

LAPORAN PROJECT AKHIR

Implementasi IPTables untuk Mencegah Serangan DDoS

(Studi Kasus: Kali Linux sebagai Attacker dan Ubuntu Server sebagai Target)



*Disusun oleh
Glenvio Regalito Raharjo*

*Sekolah
SMK Telkom Purwokerto*

*Program
D1 Cyber Security Officer*

*Tahun
2025*

1. Identitas Praktikan

- **Nama :** Glenvio Regalito Raharjo
 - **Kelas / Program :** D1 Cyber Security Officer
 - **Judul Project :** Implementasi IPTables untuk Mencegah Serangan DDoS
 - **Lingkungan Praktikum :**
 - Windows 11
 - WSL (Windows Subsystem for Linux)
 - Kali Linux (Penyerang)
 - Ubuntu Server 24.04 (Target)
 - **Tanggal Praktikum :** 18/12/2025
-

2. Pendahuluan

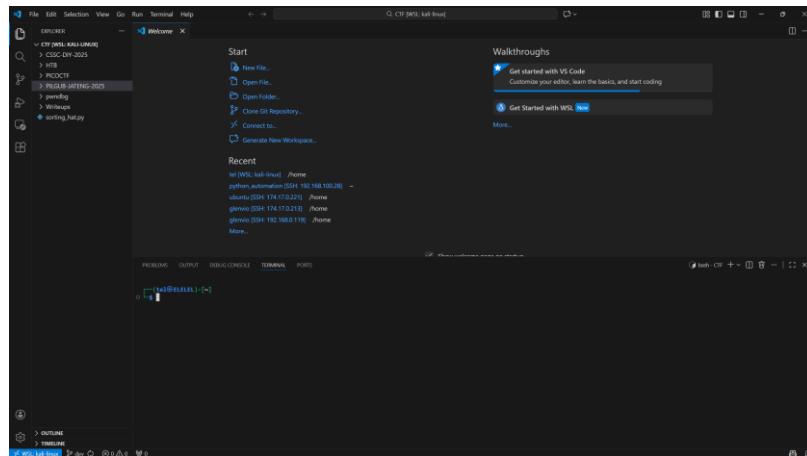
Serangan **Distributed Denial of Service (DDoS)** merupakan salah satu serangan yang bertujuan untuk membuat layanan server tidak dapat diakses dengan cara membanjiri server menggunakan permintaan dalam jumlah besar.

Pada project ini dilakukan simulasi serangan DDoS menggunakan Kali Linux (WSL) dan dilakukan pengamanan server Ubuntu (VBOX) menggunakan **IPTables** untuk membatasi lalu lintas jaringan berlebih.

3. Topologi dan Lingkungan LAB

Praktikum dilakukan menggunakan dua lingkungan sistem operasi yang berbeda. Kali Linux dijalankan pada **WSL (Windows Subsystem for Linux)** dan digunakan sebagai mesin penyerang. Sementara itu, **Ubuntu Server dijalankan pada mesin virtual (VirtualBox)** dan digunakan sebagai web server target dengan alamat IP **192.168.1.13**. Kedua sistem saling terhubung melalui jaringan lokal sehingga memungkinkan proses pengujian dan simulasi serangan dilakukan.

- **Kali Linux (WSL)** digunakan sebagai mesin penyerang dan diakses melalui **Visual Studio Code (VS Code)** untuk mempermudah proses pengelolaan terminal dan eksekusi perintah dibandingkan menggunakan Command Prompt secara langsung.



- **Ubuntu Server** digunakan sebagai web server target dan dijalankan pada mesin virtual (VirtualBox) dengan alamat IP **192.168.1.13**, yang diakses melalui **SSH menggunakan Command Prompt (CMD)** untuk keperluan konfigurasi dan manajemen server.

```

glenvio@server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:09:27:cb:24:fc brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.13/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
            valid_lft 85888sec preferred_lft 85888sec
            inet6 fe80::a00:27ff:fe:cb24fc/64 scope link
                valid_lft forever preferred_lft forever
glenvio@server:~$ 

```

Kali Linux (WSL) dan Ubuntu Server (VirtualBox) saling terhubung melalui **jaringan lokal yang sama**, sehingga dapat berkomunikasi satu sama lain.

4. Persiapan Ubuntu Server (Target)

4.1 Instalasi Ubuntu Server

Ubuntu Server 24.04 dijalankan pada Virtualbox dan digunakan sebagai web server.

4.2 Instalasi Apache2

`sudo apt update`

`sudo apt install apache2 -y`

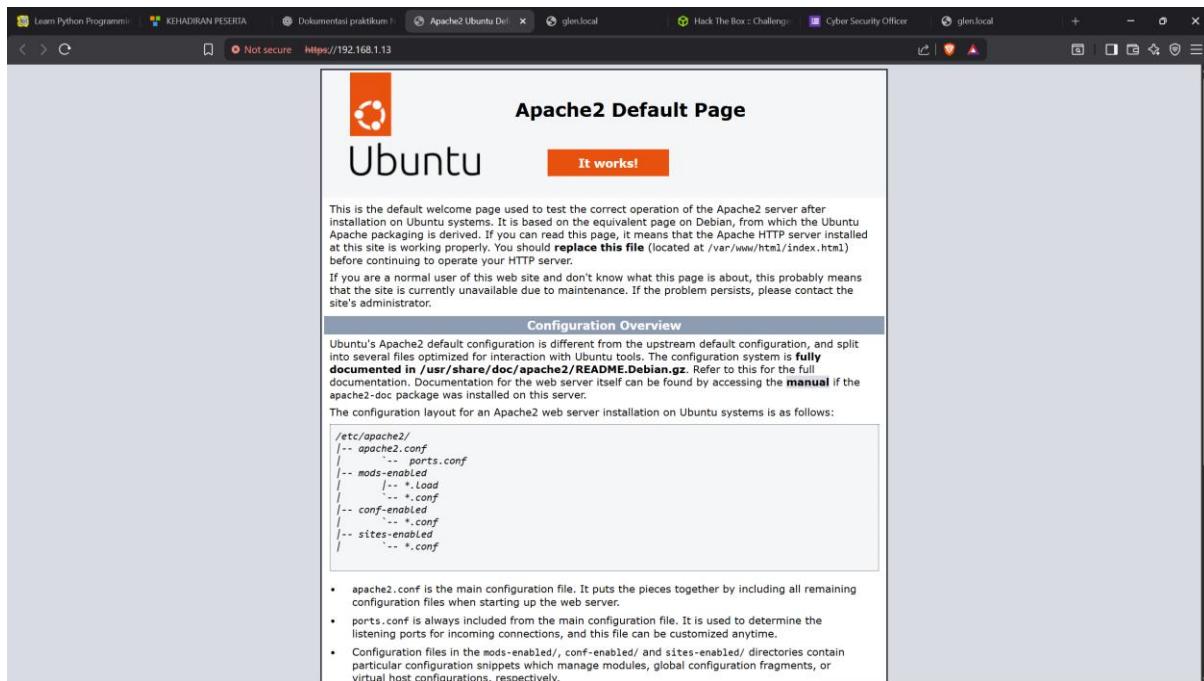
`systemctl status apache2`



Apache berhasil dijalankan dan dapat diakses melalui browser dengan ip 192.168.1.13

4.3 Konfigurasi HTTPS

HTTPS dikonfigurasi menggunakan **SSL self-signed certificate** dengan OpenSSL.



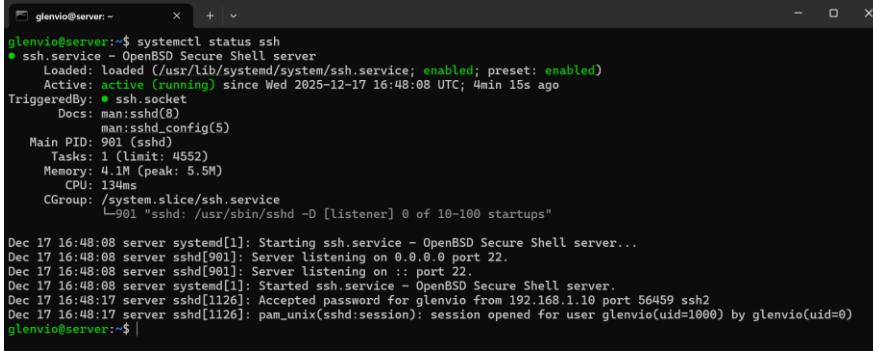
<https://192.168.1.13/>

4.4 Instalasi Service Tambahan

sudo apt install openssh-server vsftpd telnetd -y

Service yang berjalan:

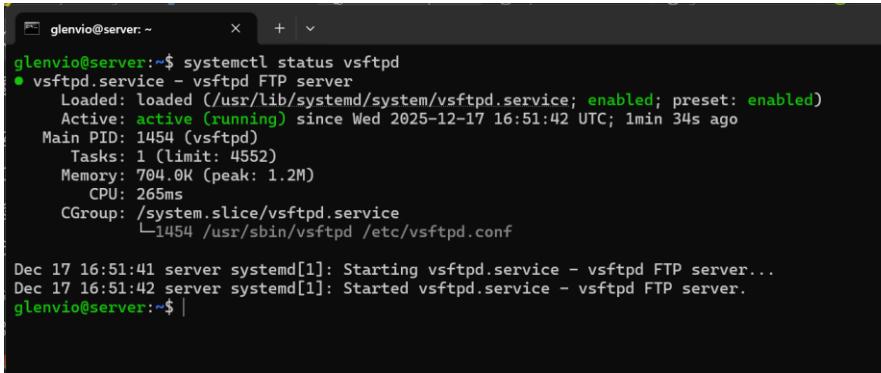
- SSH



```
glenvio@server:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-12-17 16:48:08 UTC; 4min 15s ago
TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 901 (sshd)
    Tasks: 1 (limit: 4552)
   Memory: 4.1M (peak: 5.5M)
     CPU: 134ms
    CGroup: /system.slice/ssh.service
            └─901 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 17 16:48:08 server systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 17 16:48:08 server sshd[901]: Server listening on 0.0.0.0 port 22.
Dec 17 16:48:08 server sshd[901]: Server listening on :: port 22.
Dec 17 16:48:08 server systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Dec 17 16:48:17 server sshd[1126]: Accepted password for glenvio from 192.168.1.10 port 56459 ssh2
Dec 17 16:48:17 server sshd[1126]: pam_unix(sshd:session): session opened for user glenvio(uid=1000) by glenvio(uid=0)
glenvio@server:~$ |
```

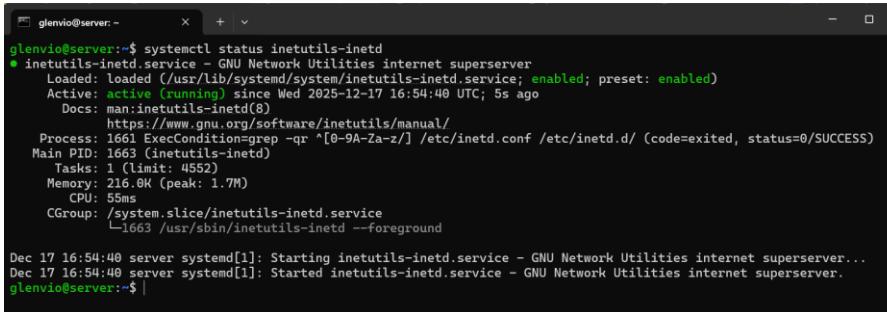
- FTP



```
glenvio@server:~$ systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
  Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-12-17 16:51:42 UTC; 1min 34s ago
    Main PID: 1454 (vsftpd)
      Tasks: 1 (limit: 4552)
     Memory: 704.0K (peak: 1.2M)
       CPU: 265ms
      CGroup: /system.slice/vsftpd.service
              └─1454 /usr/sbin/vsftpd /etc/vsftpd.conf

Dec 17 16:51:41 server systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Dec 17 16:51:42 server systemd[1]: Started vsftpd.service - vsftpd FTP server.
glenvio@server:~$ |
```

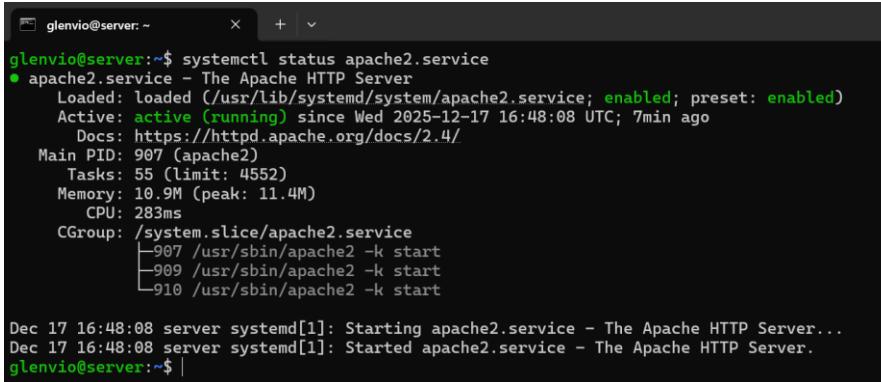
- Telnet



```
glenvio@server:~$ systemctl status inetutils-inetd
● inetutils-inetd.service - GNU Network Utilities internet superserver
  Loaded: loaded (/usr/lib/systemd/system/inetutils-inetd.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-12-17 16:54:40 UTC; 5s ago
    Docs: man:inetutils-inetd(8)
          https://www.gnu.org/software/inetutils/manual/
  Process: 1661 ExecCondition=grep -qr ^[0-9A-Za-z/] /etc/inetd.conf /etc/inetd.d/ (code=exited, status=0/SUCCESS)
  Main PID: 1663 (inetutils-inetd)
    Tasks: 1 (limit: 4552)
   Memory: 216.0K (peak: 1.7M)
     CPU: 55ms
    CGroup: /system.slice/inetutils-inetd.service
            └─1663 /usr/sbin/inetutils-inetd --foreground

Dec 17 16:54:40 server systemd[1]: Starting inetutils-inetd.service - GNU Network Utilities internet superserver...
Dec 17 16:54:40 server systemd[1]: Started inetutils-inetd.service - GNU Network Utilities internet superserver.
glenvio@server:~$ |
```

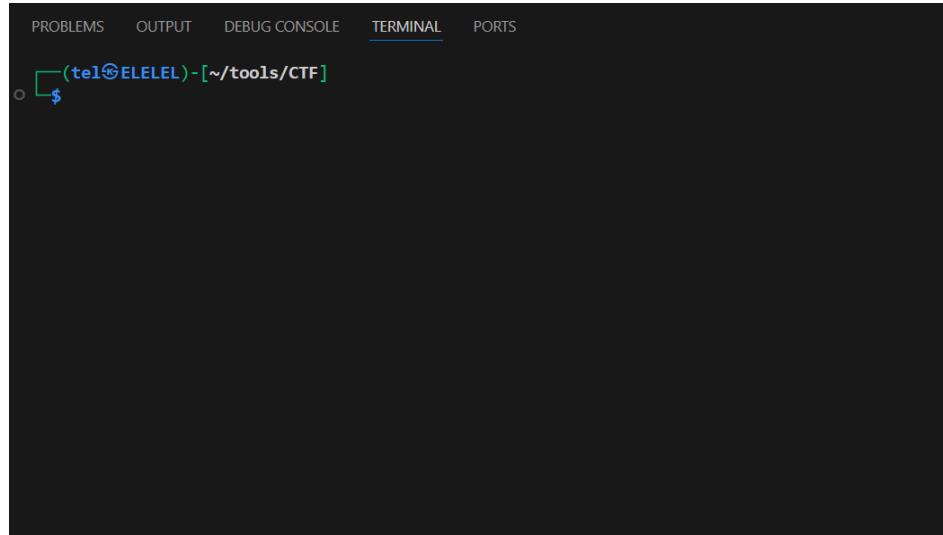
- Apache (HTTP/HTTPS)



```
glenvio@server:~$ systemctl status apache2.service
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-12-17 16:48:08 UTC; 7min ago
    Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 907 (apache2)
    Tasks: 55 (limit: 4552)
   Memory: 10.9M (peak: 11.4M)
     CPU: 283ms
    CGroup: /system.slice/apache2.service
            ├─907 /usr/sbin/apache2 -k start
            ├─909 /usr/sbin/apache2 -k start
            ├─910 /usr/sbin/apache2 -k start

Dec 17 16:48:08 server systemd[1]: Starting apache2.service - The Apache HTTP Server...
Dec 17 16:48:08 server systemd[1]: Started apache2.service - The Apache HTTP Server.
glenvio@server:~$ |
```

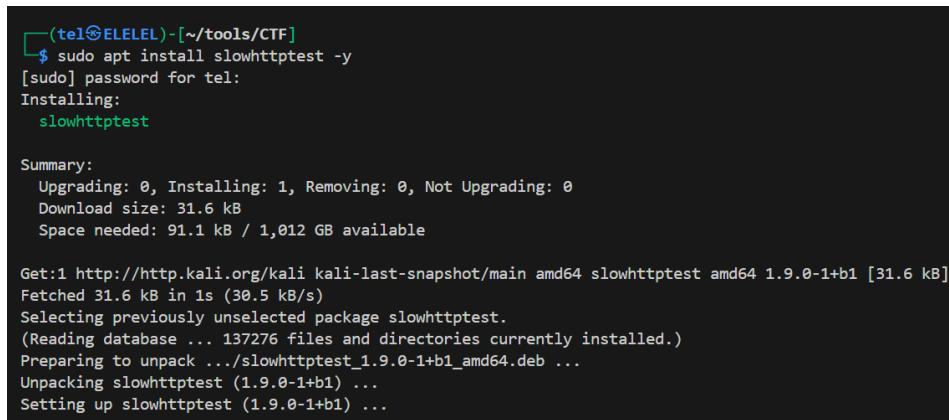
5. Persiapan Kali Linux (Penyerang)



```
(tel㉿ELELEL) - [~/tools/CTF]
$
```

5.1 Instalasi Tool Serangan

```
sudo apt install slowhttptest -y
```



```
$ sudo apt install slowhttptest -y
[sudo] password for tel:
Installing:
  slowhttptest

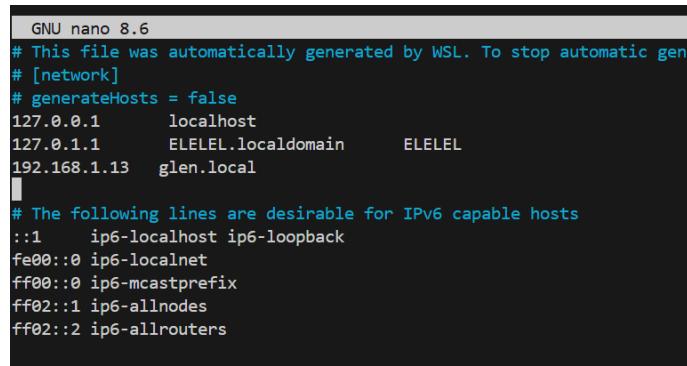
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 31.6 kB
  Space needed: 91.1 kB / 1,012 GB available

Get:1 http://http.kali.org/kali kali-last-snapshot/main amd64 slowhttptest amd64 1.9.0-1+b1 [31.6 kB]
Fetched 31.6 kB in 1s (30.5 kB/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 137276 files and directories currently installed.)
Preparing to unpack .../slowhttptest_1.9.0-1+b1_amd64.deb ...
Unpacking slowhttptest (1.9.0-1+b1) ...
Setting up slowhttptest (1.9.0-1+b1) ...
```

5.2 Konfigurasi Hosts

```
sudo nano /etc/hosts
```

Menambahkan IP Ubuntu Server agar dapat diakses melalui domain lokal.



```
GNU nano 8.6
# This file was automatically generated by WSL. To stop automatic gene
# [network]
# generateHosts = false
127.0.0.1      localhost
127.0.1.1      ELELEL.localdomain      ELELEL
192.168.1.13   glen.local

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

5.3 Pengujian Koneksi

ping ip_ubuntu_server

```
(tel@ELELEL) [~/tools/CTF]
$ ping 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
64 bytes from 192.168.1.13: icmp_seq=1 ttl=63 time=2.84 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=63 time=1.20 ms
64 bytes from 192.168.1.13: icmp_seq=3 ttl=63 time=3.33 ms
64 bytes from 192.168.1.13: icmp_seq=4 ttl=63 time=5.14 ms
64 bytes from 192.168.1.13: icmp_seq=5 ttl=63 time=1.33 ms
```

6. Tahap Penyerangan (Before IPTables)

6.1 Scanning Port

nmap -sS ip_ubuntu_server

Port yang terbuka:

- 80 (HTTP)
- 443 (HTTPS)
- 22 (SSH)

```
(tel@ELELEL) [~/tools/CTF]
$ nmap -sS 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 09:09 WIB
Nmap scan report for glen.local (192.168.1.13)
Host is up (0.020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

6.2 Simulasi Serangan DDoS

slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://ip_ubuntu_server -x 24 -p 3

Hasil:

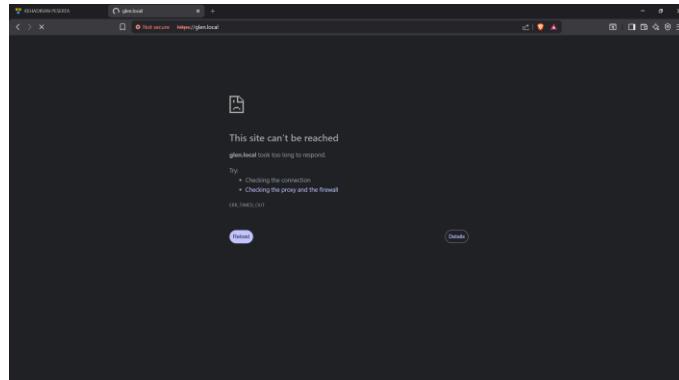
- Server melambat
- Apache mengalami peningkatan request
- Respon web tidak stabil



Sebelum dilakukan simulasi serangan, web server Apache dapat diakses dengan normal. Halaman web tampil stabil dan responsif tanpa kendala.

```
(tel㉿ELELEL) -[~/tools/CTF]
$ slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u https://192.168.1.13 -x 24 -p 3
Thu Dec 18 09:10:46 2025:
Thu Dec 18 09:10:46 2025:
      slowhttptest version 1.9.0
  - https://github.com/shekyan/slowhttptest -
test type:           SLOW HEADERS
number of connections:   1000
URL:                 https://192.168.1.13/
verb:                GET
cookie:
Content-Length header value:    4096
follow up data max size:        52
interval between follow up data: 10 seconds
connections per seconds:       200
probe connection timeout:       3 seconds
test duration:                 240 seconds
using proxy:                   no proxy
```

Simulasi serangan kemudian dilakukan menggunakan tool **slowhttptest** dengan perintah `slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u https://192.168.1.13 -x 24 -p 3`



Setelah serangan dijalankan, performa web server menurun secara signifikan. Akses ke website menjadi lambat dan tidak stabil akibat banyaknya koneksi yang dibuka secara bersamaan, yang menunjukkan bahwa serangan DDoS berhasil memengaruhi ketersediaan layanan.

7. Konfigurasi IPTables (Firewall)

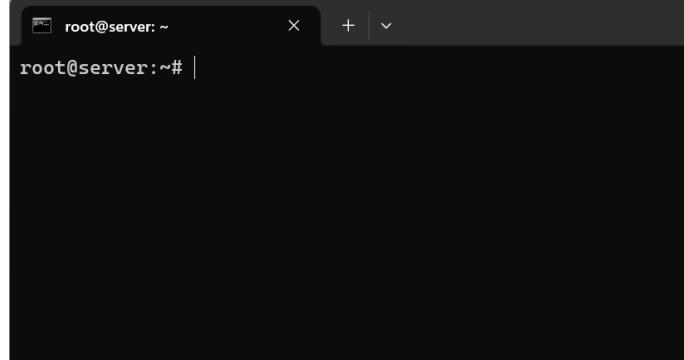
Pada tahap ini dilakukan konfigurasi firewall menggunakan IPTables untuk meningkatkan keamanan server terhadap serangan DDoS. Konfigurasi ini diterapkan setelah dilakukan simulasi serangan, di mana server mengalami penurunan performa akibat banyaknya koneksi yang masuk secara bersamaan. Dengan penerapan IPTables, diharapkan lalu lintas jaringan dapat dikontrol sehingga hanya koneksi yang sah yang diizinkan mengakses layanan server.

7.1 Rule IPTables

Cara Meng-apply Rule IPTables

Masuk sebagai root:

```
sudo -i
```

A screenshot of a terminal window titled "root@server: ~". The window is dark-themed with white text. It shows a single character input field at the bottom and a blank command history area above it.

Lalu jalankan rule berurutan:

```
iptables -F
```

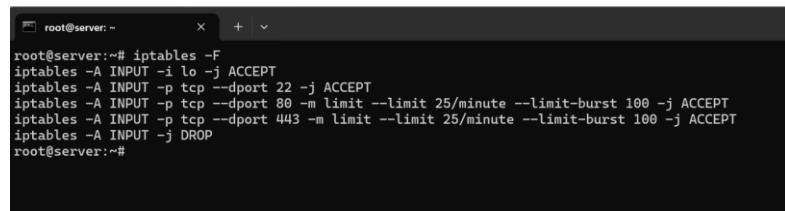
```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

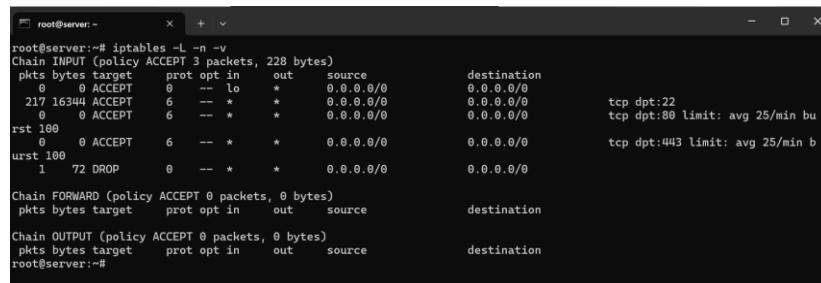
```
iptables -A INPUT -p tcp --dport 443 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

```
iptables -A INPUT -j DROP
```

A screenshot of a terminal window titled "root@server: ~". The window shows several lines of iptables commands being run sequentially. The output of each command is visible as it is typed. The commands include clearing the table, adding rules for local traffic, port 22, port 80, port 443, and finally dropping all other traffic.

7.2 Cek Rule

```
iptables -L -n -v
```

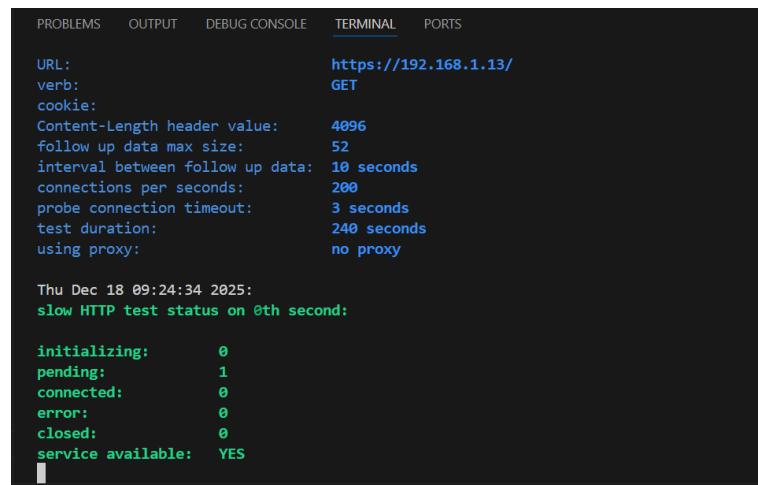
A screenshot of a terminal window titled "root@server: ~". The window displays the output of the "iptables -L -n -v" command. It shows three chains: INPUT, FORWARD, and OUTPUT. The INPUT chain has rules for local traffic (-i lo), port 22, port 80 (with rate limiting), port 443 (with rate limiting), and a final DROP rule. The FORWARD and OUTPUT chains both have an ACCEPT rule for all traffic.

Penerapan rule IPTables dilakukan untuk meningkatkan keamanan server setelah dilakukan simulasi serangan DDoS. Tujuan utama dari konfigurasi ini adalah membatasi lalu lintas

jaringan yang masuk ke server agar tidak terjadi pembukaan koneksi secara berlebihan yang dapat menyebabkan layanan web menjadi lambat atau tidak stabil.

8. Tahap Penyerangan (After IPTables)

Serangan diulang menggunakan **slowhttptest** setelah IPTables diaktifkan.



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

URL: https://192.168.1.13/
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy

Thu Dec 18 09:24:34 2025:
slow HTTP test status on 0th second:

initializing: 0
pending: 1
connected: 0
error: 0
closed: 0
service available: YES
```

Hasil:

- Server tetap berjalan
- Apache masih responsif
- Paket serangan dibatasi oleh firewall



Setelah penerapan IPTables, dampak serangan DDoS dapat dikurangi, namun belum sepenuhnya dihilangkan. Hal ini disebabkan karena serangan Slow HTTP bekerja pada level aplikasi dengan menahan koneksi dalam waktu lama. Oleh karena itu, IPTables berperan sebagai lapisan awal pertahanan dan perlu dikombinasikan dengan mekanisme keamanan tambahan untuk perlindungan yang lebih maksimal.

9. Analisis Before & After

Kondisi	Sebelum IPTables	Sesudah IPTables
Respon Server	Sangat lambat dan tidak stabil saat serangan berlangsung	Lebih stabil, meskipun sesekali terjadi penurunan respon
Serangan	Berhasil memengaruhi ketersediaan layanan	Dampak serangan berkurang, namun belum sepenuhnya terblokir
Apache	Tetap running tetapi mengalami overload	Tetap running dan beban lebih terkendali

Berdasarkan hasil pengujian, penerapan IPTables mampu mengurangi dampak serangan DDoS, khususnya serangan Slow HTTP. Meskipun server masih menerima sebagian koneksi serangan, performa layanan menjadi lebih terkendali dibandingkan sebelum firewall diterapkan.

10. Kesimpulan

Berdasarkan hasil pengujian, penerapan IPTables pada Ubuntu Server mampu mengurangi dampak lalu lintas berlebih yang dihasilkan oleh simulasi serangan DDoS. Setelah firewall diterapkan, performa layanan web menjadi lebih terkendali dan server tetap berjalan meskipun masih terdapat percobaan serangan.

11. Penutup

Melalui project ini dapat disimpulkan bahwa IPTables berperan sebagai solusi dasar dalam mitigasi serangan DDoS pada server Linux. Meskipun belum sepenuhnya menghentikan serangan Slow DDoS, konfigurasi IPTables terbukti membantu menjaga ketersediaan layanan dan dapat dikombinasikan dengan mekanisme keamanan lain untuk perlindungan yang lebih optimal.