LAPORAN ADVANCE NETWORK SECURITY AND PROTOCOLS

Simulasi Serangan Denial of Service dan langkah mitigasi dengan firewall

DISUSUN OLEH :

NAMA : NUR ALIYAH AMALIANI

KELAS : 5 JK-B

NIM : 105841106923

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

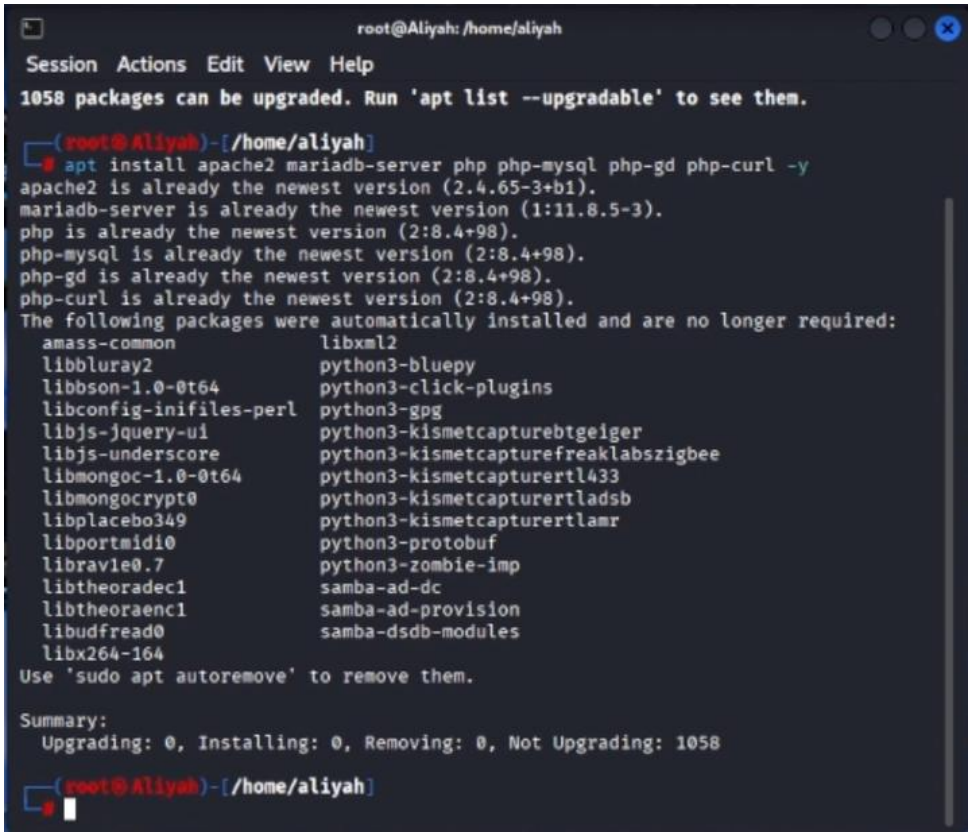
2025

1. DVWA Installation

a. Memperbarui Repositori System

Langkah pertama, masuk sebagai supepuser menggunakan perinta sudo su. Setelah mendapatkan akses root, jalankan perintah apt update untuk memperbarui daftar paket dari repositori. Hal ini memastikan kita mendapatkan versi terbaru dari perangkat lunak yang akan diinstall

b. Instalasi Web Server dan Database



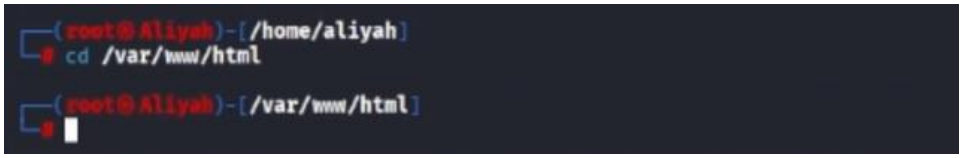
Selanjutnya, kita menginstall komponen utama server yang dibutuhkan oleh DVWA atau Damn Vurnerable Web Aplication.

Perintah apt install apache2 mariadb-server php php-myssql php-gd php-curl -y digunakan untuk memasang Apache sebagai web server, MariaDB sebagai Database, serta PHP beserta modul-modul pendukungnya.

c. Menjalankan dan mengaktifkan Apache2 dan MariaDB

Setelah instalasi selesai, layanan Apache dan MariaDB harus dijalankan. Perintah systemctl start digunakan untuk menjalankan layanan ini, sementara systemctl enable untuk memastikan bahwa kedua layanan tersebut akan berjalan otomatis setiap kali linux melakukan proses booting.

d. Berpindah ke direktori web Root



Sebelum mengunduh source code aplikasi, kita harus berpindah ke direktori kerja web server apache terlebih dahulu. Dengan menggunakan perintah cd /var/www/html agar file aplikasi nantinya tersimpan di lokal yang bisa diakses oleh browser.

e. Mengunduh Source code DVWA via Git

Di dalam direktori /var/www/html, dijalankan perintah git clone https://github.com/digininja/DVWA.git. Perintah ini akan menyalin seluruh folder aplikasi DVWA dari repositori GitHub ke dalam server lokal kita

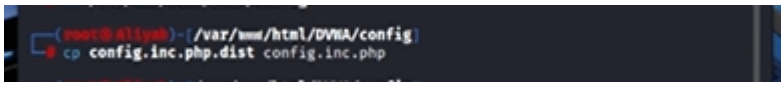
f. Mengatur Hak Akses Direktori

Langkah selanjutnya adalah memberikan izin akses penuh pada folder DVWA dengan perintah chmod -R 777 /var/www/html/DVWA. Hal ini dilakukan agar aplikasi memiliki izin untuk menuliskan file konfigurasi atau mengunggah data selama proses pengaturan awal browser nantinya.

g. Masuk ke Direktori Konfigurasi

Setelah mengunduh file aplikasi, kita perlu masuk ke folder konfigurasi untuk mengatur koneksi database. Gunakan perintah cd /var/www/html/DVWA/config untuk berpindah ke direktori tempat file pengaturan berada

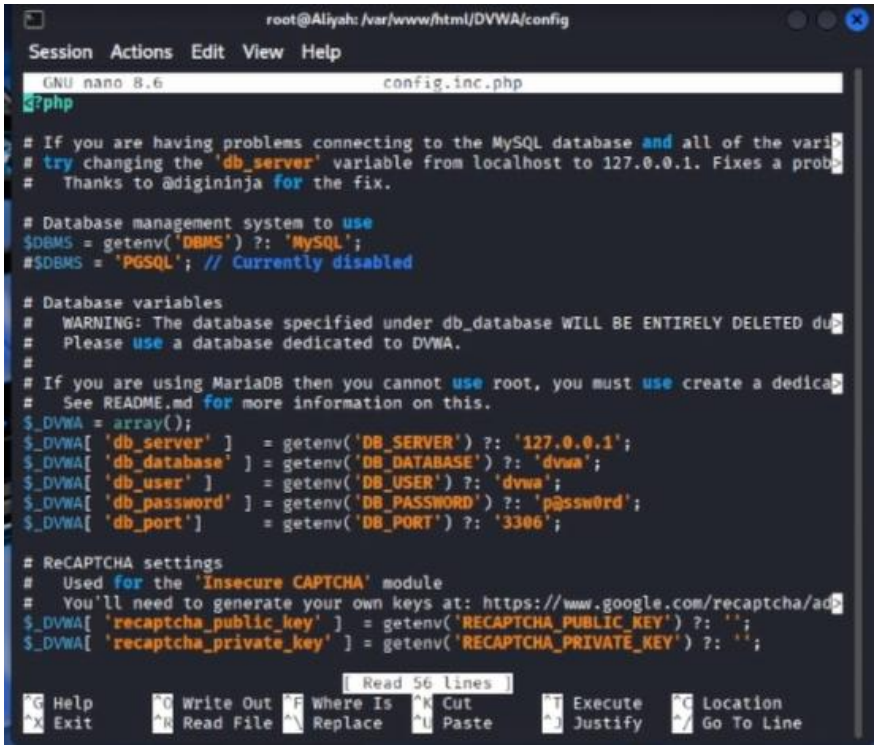
h. Menyalin File Konfigurasi Default



DVWA menyediakan file contoh konfigurasi bernama config.inc.php.dist. Kita harus menyalinnya menjadi file aktif dengan perintah cp config.inc.php.dist config.inc.php. File baru inilah yang nantinya akan kita edit.

i. Mengedit File Konfigurasi

Gunakan editor teks nano dengan perintah nano config.inc.php untuk membuka file pengaturan.

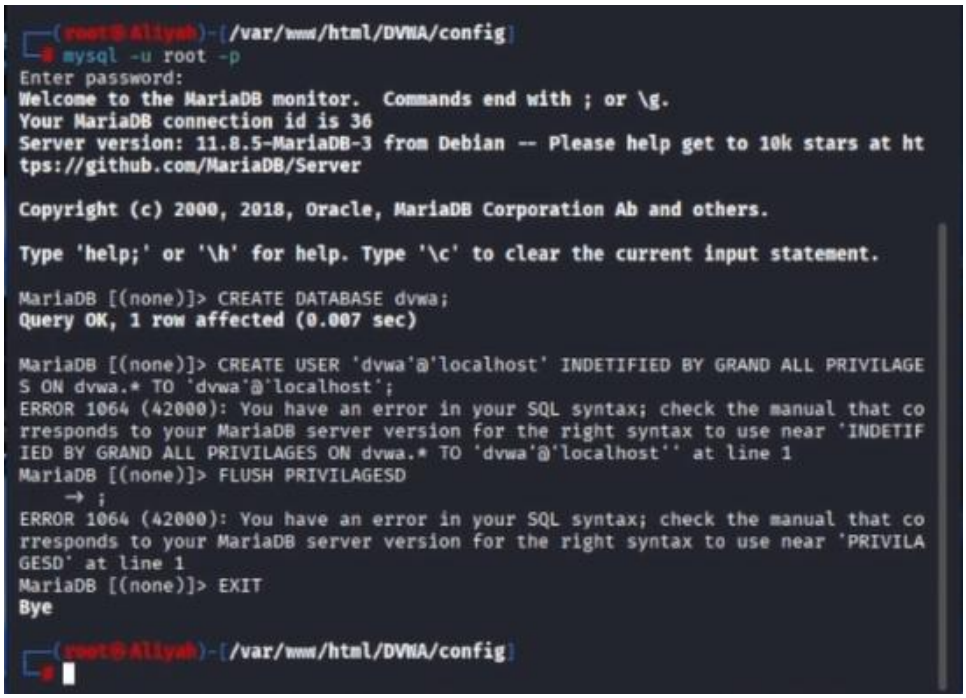


Di dalam editor, cari bagian Database variables. Pastikan nilai db_user diatur menjadi dvwa dan db_password diatur menjadi password yang Anda tentukan (dalam contoh ini terlihat

p@ssw0rd). Jangan lupa ubah db_server ke 127.0.0.1 jika terjadi kendala koneksi.

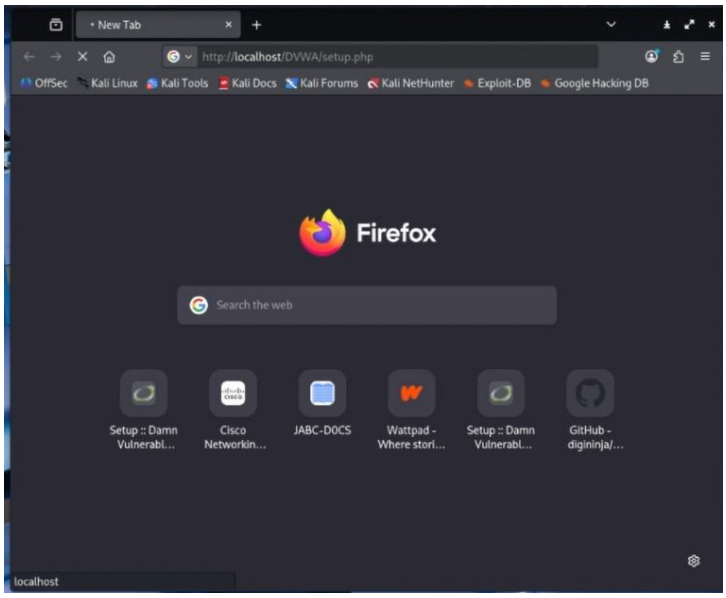
Pada file yang sama, scroll ke bawah hingga menemukan default_security_level. Untuk pemula, ubah nilainya dari impossible menjadi low. Ini akan memudahkan kita dalam mempelajari teknik eksploitasi dasar tanpa proteksi yang terlalu ketat.

j. Membuat Database di MariaDB



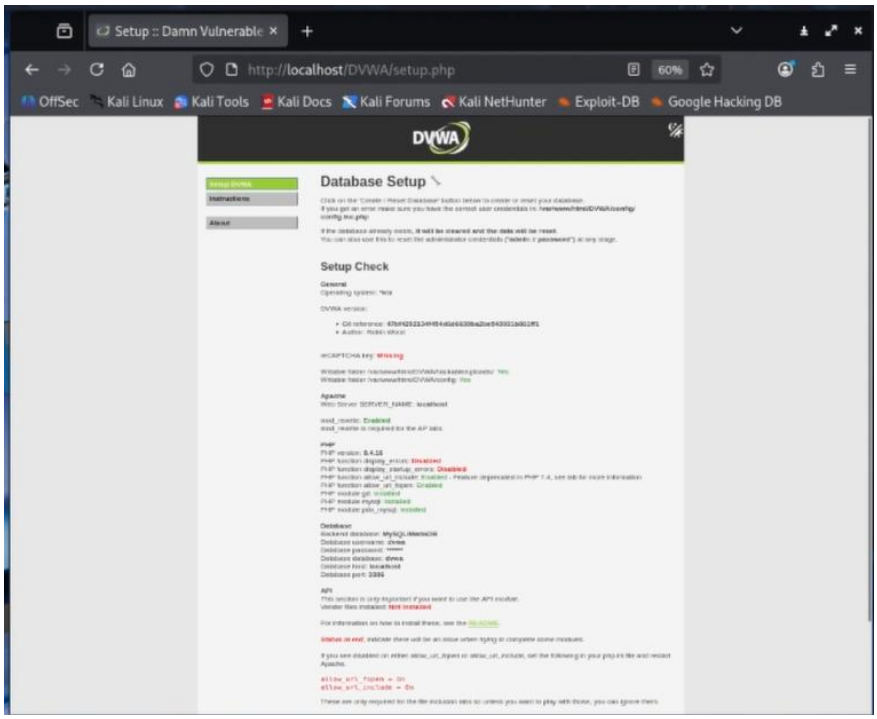
Langkah ini sangat krusial. Kita masuk ke shell database dengan perintah mysql -u root -p. Di dalamnya, kita menjalankan perintah CREATE DATABASE dvwa; untuk membuat wadah data.

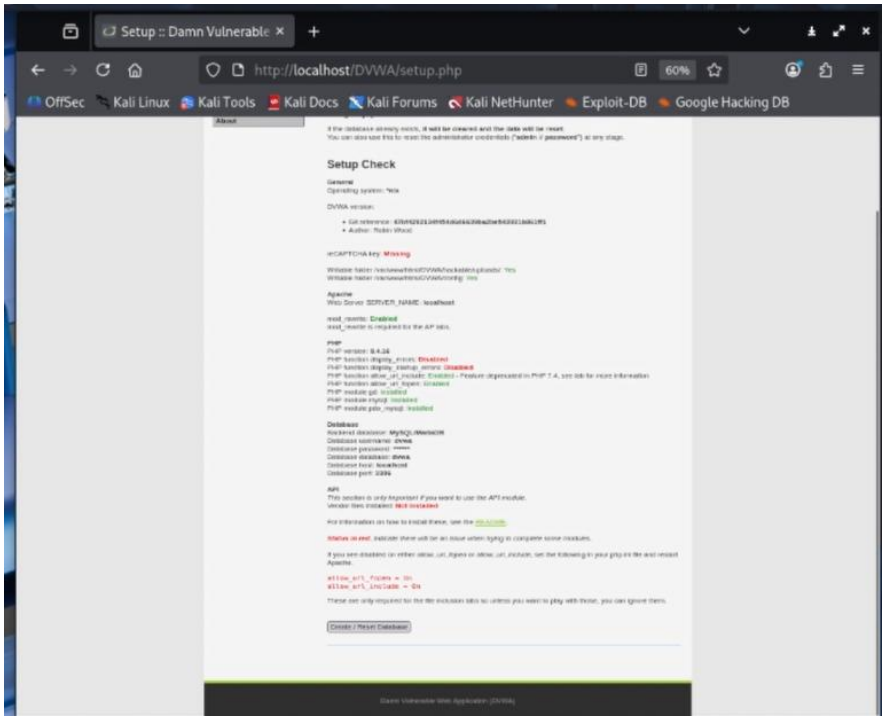
k. Mengakses DVWA melalui Browser



Buka browser Firefox dan ketikkan alamat http://localhost/DVWA/setup.php. Alamat ini akan mengarahkan Anda ke halaman pemeriksaan sistem untuk memastikan semua prasyarat instalasi telah terpenuhi.

l. Melakukan Setup Check dan Reset Database



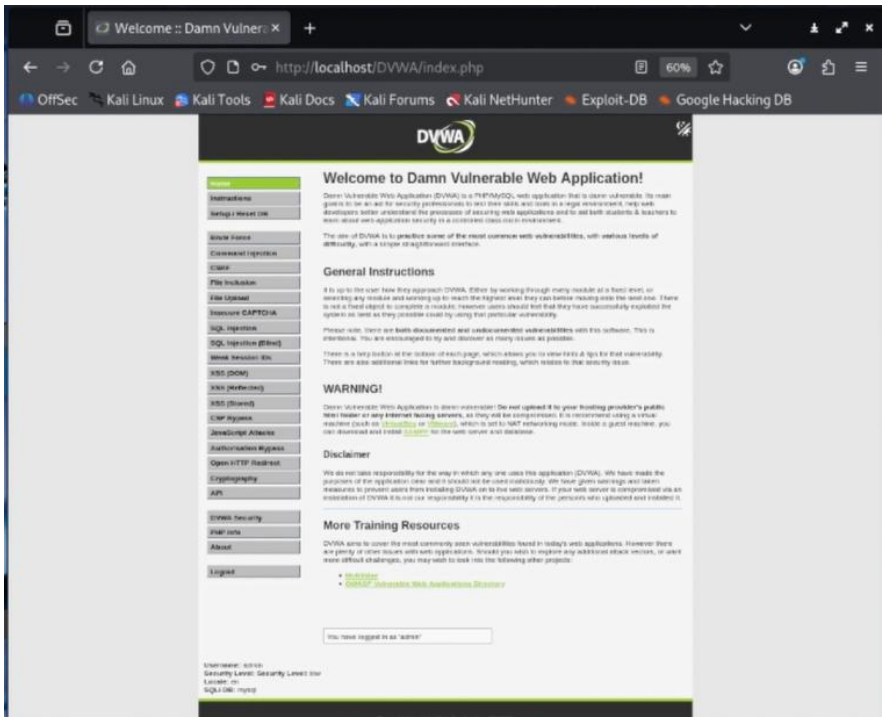


Halaman ini menampilkan status sistem. Periksa apakah variabel database sudah berwarna hijau (berhasil terhubung). Jika sudah yakin, klik tombol "Create / Reset Database" di bagian bawah halaman untuk membuat tabel-tabel yang diperlukan secara otomatis.

m. Halaman Login Aplikasi

Setelah database berhasil dibuat, Anda akan dialihkan ke halaman login. Masukkan username default yaitu admin dan

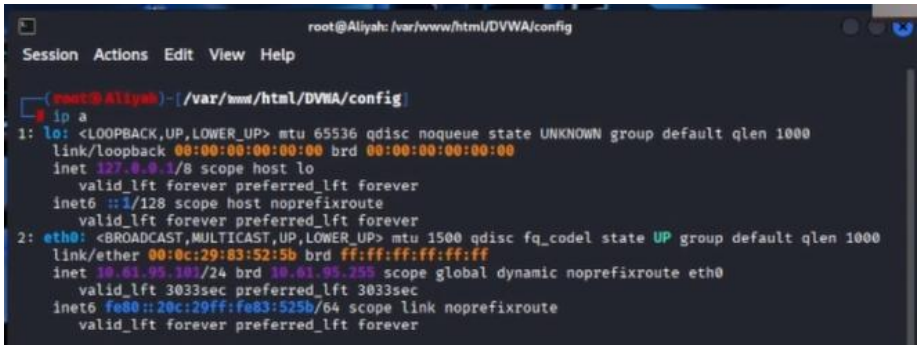
password default yaitu password. Klik **Login** untuk masuk ke dashboard utama.

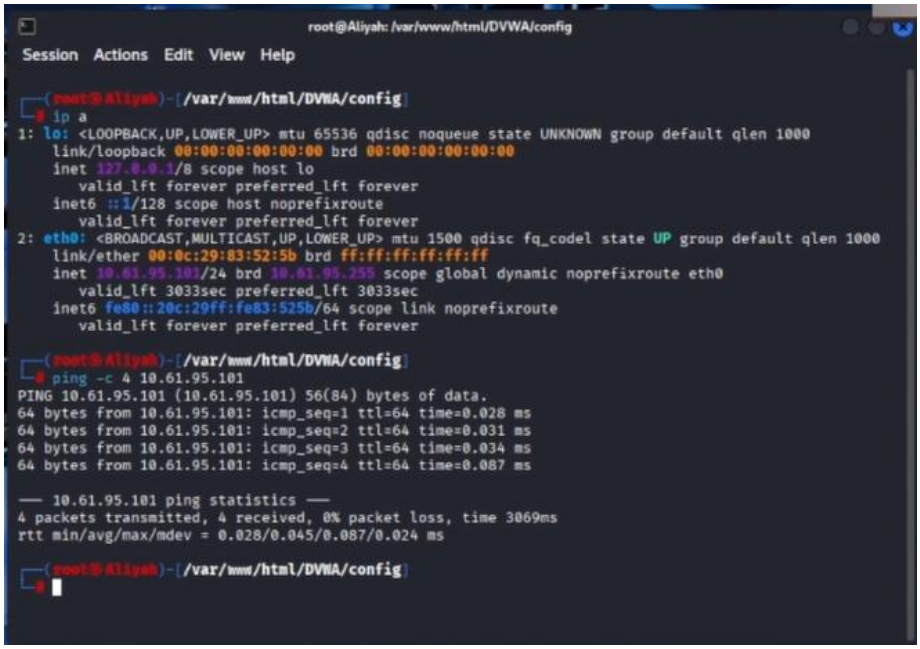


Pada bagian DVWA Security ubah menjadi LOW, agar security atau keamanya rendah.

2. Pengecekah Koneksi antar mesin virtual

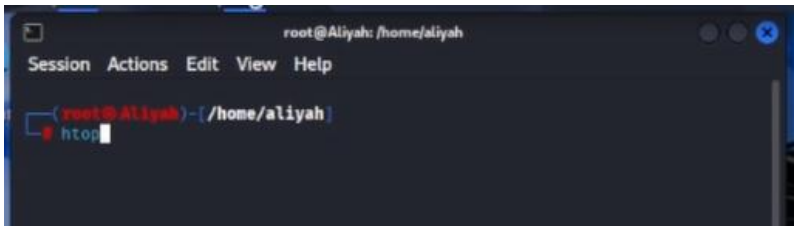
a. Mengecek Alamat IP Sistem





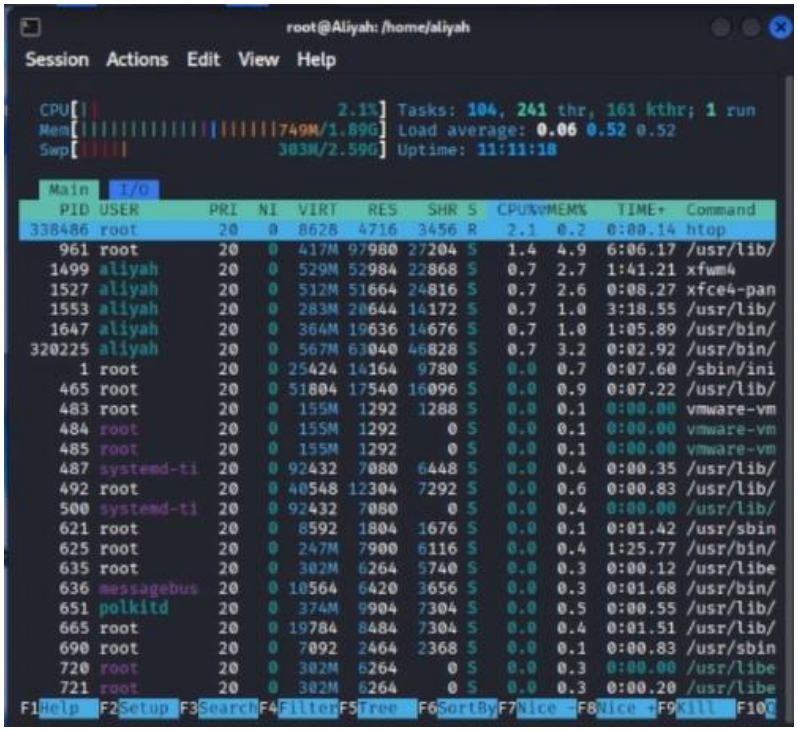
Setelah instalasi selesai, kita perlu mengetahui alamat IP lokal mesin tersebut agar bisa diakses oleh perangkat lain dalam jaringan yang sama. Perintah ip a digunakan untuk menampilkan informasi antarmuka jaringan. Terlihat pada gambar, mesin memiliki alamat IP 10.61.95.101 pada antarmuka eth0. Untuk memastikan konektivitas internal stabil, dilakukan pengujian ping ke alamat IP tersebut.

b. Membuka Monitor Proses Sistem di terminal target



Untuk memastikan server berjalan dengan lancar tanpa membebani sumber daya secara berlebihan, kita bisa memantau aktivitas sistem secara *real-time*. Perintah yang digunakan adalah htop, sebuah alat monitor sistem interaktif yang lebih informatif dibanding perintah top standar.

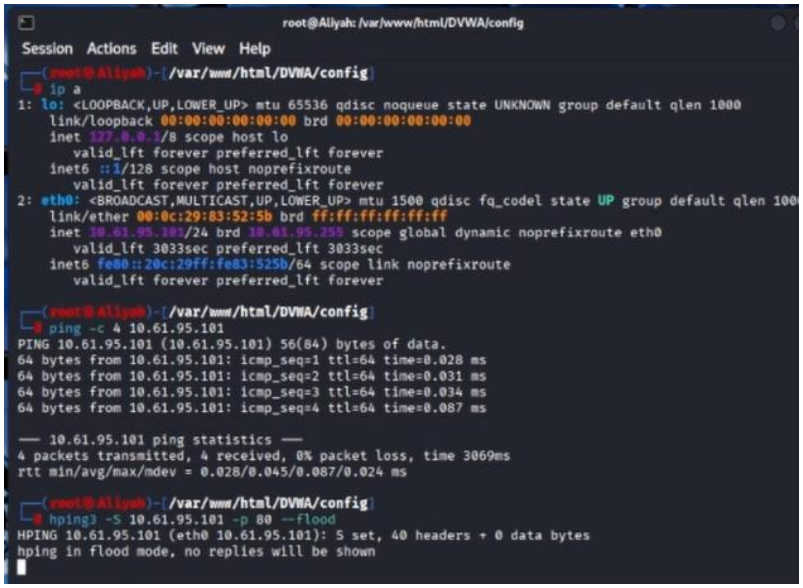
c. Memantau Penggunaan Sumber Daya (CPU & RAM)



Melalui tampilan htop, kita dapat melihat persentase penggunaan CPU, memori (RAM), serta daftar proses yang sedang berjalan. Ini sangat berguna untuk memastikan layanan Apache dan MariaDB tidak menggunakan memori secara

abnormal setelah aplikasi DVWA mulai digunakan untuk pengujian keamanan.

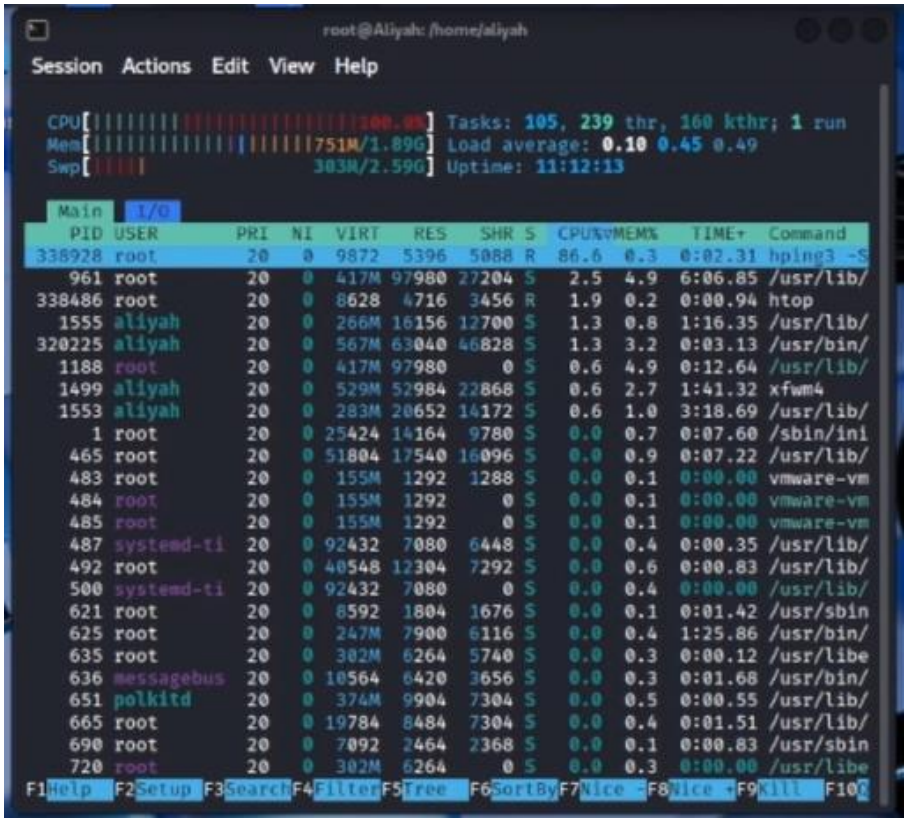
3. **Simulasi serangan Denial Of Service**



Setelah memastikan konektivitas jaringan stabil melalui perintah ping ke alamat IP 10.61.95.101, dilakukan pengujian penetrasi lebih lanjut menggunakan alat hping3. Perintah hping3 -S 10.61.95.101 -p 80 --flood dijalankan untuk mensimulasikan serangan SYN Flood. Dalam mode ini, sistem akan mengirimkan paket SYN (permintaan koneksi) secara terus-menerus ke port 80 (HTTP) tanpa menunggu jawaban, yang bertujuan untuk menguji ketahanan web server Apache dalam menangani beban trafik yang ekstrem.

4. **Monitoring penggunaan Resource pada mesin target terhadap serangan DoS**

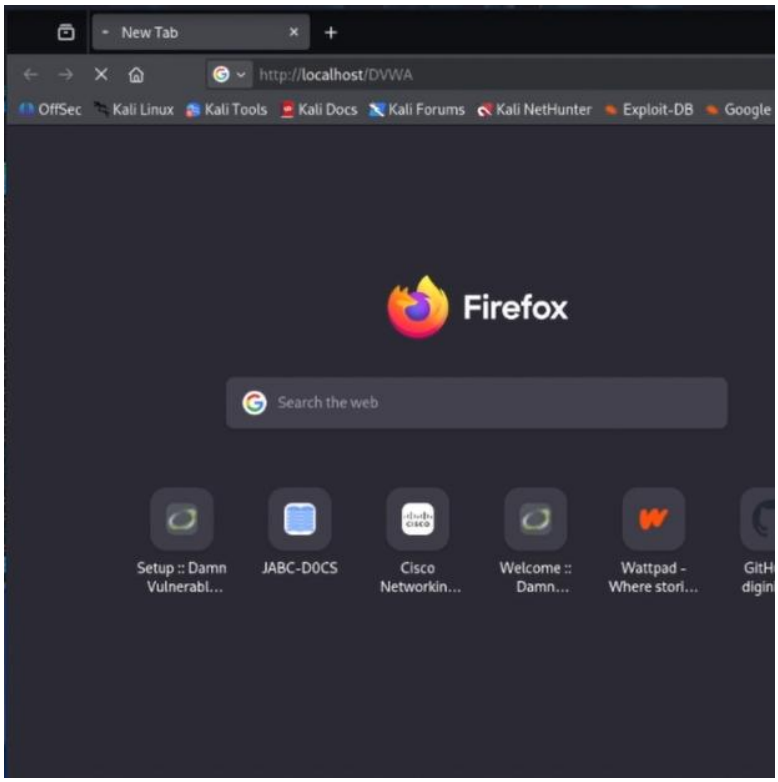
   a. Monitoring Lonjakan Beban CPU (100%)



Segera setelah serangan diluncurkan, alat monitoring htop menunjukkan dampak yang drastis. Indikator bar CPU berubah menjadi warna merah penuh dan mencapai nilai 100.0%. Hal ini membuktikan bahwa proses hping3 (PID 338928) telah memakan seluruh daya komputasi yang tersedia, yang merupakan ciri khas dari serangan *Resource Exhaustion*.

Pada tabel proses di bawahnya, kita dapat melihat secara detail bahwa proses hping3 mendominasi baris teratas dengan penggunaan CPU sebesar 86.6%. Monitoring ini sangat penting untuk membedakan antara penggunaan sumber daya yang normal dengan penggunaan yang mencurigakan (anomali) akibat aktivitas berbahaya di jaringan.

b. Pengujian Akses layanan Web

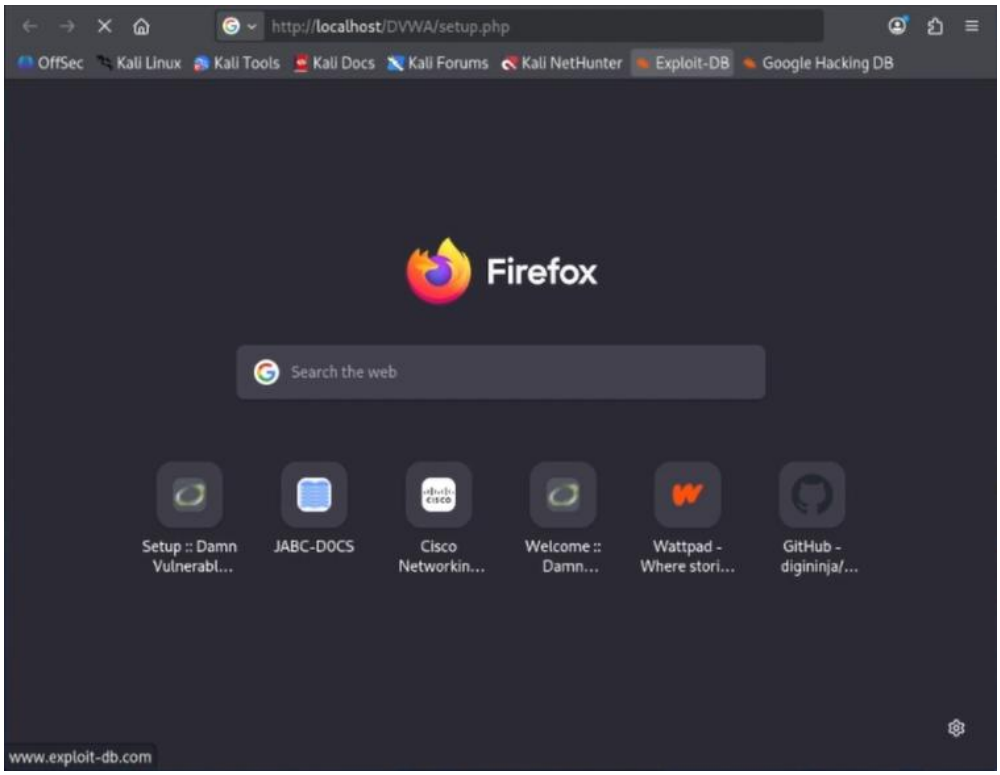


Langkah terakhir dalam monitoring ini adalah mencoba mengakses kembali alamat http://localhost/DVWA melalui browser selama serangan berlangsung. Biasanya, akibat beban CPU yang mencapai 100%, server akan menjadi sangat lambat atau bahkan gagal merespons sama sekali (*Service Unavailable*). Ini menunjukkan bahwa serangan *Denial of Service* (DoS) tersebut berhasil melumpuhkan ketersediaan layanan aplikasi web.

5. Simulasi Serangan Slowloris

Setelah pengujian dengan paket SYN, dilakukan simulasi serangan Layer 7 menggunakan alat **S**lowloris dengan perintah slowloris 10.61.95.101. Berbeda dengan *flooding* paket, Slowloris bekerja dengan membuka banyak koneksi ke web server dan menahannya selama mungkin dengan mengirimkan header HTTP yang tidak lengkap secara berkala. Terlihat pada terminal, sistem mulai membuat 150 *sockets* untuk mengikat koneksi pada server target

6. **Melakukan monitoring terhadap web server**

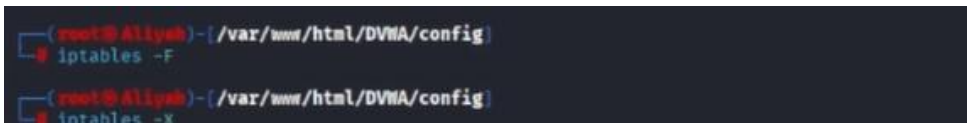


Monitoring selanjutnya adalah memverifikasi kembali ketersediaan layanan web melalui Firefox. Kita mengakses http://localhost/DVWA/setup.php untuk memastikan bahwa web server Apache kembali responsif dan mampu melayani permintaan

HTTP secara normal setelah sebelumnya sempat lumpuh akibat beban serangan.

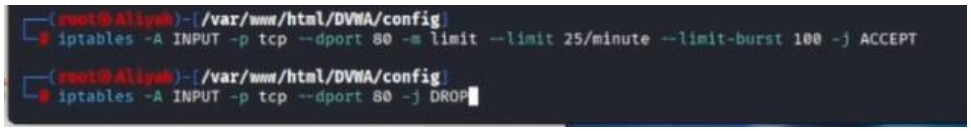
7. **Melakukan mitigasi menggunakan firewall**

   a. Pembersihan Aturan Firewall (Flush)



   Sebelum menerapkan aturan keamanan baru, administrator melakukan pembersihan total pada tabel firewall. Perintah iptables -F digunakan untuk menghapus semua aturan yang ada, dan iptables -X digunakan untuk menghapus rantai (chain) tambahan buatan pengguna. Hal ini dilakukan untuk memastikan tidak ada konflik antar aturan lama dengan aturan baru yang akan diterapkan.

   b. Mitigasi Serangan



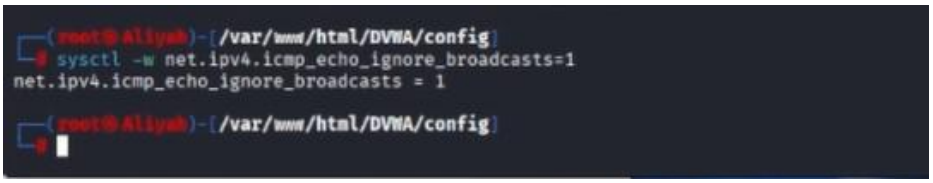
   Untuk melindungi web server dari serangan banjir koneksi pada port 80, diterapkan aturan pembatasan laju (*rate limiting*) pada protokol TCP. Perintah iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT dijalankan untuk memberikan toleransi sebanyak 100 koneksi awal (*burst*), kemudian membatasi koneksi baru berikutnya hanya 25 koneksi per menit. Hal ini secara efektif mencegah serangan *SYN Flood* atau *TCP Exhaustion* agar tidak menghabiskan sumber daya server.

Setelah ambang batas koneksi TCP yang diizinkan tercapai, sisa paket yang masuk harus ditangani agar tidak membebani sistem. Perintah iptables -A INPUT -p tcp --dport 80 -j DROP diterapkan untuk secara otomatis membuang (*drop*) semua paket TCP pada port 80 yang tidak memenuhi kriteria limit sebelumnya. Dengan aturan ini, server tetap dapat melayani pengguna sah secara terbatas sementara trafik serangan diblokir sepenuhnya oleh firewall.

c. Membatasi laju paket ICMP via IPTables

Untuk mencegah banjir paket ping, diterapkan aturan pembatasan (rate limiting). Perintah iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/second -j ACCEPT memungkinkan hanya satu paket ping per detik yang diterima. Sisanya akan dibuang melalui perintah iptables -A INPUT -p icmp --icmp-type echo-request -j DROP, sehingga server tetap dapat diping namun tidak bisa dilumpuhkan oleh serangan banjir ICMP.

d. Mitigasi Serangan ICMP (Ping) FLood



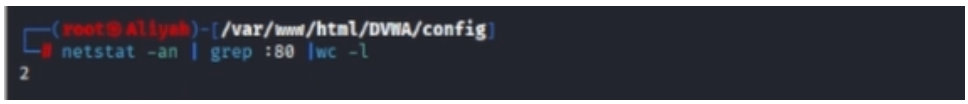
Salah satu cara untuk mengamankan server dari deteksi dan serangan berbasis ICMP adalah dengan mengabaikan permintaan broadcast. Perintah sysctl -w

net.ipv4.icmp_echo_ignore_broadcasts=1 dijalankan untuk memerintahkan kernel Linux agar tidak menanggapi pesan ping yang dikirim ke alamat broadcast jaringan, guna mencegah serangan *smurf*.

e. Memverifikasi Status Aturan Firewall

Setelah semua aturan diterapkan, perintah iptables -L -v -n dijalankan untuk melihat daftar aturan aktif secara mendetail. Terminal menunjukkan bahwa rantai INPUT kini telah memiliki kebijakan pembatasan untuk protokol TCP (port 80) dan ICMP. Kolom pkts dan bytes akan mencatat setiap paket yang diblokir oleh sistem keamanan ini secara *real-time*.

f. Monitoring Koneksi Aktif (Netstat)



Terakhir, perintah netstat -an | grep :80 | wc -l digunakan untuk menghitung jumlah koneksi aktif pada port web (80). Hasil angka 2 pada terminal menunjukkan bahwa jumlah koneksi kini sangat terkendali, menandakan bahwa web server tidak lagi dibanjiri oleh ribuan koneksi palsu dan siap melayani pengguna sah kembali dengan aman.