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.

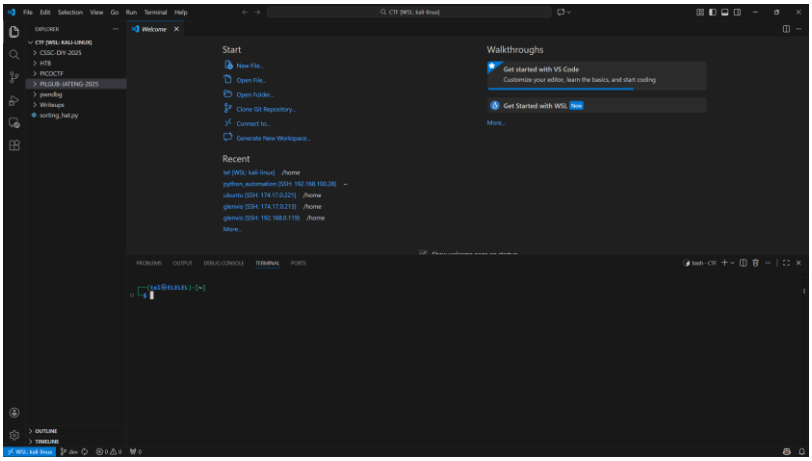
Pada project ini dilakukan simulasi serangan DDoS menggunakan Kali Linux (WSL) dan dilakukan pengamanan server Ubuntu (VBOX) menggunakan **IPTables** untuk membatasi lalu lintas jaringan berlebih.

---

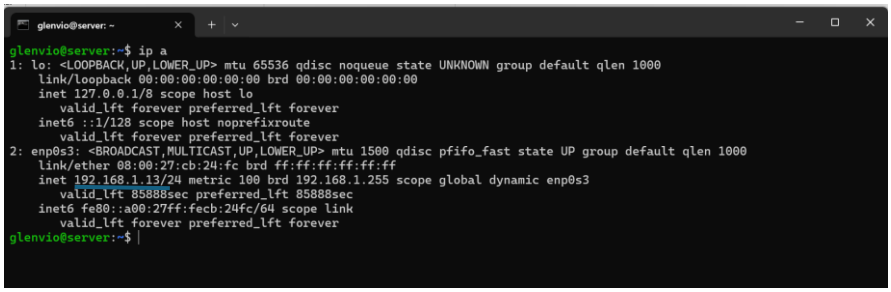
3. Topologi dan Lingkungan LAB

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.



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

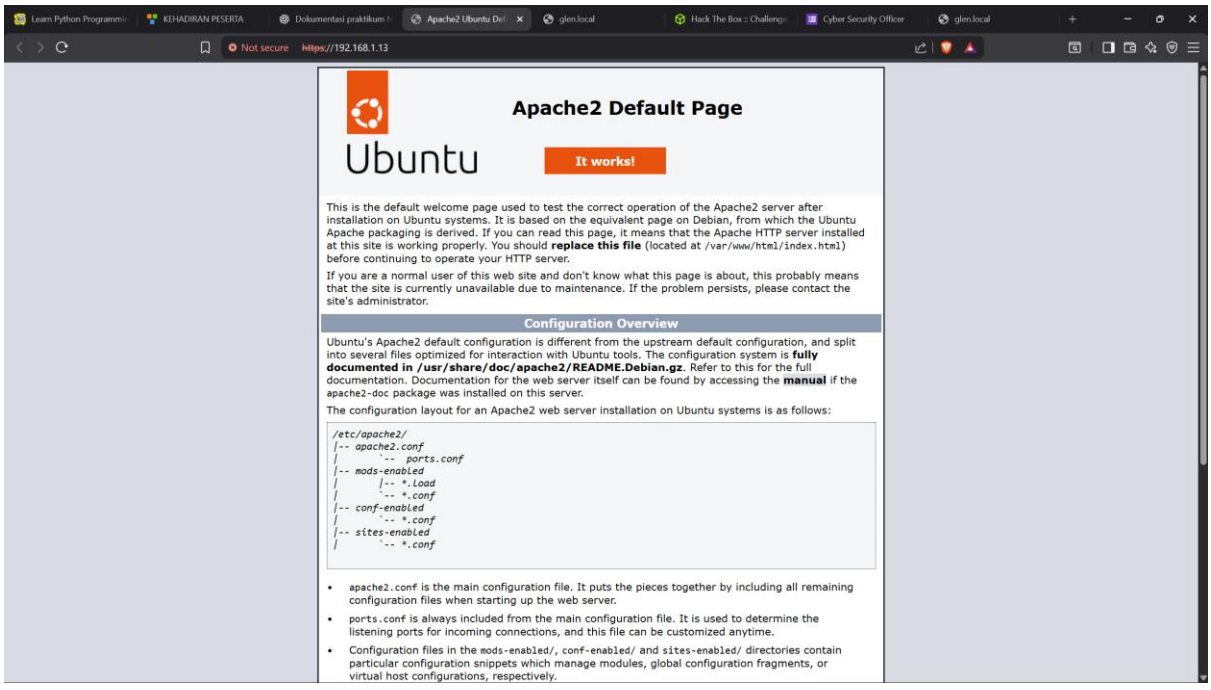
sudo apt install apache2 -y

systemctl status apache2

Apache berhasil dijalankan dan dapat diakses melalui browser denga nip 192.168.1.13

4.3 Konfigurasi HTTPS

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



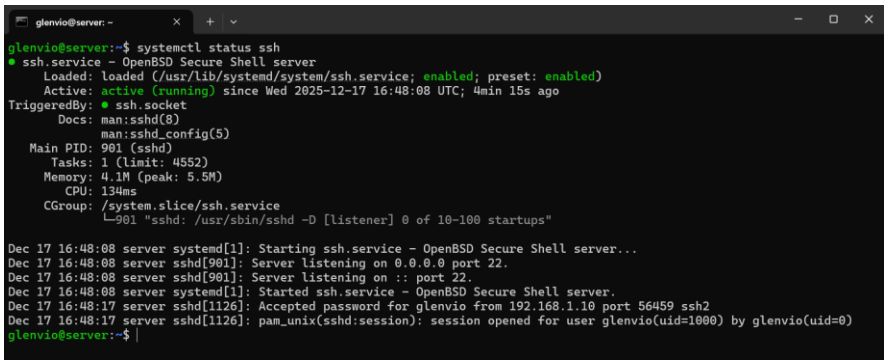
https://192.168.1.13/

4.4 Instalasi Service Tambahan

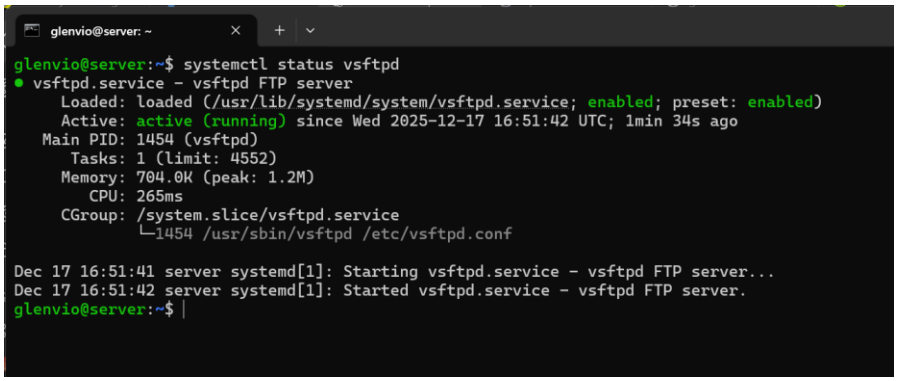
sudo apt install openssh-server vsftpd telnetd -y

Service yang berjalan:

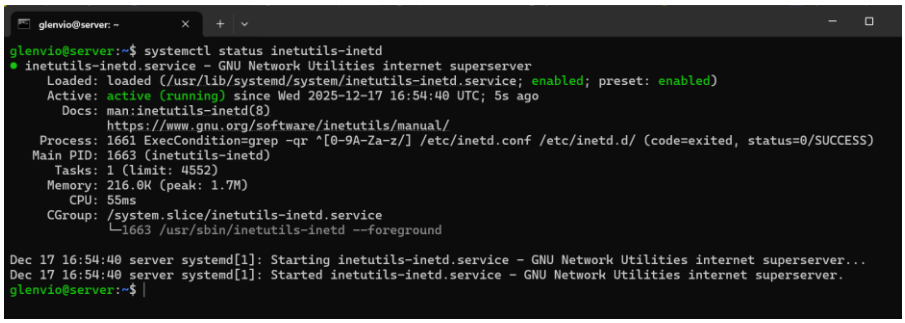
- SSH



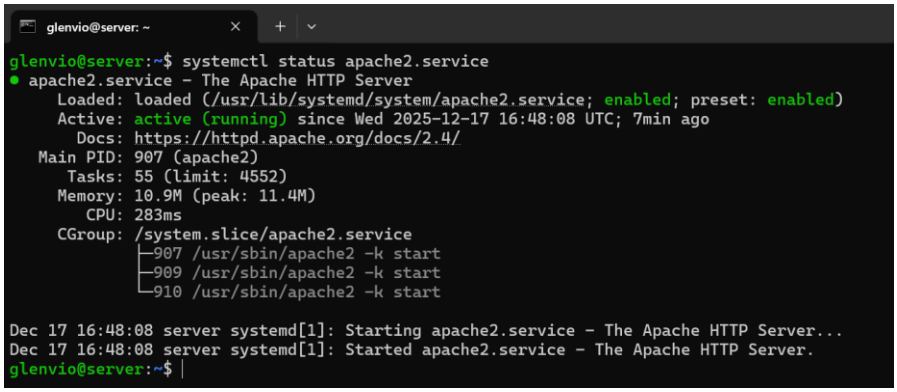
- FTP



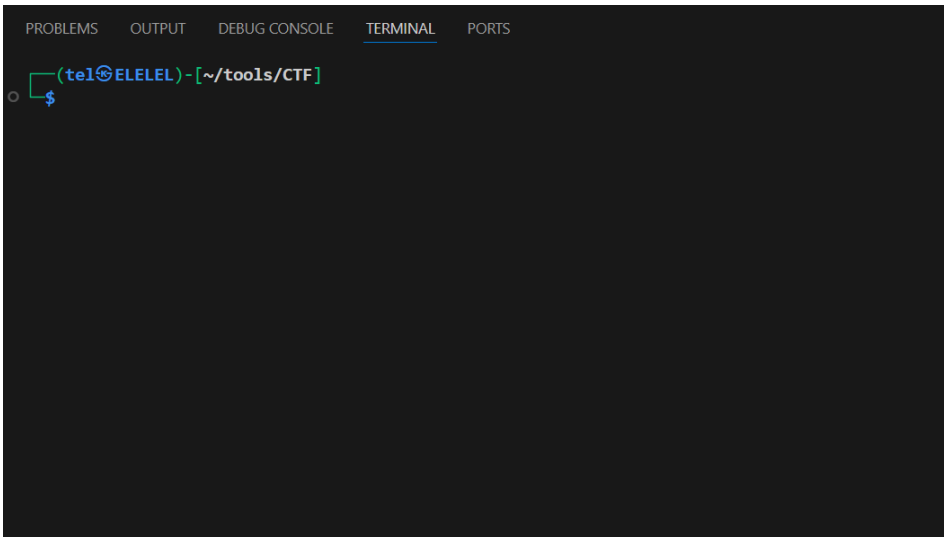
- Telnet



- Apache (HTTP/HTTPS)

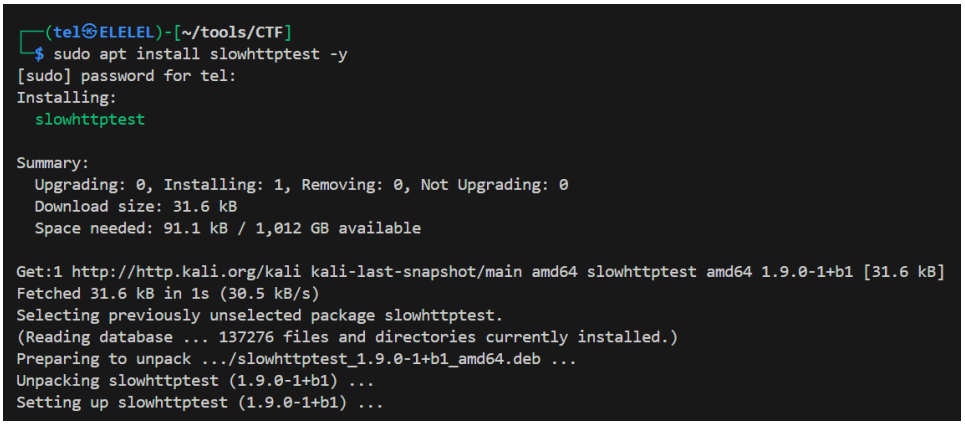


5. Persiapan Kali Linux (Penyerang)



5.1 Instalasi Tool Serangan

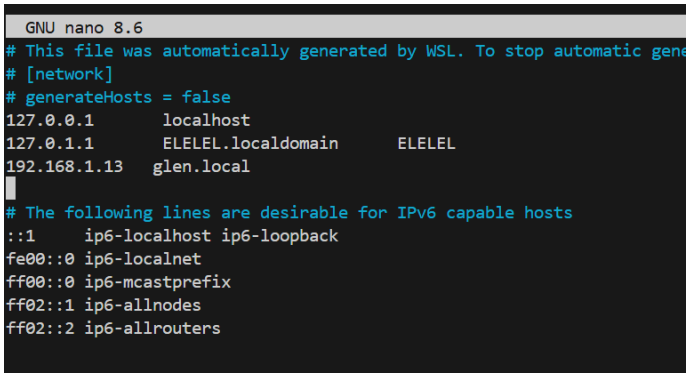
sudo apt install slowhttptest -y



5.2 Konfigurasi Hosts

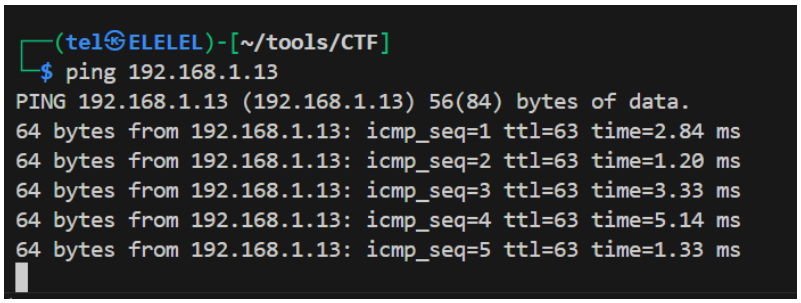
sudo nano /etc/hosts

Menambahkan IP Ubuntu Server agar dapat diakses melalui domain lokal.



5.3 Pengujian Koneksi

ping ip_ubuntu_server



---

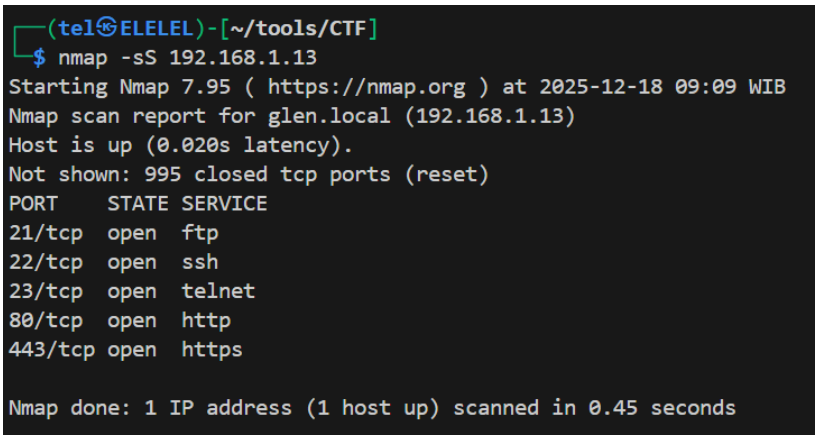
6. Tahap Penyerangan (Before IPTables)

6.1 Scanning Port

nmap -sS ip_ubuntu_server

Port yang terbuka:

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

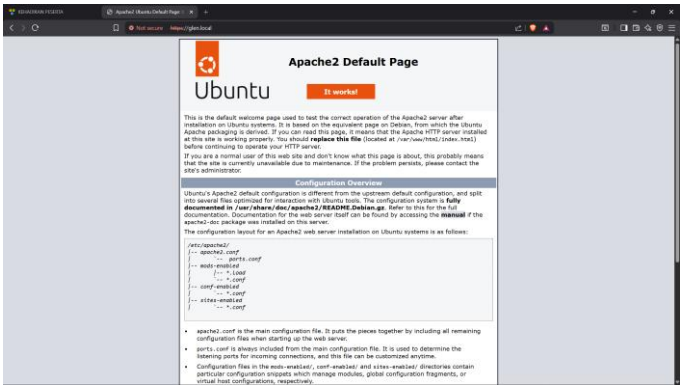


6.2 Simulasi Serangan DDoS

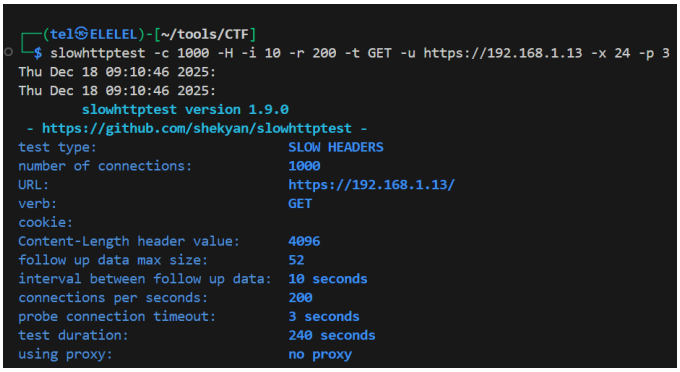
slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://ip_ubuntu_server -x 24 -p 3

Hasil:

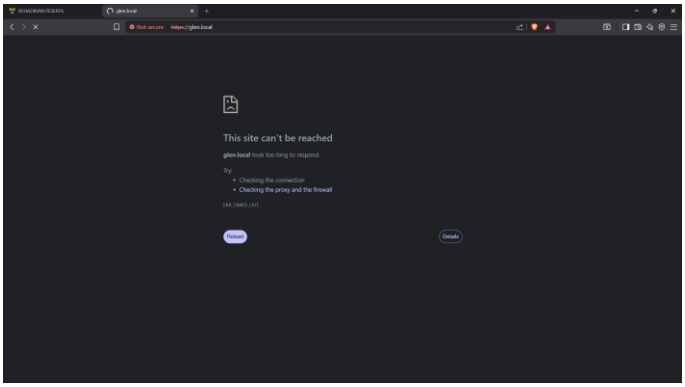
- Server melambat
- Apache mengalami peningkatan request
- Respon web tidak stabil



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



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)

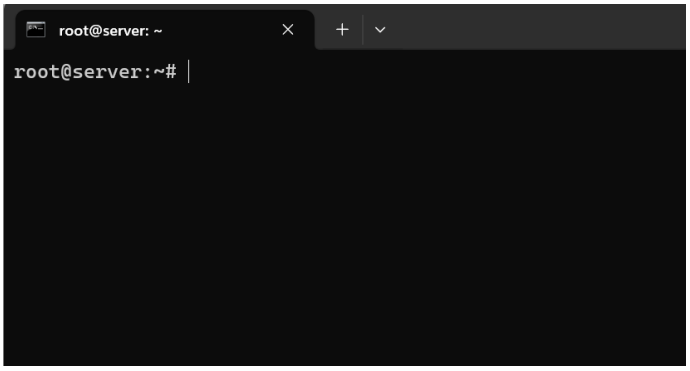
Pada tahap ini dilakukan konfigurasi firewall menggunakan IPTables untuk meningkatkan keamanan server terhadap serangan DDoS. Konfigurasi ini diterapkan setelah dilakukan simulasi serangan, di mana server mengalami penurunan performa akibat banyaknya koneksi yang masuk secara bersamaan. Dengan penerapan 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



Lalu jalankan rule berikut **berurutan**:

iptables -F

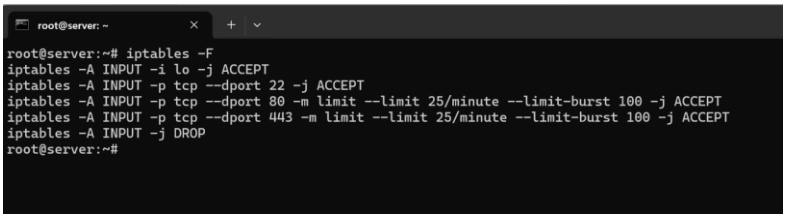
iptables -A INPUT -i lo -j ACCEPT

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

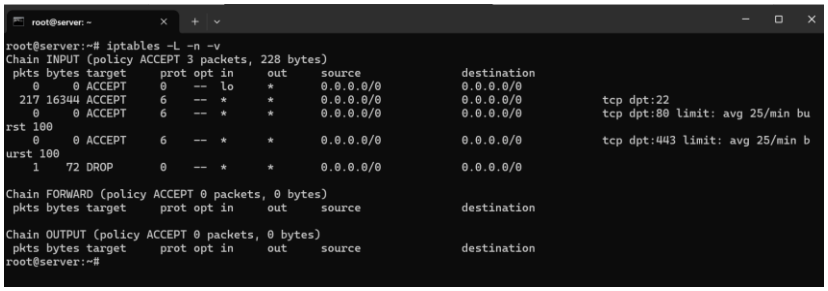
iptables -A INPUT -p tcp --dport 443 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

iptables -A INPUT -j DROP



7.2 Cek Rule

iptables -L -n -v



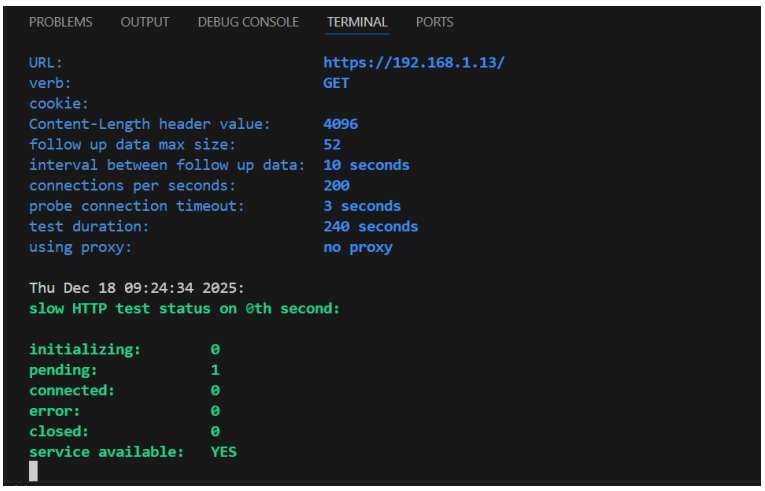
Penerapan rule IPTables dilakukan untuk meningkatkan keamanan server setelah dilakukan simulasi serangan DDoS. Tujuan utama dari konfigurasi ini adalah membatasi lalu lintas

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

---

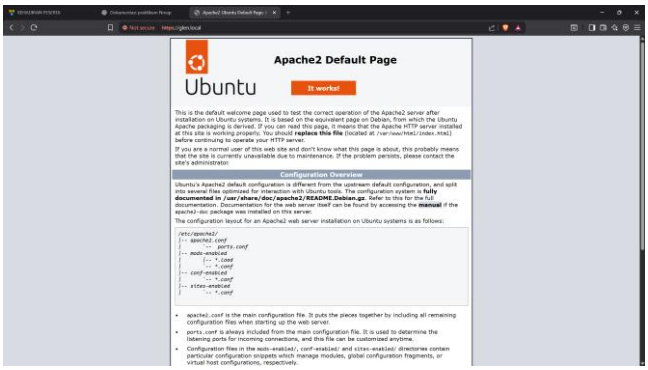
8. Tahap Penyerangan (After IPTables)

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



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.