ADVANCED NETWORK SECURITY AND PROTOCOLS

Simulasi Denial of Service (DOF) Attack dengan Hping3 dan Mitigasi Firewall

Disusun Oleh:

NAMA : SUKMA WARDIA NINGSIH

NIM : (105841112723)

KELAS : 5-JK B

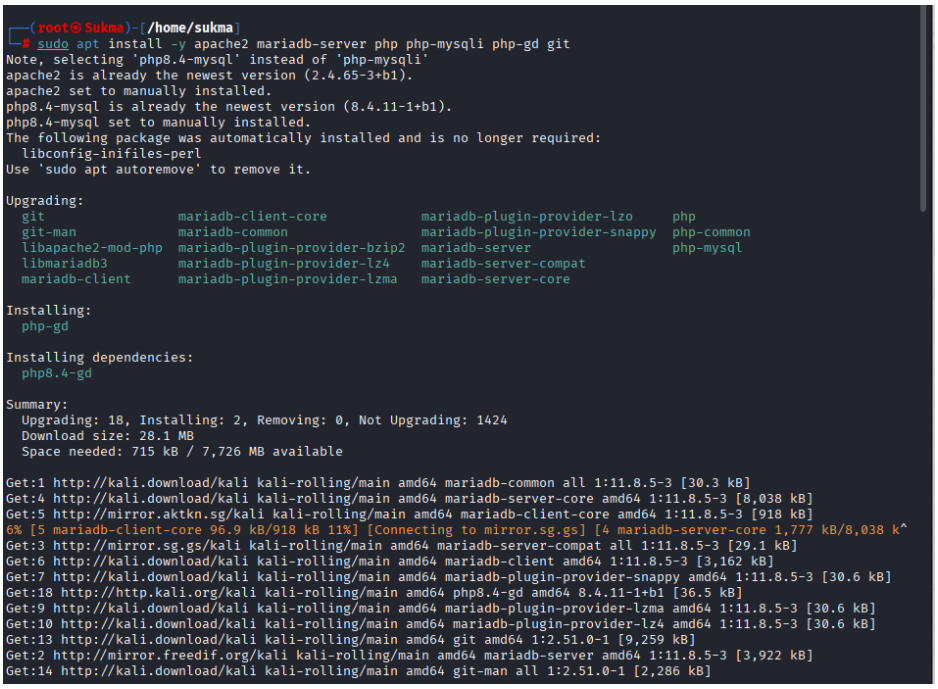
PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

A. Download dan Setup awal

1. Instalasi DVWA di target VM



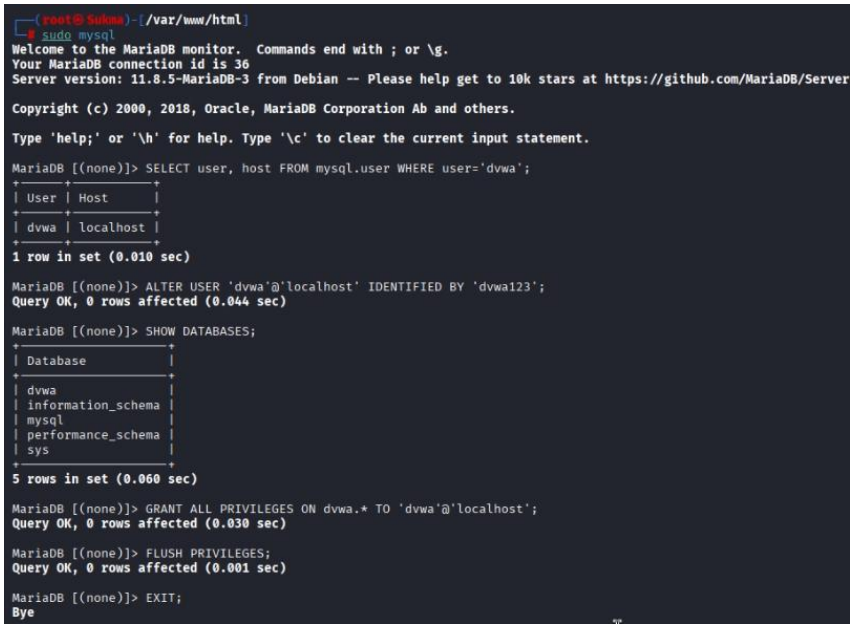
sudo apt update
sudo apt install -y apache2 mariadb-server php php-mysqli php-gd git
Perintah ini memperbarui repositori dan memasang Apache, MariaDB, PHP, dan git.

cd /var/www/html memindahkan direktori kerja ke root dokumen default Apache, yaitu tempat file web disajikan.
sudo git clone https://github.com/digininja/DVWA.git
mendownload source code DVWA langsung dari GitHub ke dalam folder /var/www/html/DVWA

- *cd /var/www/html/DVWA* masuk ke direktori DVWA.
- *sudo chmod -R 777*. memberikan permission penuh (read, write, execute) ke semua user pada seluruh isi folder DVWA; ini memang tidak aman untuk production tetapi umum dipakai pada lab DVWA agar tidak ada masalah permission saat menulis file atau upload.
- *cd config* masuk ke direktori konfigurasi DVWA.
- *sudo cp config.inc.php.dist config.inc.php* menyalin file template konfigurasi menjadi file konfigurasi aktif yang akan diedit.

2. Setup database

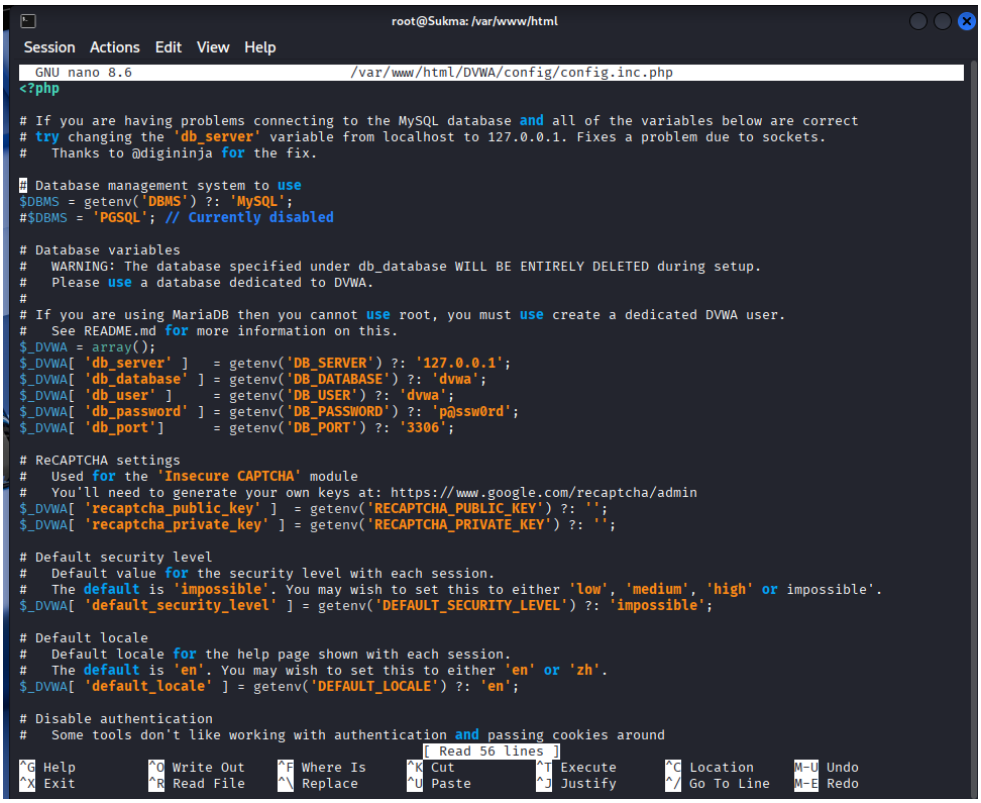
```bash
sudo systemctl start mariadb
sudo mysql <<EOF
CREATE DATABASE dvwa;
CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'dvwa123';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
FLUSH PRIVILEGES;
EXIT;
EOF
```



- sudo systemctl start mariadb menyalakan layanan database MariaDB sehingga dapat menerima koneksi.

- `sudo mysql <<EOF ... EOF` menjalankan beberapa perintah SQL sekaligus di dalam client MariaDB dengan hak root:
- CREATE DATABASE dvwa; membuat database baru bernama dvwa yang akan dipakai DVWA.
- CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'dvwa123'; membuat user database bernama dvwa dengan password dvwa123 yang hanya boleh login dari local machine.
- GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost'; memberikan semua hak akses (select, insert, update, dll.) pada database dvwa kepada user tersebut.
- FLUSH PRIVILEGES; memaksa MariaDB memuat ulang tabel hak akses sehingga perubahan segera berlaku.

3. Edit konfigurasi DVWA



sudo nano /var/www/html/DVWA/config/config.inc.php

Perintah ini membuka file konfigurasi DVWA di text editor nano agar parameter koneksi database dapat disesuaikan.

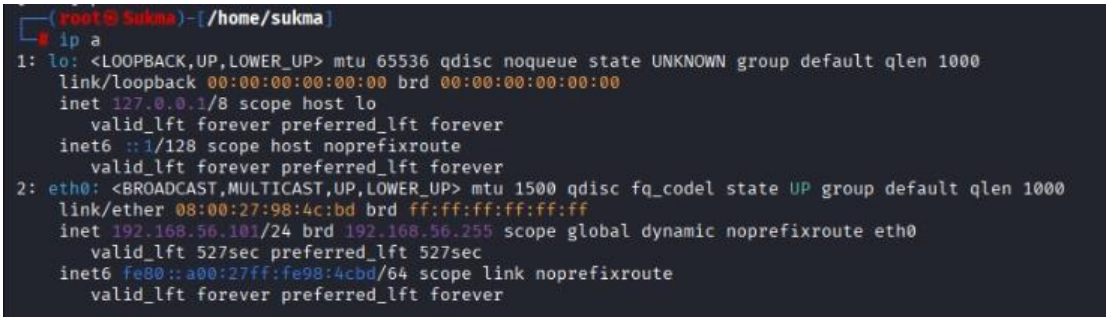
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'dvwa123';

Ini yang kita pakai untuk menggunakan database local dvwa dengan user dan password yang baru di buat.

4. Restart apache

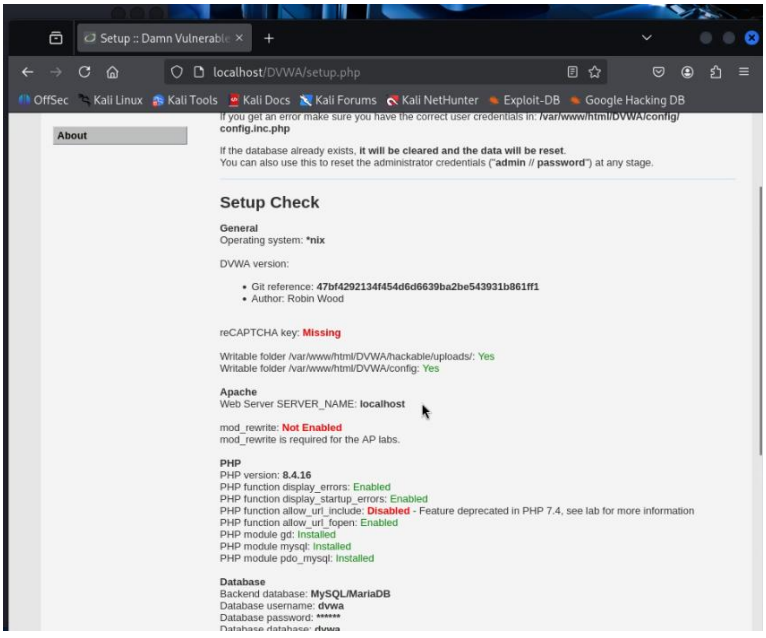
```
┌──(root㉿Sukma)-[/var/www/html]
└─# sudo systemctl restart apache2
sudo systemctl enable apache2

Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```

- *sudo systemctl restart apache2* me-restart layanan Apache sehingga meng-load konfigurasi baru dan mulai menyajikan DVWA.
- *sudo systemctl enable apache2* membuat Apache otomatis start setiap kali sistem boot, sehingga server web selalu aktif tanpa perlu start manual.



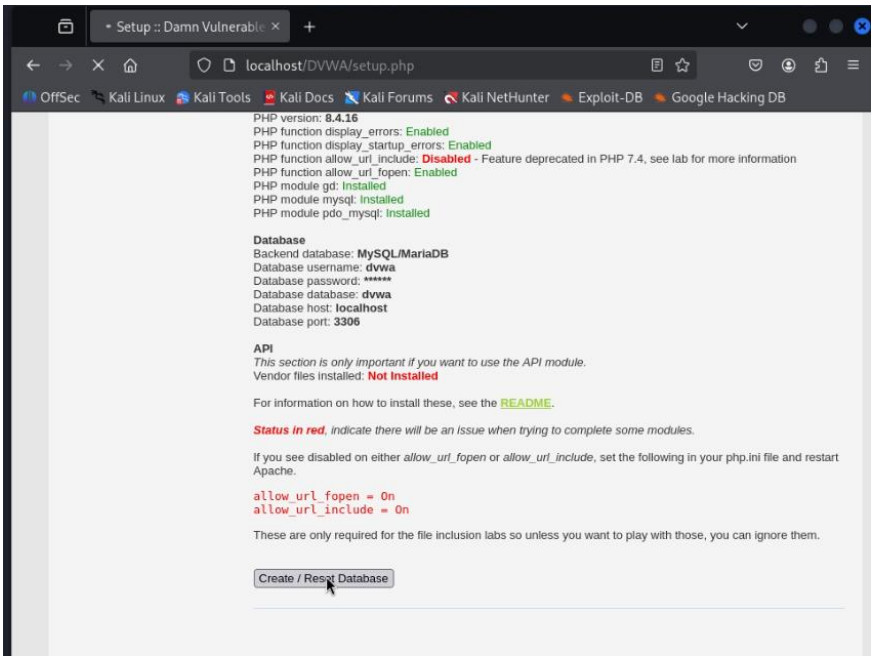
ip a digunakan untuk melihat alamat IP yang didapat pada setiap interface; di sini digunakan untuk memastikan attacker dan target berada di jaringan yang sama.

5. Setup DVWA via Web (Browser)

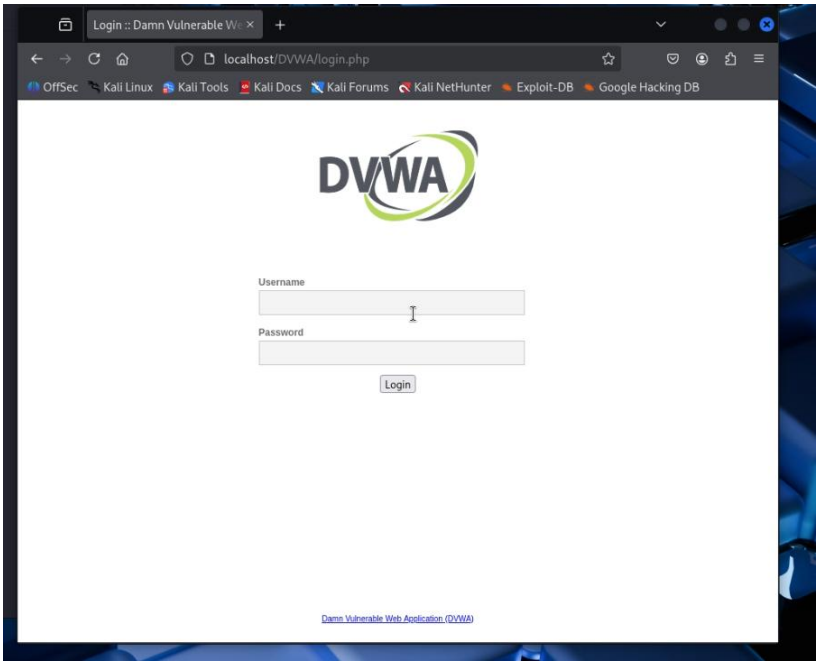


http://localhost/DVWA/setup.php **DVWA Setup Check** merupakan halaman awal yang digunakan untuk memastikan bahwa seluruh komponen yang

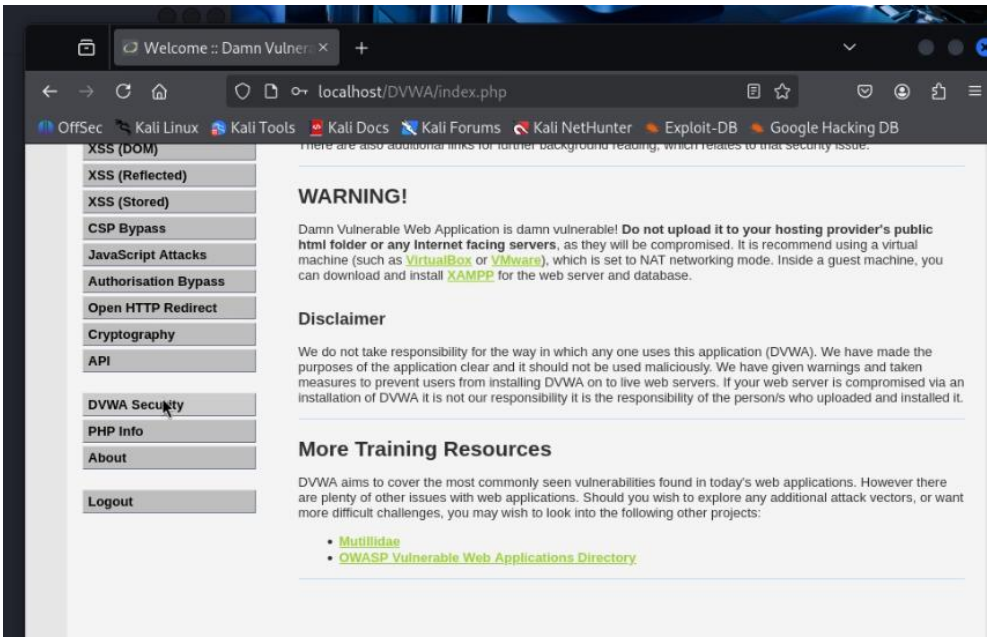
dibutuhkan oleh aplikasi **Damn Vulnerable Web Application (DVWA)** telah terpasang.



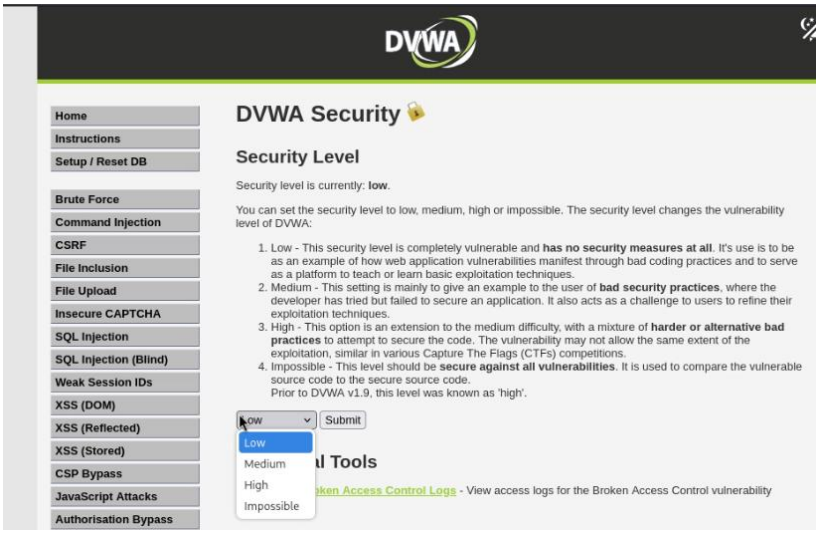
Masih di subbab yang sama, setelah langkah reset database sebelum login pertama.



Login sesuaikan dengan edit konfigurasi yang di ganti tadi, jika berhasil login berarti DvWA sudah bisa di akses.



Ini tampilan setelah berhasil masuk, setelah itu atur DvWA security



Lalu atur keamanan di level Low DVWA sebelum kamu mulai serangan DoS.

6. Port Scanning dengan Nmap

```
┌──(root㉿Sukma)-[/home/sukma]
└─# nmap -p 1-100 192.168.56.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-28 20:17 WITA
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0000090s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

- *nmap -p 1-100 192.168.56.101* adalah tool untuk scanning port dan deteksi service.
- Opsi -p 1-100 membatasi scanning pada port TCP 1 sampai 100.
- 80/tcp open http menunujukkan port 80 terbuka.

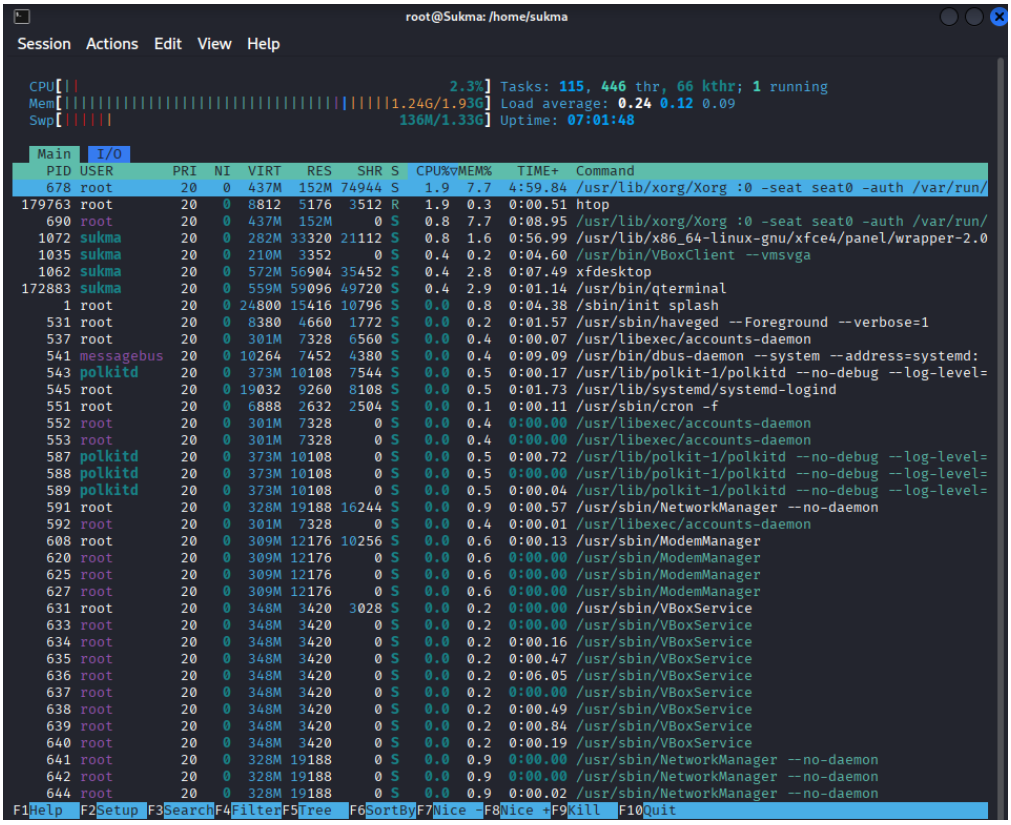
B. Eksekusi serangan DoS dengan HPING3

1. Monitoring baseline di target.

```
┌──(root㉿Sukma)-[/home/sukma]
└─# sudo apt install htop
The following package was automatically installed and is no longer required:
  libconfig-inifiles-perl
Use 'sudo apt autoremove' to remove it.

Installing:
  htop

Suggested packages:
  strace

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1429
  Download size: 171 kB
  Space needed: 434 kB / 7,630 MB available

Get:1 http://xsrv.moratelindo.io/kali kali-rolling/main amd64 htop amd64 3.4.1-5 [171 kB]
Fetched 171 kB in 2s (104 kB/s)
Selecting previously unselected package htop.
(Reading database ... 416683 files and directories currently installed.)
Preparing to unpack .../htop_3.4.1-5_amd64.deb ...
Unpacking htop (3.4.1-5) ...
Setting up htop (3.4.1-5) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for man-db (2.13.1-1) ...
```

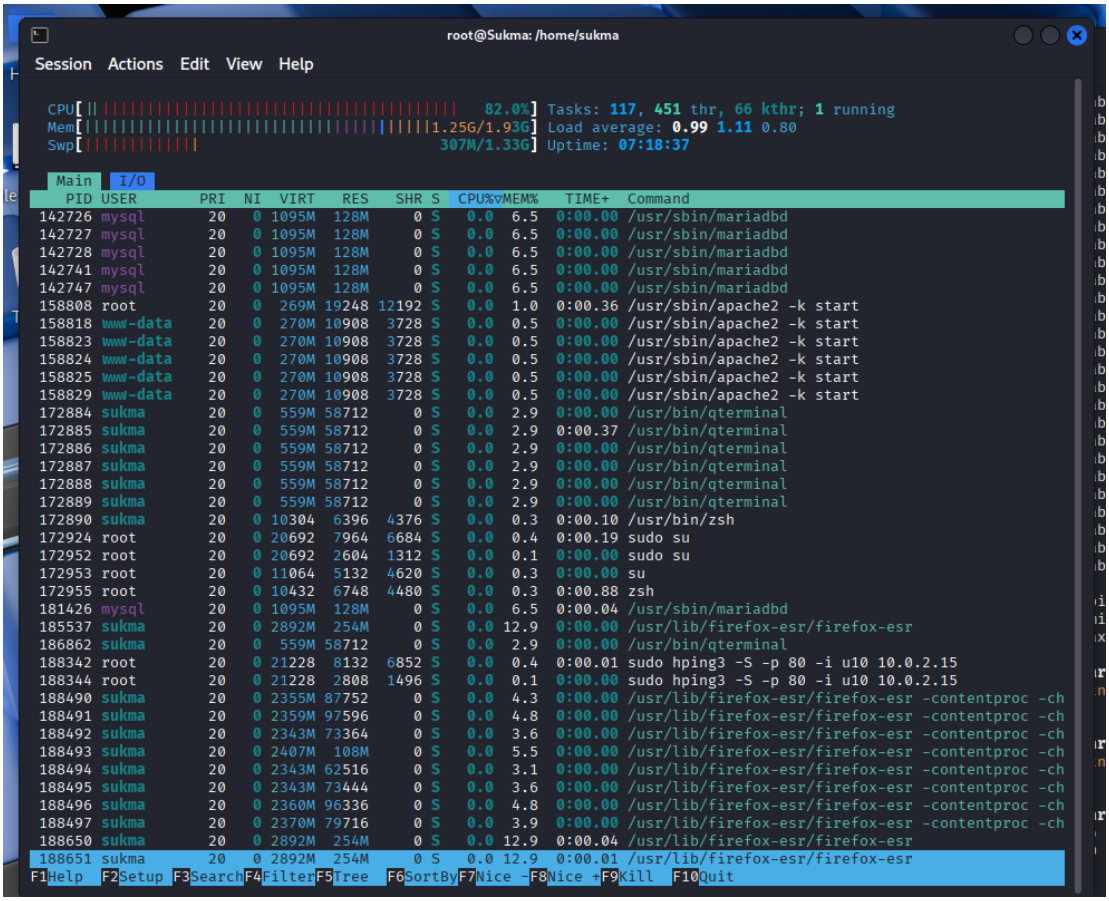
Melakukan pendownload tan terlebih dahulu jika dalam kali linux nya blm terdownload.

2. Melakukan Htop

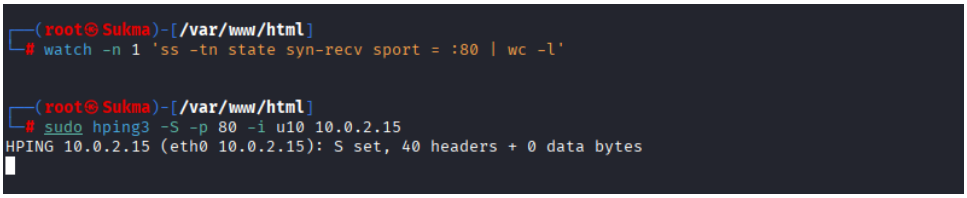


Saat melakuka Htop CPU Cuma sekitar 2-3%, load average 0.24/0.12/0.09, hamper tidak ada proses yang berat

3. Saat melakukan serangan

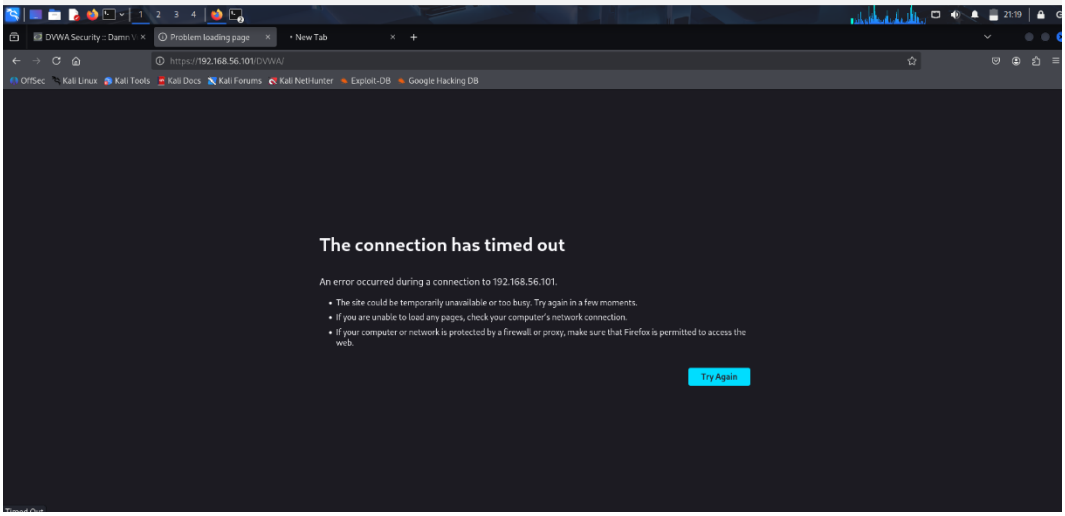


Ini peningkatan CPU 82.0% saat serangan sedang berjalan



- Perintah ini *menjalankan ss -tn state syn-recv sport = :80 | wc -l* setiap satu detik, di mana ss -tn menampilkan koneksi TCP dalam bentuk numerik, state syn-recv memfilter hanya koneksi yang berada pada status SYN-RECV (half-open), sport = :80 membatasi pada port sumber 80, dan wc -l menghitung jumlah baris sehingga diperoleh total koneksi half-open pada port 80; nilai yang kecil pada tahap ini menunjukkan kondisi normal sebelum serangan.

- *sudo hping3 -1 -i u10 192.168.56.101* mengirim ICMP echo request berkecepatan sangat tinggi ke 192.168.56.101 untuk melakukan ping flood / ICMP DoS, biasanya dipakai di lab untuk menguji bagaimana server atau firewall merespons serangan ICMP flood.



Pada saat serangan berjalan web di kali itu tidak bisa di buka karena hping3 (SYN flood) mengirim sangat banyak paket SYN ke port 80 sehingga server sibuk membuka koneksi palsu dan tabel koneksinya penuh, Akibatnya permintaan normal dari browser tidak mendapat respon tepat waktu.

```
┌──(root㉿Sukma)-[/home/sukma]
└─# sudo iptables -A INPUT -p tcp --syn --dport 80 -m limit --limit 20/second --limit-burst 100 -j ACCEPT
sudo iptables -A INPUT -p tcp --syn --dport 80 -j DROP
sudo iptables -L -n

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.56.102       0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02 limit: avg 20/sec burst 100
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Pada tahap ini diterapkan aturan firewall iptables yang membatasi paket SYN ke port 80 maksimal 20 paket per detik dan menjatuhkan sisanya, sehingga traffic flood dari hping3 tidak lagi membebani web server secara berlebihan. Setelah itu, htop dijalankan kembali untuk mengamati penurunan penggunaan CPU dan stabilitas sistem setelah mitigasi.