dilakukan dengan aktivitas sesudah dan sebelum konfigurasi terhadap serangan protokoll http. Pada perangkat keras yang telah disediakan dengan karakteristik *switch unmanage* dan tipe kabel cat 6 serta tipe jaringan dengan menggunakan protocol dhcp.

Design, tahapan dengan mengilustrasikan atau membuat topologi jaringan untuk pengujian yang akan dilakukan. Ini adalah bagian dari skenario agar mudah di pahami bahwa topologi akan menceritakan konsep kerja yang dimaksud. Pada topologi digambar 3 menunjukkan sebuah *host* virtualisasi dengan garis putus-putus yang dihasilkan dari komputer *server*.

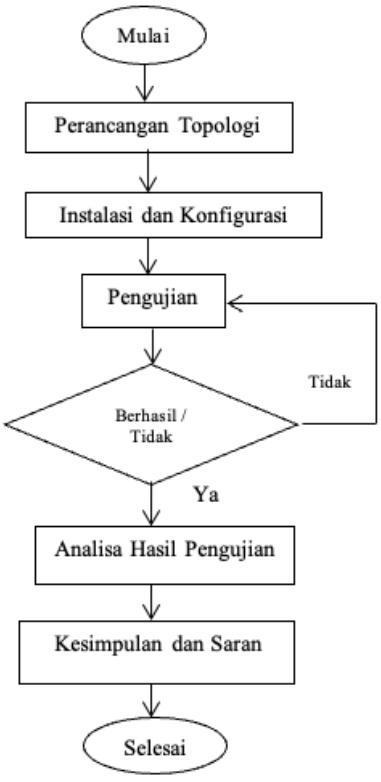
Implement, pada tahap ini adalah dilakukan konfigurasi pada komputer virtual. Konfigurasi pada system operasi dengan instalasi web server apache, serta modul-modul yang dibutuhkan. Kemudian dilanjutkan dengan pengujian beberapa kali, sampai hasil yang diharapkan tercapai. Pengujian disini maksudnya adalah posisi dimana sebelum konfigurasi dan sesudah konfigutasi *iptables* terpasang dengan baik.

Operate, tahapan ini dimana kita melakukan monitoring pada log-log yang dihasilkan pada traffic jaringan, apakah *firewall* masih posisi masih terpasang atau ada perubahan konfigurasi. Monitoring ini wajib dilakukan untuk menjaga stabilitas sumber daya misalnya processor, hard disk, memory dan sebagainya.

Optimize, pada tahapan ini diminta untuk proaktif dalam menyelesaikan masalah yang mengganggu kinerja *performance* dari *web server*. Kemudian diharapkan mampu melakukan modifikasi pada konfigurasi untuk pengembangan maupun pada topologi jaringan.

2.2. Alur Penelitian

Pendekatan penelitian ini melalui beberapa tahapan yang dituangkan dalam kerangka penelitian. Kerangka penelitian secara sistematis menggambarkan langkah-langkah penelitian, termasuk proses desain, pengujian, dan analisis.



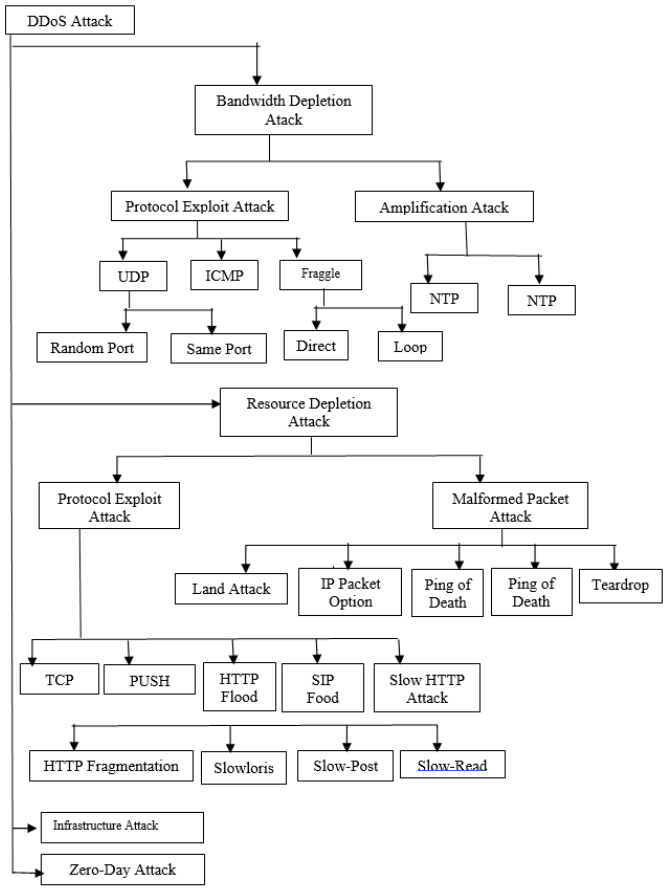
Gambar 3. Alur Penelitian

Tahapan awal penelitian adalah merancang, membangun topologi kemudian melakukan instalasi dan konfigurasi environment yang dibutuhkan dalam menyediakan web server untuk di uji. Penjelasan alur penelitian adalah sebagai berikut:

a. Perancangan topologi, sebagai ilustrasi konsep pengujian dan kebutuhan penelitian yang terdiri dari PC, laptop, kabel dan *switch*.
b. Instalasi dan konfigurasi, menyiapkan komponen-komponen perangkat keras dan perangkat lunak serta melakukan instalasi sesuai topologi. Kemudian dilanjutkan dengan konfigurasi *web server* untuk pengujian di tahapan selanjutnya.
c. Pengujian yaitu dilakukan penyerangan terhadap *web server* apakah berdampak dari serangan tersebut dengan pengujian sebelum dan sesudah konfigurasi.
d. Pengambilan hasil setelah pengujian, apakah dengan konfigurasi sudah berhasil atau belum, maka pengujian akan dilakukan berulang-ulang sampai berhasil.
e. Analisa pengujian memisahkan hasil sebelum konfigurasi dan setelah konfigurasi supaya menunjukkan adanya perbedaan terhadap *web server* yang diserang LOIC tidak berdampak sama sekali dikarenakan IPTABLES bekerja.
f. Kesimpulan dari percobaan bahwa *web server* menunjukkan stabilitas tidak mengalami gangguan walau DoS sedang berlangsungJelaskan metode penelitian secara umum, rumus atau tahapan penyelesaian masalah secara detail dan lengkap.

2.3. DDoS

Spektrum lengkap serangan DDoS diilustrasikan secara komprehensif pada Gambar 4, dikategorikan berdasarkan dampaknya pada jaringan atau sumber daya yang ditargetkan. Korban yang paling sering terkena dampak adalah *web* dan *server proxy* yang beroperasi dengan sumber daya terbatas untuk menawarkan layanan mereka.



Gambar 4. Spektrum Serangan DDoS

Sebagai praktik standar untuk mengelola lalu lintas jaringan berlebih, *server* ini membuang paket yang melampaui ambang batas tertentu. Tindakan ini juga berfungsi sebagai pengingat bagi pengirim paket untuk mengurangi kecepatan pengirimannya. Ketika pengirim yang berwenang menanggapi pesan dengan memperlambat pengirimannya, penyerang menganggapnya sebagai kemenangan dan melipatgandakannya dengan meningkatkan kecepatan. Hal ini mengakibatkan sumber daya sistem korban, seperti memori dan CPU, kebanjiran dan tidak dapat berfungsi seperti biasa. Akibatnya, permintaan pengguna asli ditolak, dan *bandwidth* jaringan terkuras oleh serangan lain yang lebih rentan. Dalam kasus ini, aliran paket *traffic bandwidth* yang berlebihan membanjiri jaringan, dan ini membahayakan korban tetapi juga sistem lain yang bergantung pada jalur serangan ini, dengan demikian, ini memberikan efek besar pada jaringan dan sistem yang terhubung ke jaringan itu. Oleh karena itu, klasifikasi serangan DDoS perlu mempertimbangkan dua dampak ini dan mengkategorikan serangan DDoS menjadi dua kelompok besar: serangan pengurasan *bandwidth* dan serangan pengurasan sumber daya. Namun, pada kenyataannya, sebuah serangan dapat memiliki kedua dampak tersebut dan dapat memberikan pengaruh setinggi mungkin ke seluruh Internet. Jenis ini disebut sebagai serangan Infrastruktur [5].

2.4. IPTables dan *Low Orbit Ion Cannon* (LOIC)

IPTables adalah *firewall open-source* yang mumpuni yang disertakan dalam Linux 2.4.x dan versi yang lebih baru. *Iptables* dapat diandalkan dan kuat dan menawarkan ketergantungan yang tinggi. Sebelum *IPTables*, *ipchains* (Linux 2.2.x) dan *ipfwadm* (Linux 2.0.x) digunakan untuk memfilter sistem Linux. *Iptables* didasarkan pada modul Netfilter yang dapat memeriksa konten paket untuk *string* tertentu dengan menggunakan kemampuan dukungan pencocokan *string* dari *kernel* Linux. Oleh karena itu, *iptables* dapat digunakan untuk mendeteksi serangan pada lapisan aplikasi. Pada dasarnya, *Intrusion Detection System* (IDS) digunakan untuk mendeteksi serangan berbasis konten karena kemampuannya untuk melihat ke dalam paket. IDS mendeteksi serangan dengan mencocokkan tanda tangan dengan serangan, yang meningkatkan waktu analisis karena IDS diimplementasikan sebagai perangkat lunak aplikasi. Sebaliknya, *iptables* dapat mencocokkan *string* lebih cepat karena menggunakan dukungan pencocokan *string* yang diimplementasikan dalam kernel itu sendiri. [6]. *Iptables* disini digunakan sebagai *tools* yang akan mencegah serangan DDoS yang dilancarkan oleh LOIC yang tujuannya melumpuhkan protokol HTTP.

Aplikasi serangan Denial of Service yang melakukan *stress test* jaringan tersedia dalam bentuk *open source*. Terdapat dua versi antara lain opsi biner dan LOIC berbasis web. *Tools* ini mengharuskan memasukkan URL server target, beserta alamat IP-nya, untuk membanjirinya dengan paket TCP, UDP, dan HTTP [7] .

Untuk meminimalisir serangan DoS, pada komputer target perlu ditambahkan *IPTables* agar banyaknya permintaan ke protokol http tidak menguras kinerja CPU server, berikut perintah untuk instalasi *IPTables*.

```
# apt install iptables
```

Dilanjutkan konfigurasi untuk meminimalisir serangan DoS dengan menambahkan *script* sebagai berikut [12].

```
# iptables -A INPUT -p tcp -m state --state NEW -m limit --limit 2/second --limit-burst 2 -j ACCEPT
# iptables -A INPUT -p tcp -m state --state NEW -j LOG --log-prefix "DoS terdeteksi"
# iptables -A INPUT -p tcp -m state --state NEW -j DROP
```

Untuk mendeteksi serangan *port scanning* dapat menambahkan konfigurasi *script* sebagai berikut:

```
# Iptables -A INPUT -p tcp -i ens33 -m state --state NEW -m recent --update --seconds 30 --
  hitcount 10 -j LOG --log-prefix “port scan detected”

# Iptables -A FORWARD -p tcp -i tcp ens33 -m state --state NEW -m recent  --update  --seconds
  30  --hitcount 10  -j LOG  --log-prefix  “port scan detected”
```

Dilanjutkan dengan *script IPTables* untuk menghalau serangan *port scanning* sehingga serangan tersebut tidak mendapatkan informasi komputer target.

```
# iptables -N portscan
# iptables -A portscan -j LOG --log-level 4 --log-prefix 'Blocked_scans '
# iptables -A portscan -j DROP

# iptables -A INPUT -m recent --name portscan --rcheck --seconds 86400 -j portscan
# iptables -A INPUT -m recent --name UDP_FLOOD --rcheck --seconds 86400 -j portscan

# iptables -A INPUT -m recent --name portscan --remove
# iptables -A INPUT -m recent --name UDP_FLOOD –remove
# iptables -A INPUT -p tcp -m tcp -m recent -m state --state NEW --name portscan --set -j
  portscan
```

Script *IPTables* di atas melakukan pemblokiran IP komputer yang menyerang komputer target selama 1 hari, ketika pemblokiran telah mencapai 1 hari maka akan dilepaskan dari pemblokiran secara otomatis.

2.5. VirtualBox dan Apache

VirtualBox adalah produk virtualisasi dengan arsitektur x86 dan AMD64/Intel64 yang tangguh untuk penggunaan bisnis dan rumahan. *VirtualBox* adalah produk yang sangat kaya fitur dan berkinerja tinggi untuk pelanggan perusahaan, tetapi juga merupakan satu-satunya solusi profesional yang tersedia secara bebas sebagai perangkat lunak open source di bawah ketentuan GNU *General Public License* (GPL) versi 3.

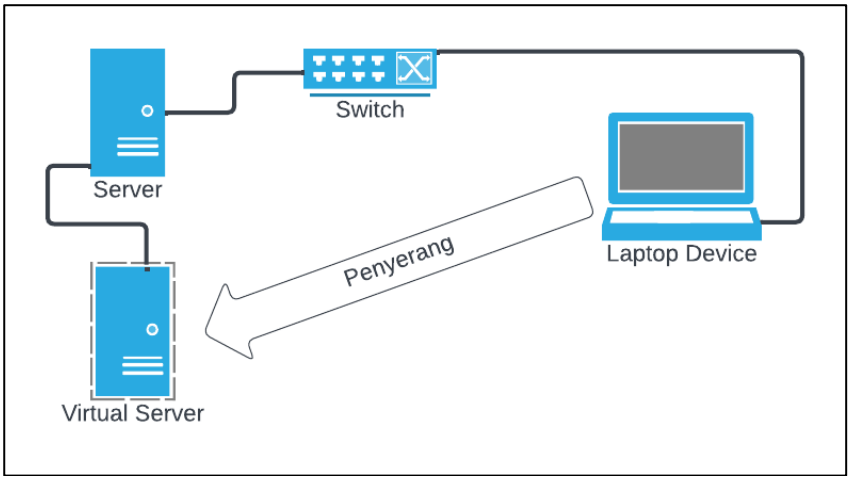
Saat ini, VirtualBox berjalan pada host Windows, Linux, macOS, dan Solaris, dan mendukung sejumlah besar sistem operasi tamu, termasuk tetapi tidak terbatas pada Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS /Windows 3.x, Linux (2.4, 2.6, 3.x, dan 4.x), Solaris dan OpenSolaris, OS/2, dan OpenBSD. [8]. Komputer virtualbox dalam topologi adalah sebuah komputer target yang akan menerima serangan dari LOIC.

Web server yang digunakan adalah apache dikarenakan kepopulerannya Menurut W3Techs (Teknologi Web -Survei Ilmiah) [9], per 1 April 2023; Apache digunakan 32,1% berada pada peringkat dua dari semua web server. Apache juga termasuk aplikasi yang bersifat opensources sebagai sumber yang terbuka dan system modul yang dimuat secara dinamis. Instalasi dilakukan dengan paket baris perintah *apt-get* [10]. Berikut perintah instalasi web server apache dan paket PHP yang digunakan pada VirtualBox.

```
# apt install apache2
# apt install php libapache2-mod-php php-mysql
```

2.6. Topologi Pengujian

Pada gambar dibawah ini adalah topologi pengujian ketika dilakukan uji serangan terhadap komputer virtualbox.



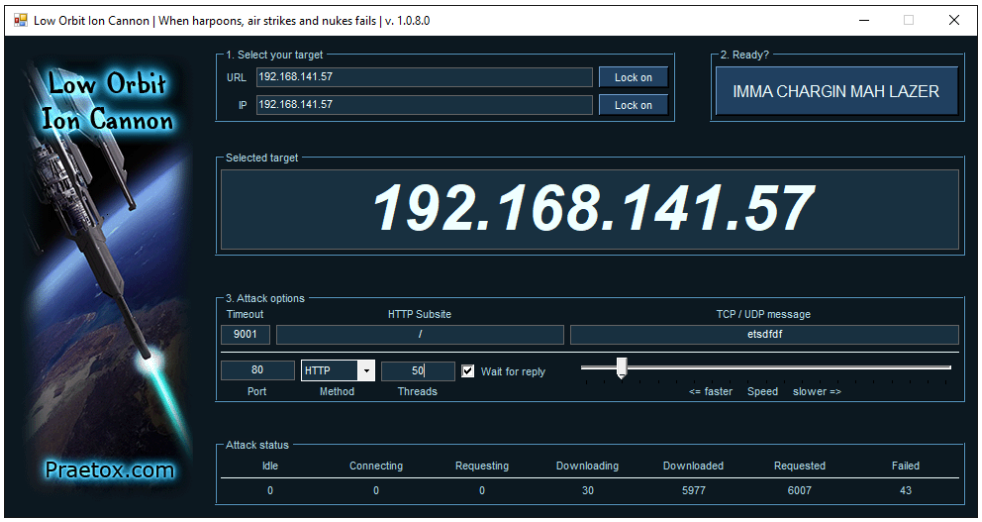
Gambar 5. Topologi Pengujian

Pada gambar 5 menunjukkan bahwa komputer penyerang mencoba melumpuhkan porotokol HTTP yang dimiliki komputer *virtual server* virtualbox dengan tools DoS LOIC. Perlu dilakukan pengujian sebelum dan sesudah konfigurasi menggunakan *Iptables* sehingga terlihat bahwa *firewall iptables* mampu menanggulanginya.

3. HASIL DAN PEMBAHASAN

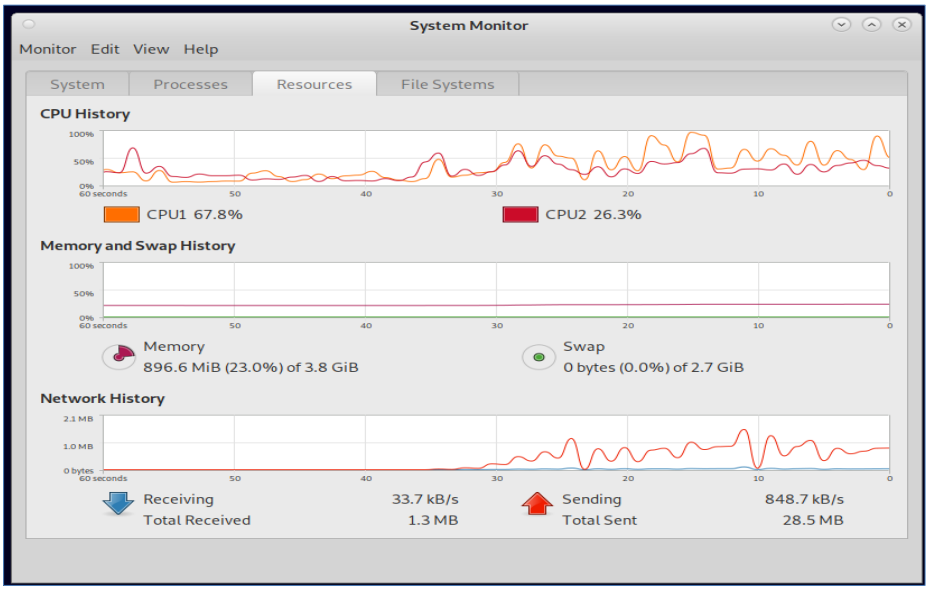
3.1 Pengujian sebelum Instalasi IPTables

Pada tahap pengujian ini menggunakan *tools* LOIC dengan cara mengisi bagian-bagian seperti *url* dan *ip address* target kemudian pada *attack option* pilih port 80, *method* http, *threads* isikan 20-50 akan terasa signifikan serangan, dan pada TCP/UDP *message* bisa kita tingkatkan kecepatan serangan dengan menggeser ke kanan yang dapat dilihat pada gambar 6.



Gambar 6. LOIC

Pada gambar 7 dapat dilihat bahwa kinerja CPU yang meningkat menjadi 67.8% ketika mendapati serangan LOIC selama 30 detik. Kinerja CPU terbebani karena melayani permintaan mengkases http secara terus menerus tanpa jeda.



Gambar 7. Monitoring sebelum konfigurasi

Kemudian pada pengujian *port scanning* pada komputer target menggunakan aplikasi nmap terlihat pada gambar 8. Aktifitas menggunakan nmap adalah melakukan *port scanning* dengan melihat layanan apa saja yang terhubung ke *network* pada komputer target. Aktifitas *port scanning* ini mampu mencari informasi layanan yang tersedia pada komputer target, misalnya versi apache yang digunakan, jenis sistem operasi yang dipakai pada komputer target.

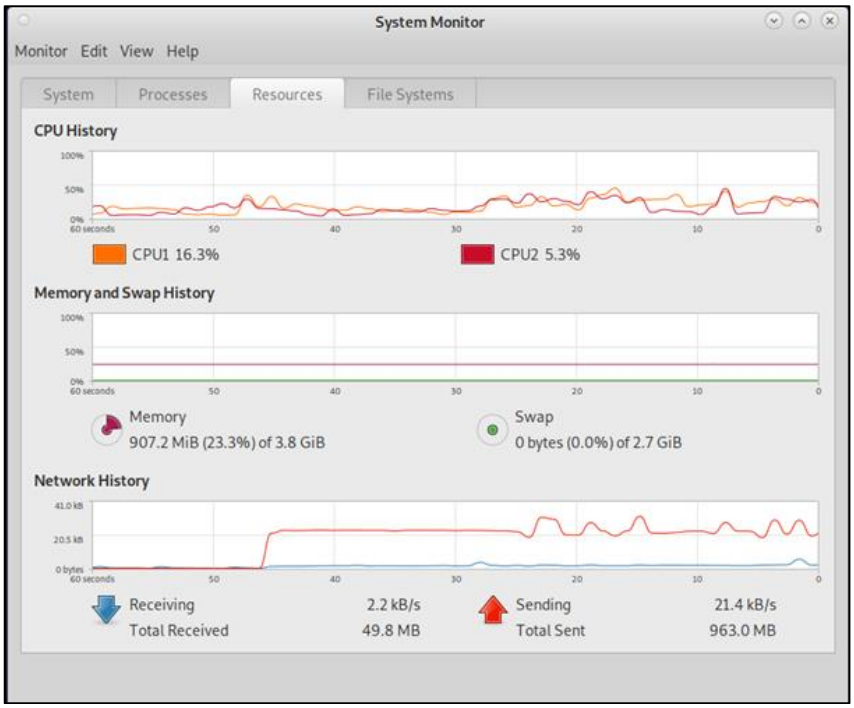
```
┌──(root@kali)-[/home/mola]
└─# nmap -p 80 -v -A 192.168.141.57

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.54 (Debian)
MAC Address: 00:0C:29:DA:8B:3A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 19.562 days (since Fri Apr  7 21:40:24 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
```

Gambar 8. Hasil *Scanning Port*

3.2 Pengujian setelah Instalasi *IPTables*

Setelah ditambahkan script *IPTables*, dilakukan percobaan serangan kembali ke komputer target. Pada gambar 9 dapat dilihat kinerja CPU tidak mengalami kenaikan dan CPU berjalan normal. *IPTables* dapat menghalau serangan DoS dengan baik dan tidak membuat sibuk protokol http melayani permintaan yang banyak.



Gambar 9. Monitoring setelah konfigurasi

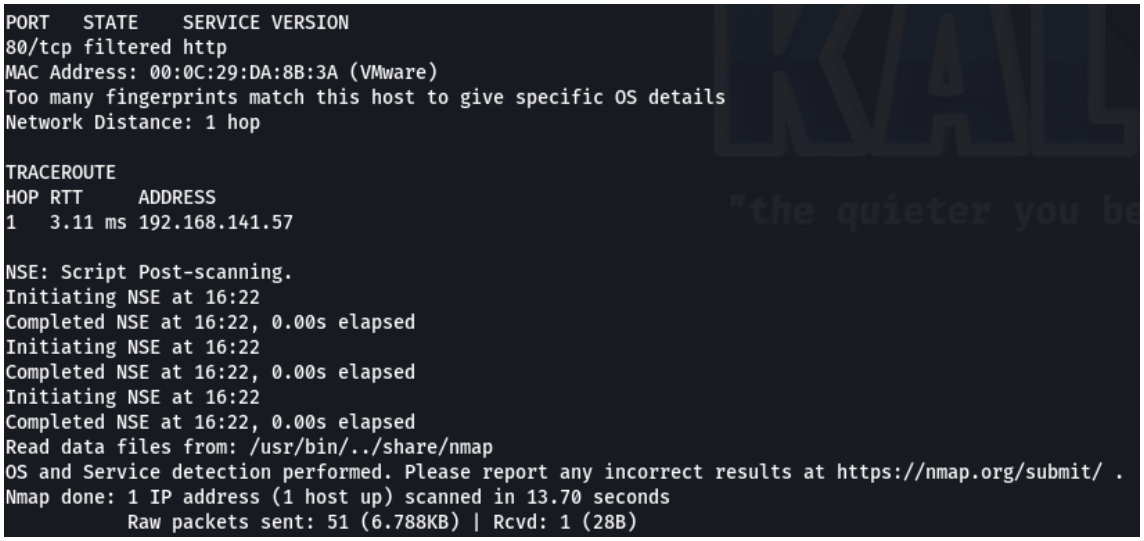
Kemudian hasil pengujian *port scanning* pada komputer target menggunakan aplikasi nmap kembali dapat dilihat pada gambar 10.

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:DA:8B:3A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 42.757 days (since Sun Mar 26 19:23:25 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   33.22 ms 192.168.141.57
```

Gambar 10. Hasil *Scanning Port*

Pada gambar 11 terlihat bahwa tidak didapati informasi mengenai komputer target sepeti jenis *web server* yang digunakan, dan jenis sistem operasi yang dipakai setelah dilakukan konfigurasi *IPTables*.



Gambar 11. Informasi yang dihasilkan *Scanning Port*

4. KESIMPULAN DAN SARAN

Berdasarkan percobaan sebelum konfigurasi *IPTables* dengan serangan LOIC dihasilkan mampu melumpuhkan komputer target dengan menguras sumber daya yang ada. Setelah dilakukan instalasi dan kofigurasi *IPTables*, dan dilakukan serangan kembali dihasilkan *IPTables* mampu menghalau serangan LOIC dan kinerja CPU komputer masih stabil. Sementara pada percobaan *scanning port* yang mencari informasi pada sebuah server melalui *network* mampu diminimalisir informasi yang didapat oleh *tools* nmap.

DAFTAR PUSTAKA

[1] Id-SIRTII, "Id-SIRTII," Jakarta, 2018. [Online]. Available: https://www.idsirtii.or.id/halaman/tentang/laporan-kegiatan.html.

[2] M. Merouane, "An approach for detecting and preventing DDoS attacks in campus," *Autom. Control Comput. Sci.*, vol. 51, no. 1, pp. 13–23, 2017, doi: 10.3103/S0146411616060043.

[3] A. Prakash and R. Priyadarshini, "An Intelligent Software defined Network Controller for preventing Distributed Denial of Service Attack," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018*, no. Icicct, pp. 585–589, 2018, doi: 10.1109/ICICCT.2018.8473340.

[4] S. H. Lee, Y. L. Shiue, C. H. Cheng, Y. H. Li, and Y. F. Huang, "Detection and Prevention of DDoS Attacks on the IoT," *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312407.

[5] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[6] N. Gandotra and L. Sen Sharma, "Exploring the use of Iptables as an Application Layer Firewall," *J. Inst. Eng. Ser. B*, vol. 101, no. 6, pp. 707–715, 2020, doi: 10.1007/s40031-020-00497-y.

[7] A. R. Assistant Professor, "Experimentation Of Denial Of Service Attack In Wireless Local Area Infrastructure Network Using Loic Tool," *Arunadevi R J. Eng. Res. Appl. www.ijera.com*, vol. 8, no. 8, pp. 51–55, 2018, doi: 10.9790/9622-0808035155.

[8] Virtualbox.org, "VirtualBox," 2023. https://virtualbox.org (accessed Apr. 11, 2023).

[9] W3techs.com, "Web Technology Surveys," *1 April 2023*, 2023. https://w3techs.com/ (accessed Apr. 30, 2023).

[10] M. Baş Seyyar, F. Ö. Çatak, and E. Gül, "Detection of attack-targeted scans from the Apache HTTP Server access logs," *Appl. Comput. Informatics*, vol. 14, no. 1, pp. 28–36, 2018, doi: 10.1016/j.aci.2017.04.002.

[11] Y. S. Pratama, A. Budiono, and A. Almaarif, "Analisis Dan Perancangan Cooling Management Data Center Berdasarkan Standar Tia-942 Menggunakan Ppdioo Life-Cycle Approach Di Pemerintahan Kabupaten Bandung Barat Analysis And Designing Of Cooling Management Data Center Based On Tia-942 Standards Using Ppdioo Life-Cycle Approach In West Bandung District Government," 2020, pp. 6656–6663, Accessed: Nov. 07, 2022. [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/12484/12253.

[12] E. S. J. Atmadji, B. M. Susanto, and R. Wiratama, "Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server," *Teknika*, vol. 6, no. 1, pp. 19–23, 2017, doi: 10.34148/teknika.v6i1.55.