

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

```
[root@Sukma]# /home/sukma]
# sudo apt install -y apache2 mariadb-server php php-mysqli php-gd git
Note, selecting 'php8.4-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.65-3+b1).
apache2 set to manually installed.
php8.4-mysql is already the newest version (8.4.11-1+b1).
php8.4-mysql set to manually installed.
The following package was automatically installed and is no longer required:
  libconfig-inifiles-perl
Use 'sudo apt autoremove' to remove it.

Upgrading:
  git           mariadb-client-core      mariadb-plugin-provider-lzo    php
  git-man        mariadb-common          mariadb-plugin-provider-snappy  php-common
  libapache2-mod-php mariadb-plugin-provider-bzip2   mariadb-server          php-mysql
  libmariadb3     mariadb-plugin-provider-lz4     mariadb-server-compat
  mariadb-client  mariadb-plugin-provider-lzma    mariadb-server-core

Installing:
  php-gd

Installing dependencies:
  php8.4-gd

Summary:
  Upgrading: 18, Installing: 2, Removing: 0, Not Upgrading: 1424
  Download size: 28.1 MB
  Space needed: 715 kB / 7,726 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 mariadb-common all 1:11.8.5-3 [30.3 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 mariadb-server-core amd64 1:11.8.5-3 [8,038 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/main amd64 mariadb-client-core amd64 1:11.8.5-3 [918 kB]
0% [5 mariadb-client-core 96.9 kB/918 kB 11%] [Connecting to mirror.sg.gsl] [4 mariadb-server-core 1,777 kB/8,038 kB]
Get:3 http://mirror.sg.gsl/kali kali-rolling/main amd64 mariadb-server-compat all 1:11.8.5-3 [29.1 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 mariadb-client amd64 1:11.8.5-3 [3,162 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 mariadb-plugin-provider-snappy amd64 1:11.8.5-3 [30.6 kB]
Get:18 http://http.kali.org/kali kali-rolling/main amd64 php8.4-gd amd64 8.4.11-1+b1 [36.5 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 mariadb-plugin-provider-lzma amd64 1:11.8.5-3 [30.6 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 mariadb-plugin-provider-lz4 amd64 1:11.8.5-3 [30.6 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 git amd64 1:2.51.0-1 [9,259 kB]
Get:2 http://mirror.freddie.org/kali kali-rolling/main amd64 mariadb-server amd64 1:11.8.5-3 [3,922 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 git-man all 1:2.51.0-1 [2,286 kB]
```

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.

```
[root@Sukma]# /home/sukma]
# cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git

Cloning into 'DVWA' ...
remote: Enumerating objects: 5622, done.
remote: Total 5622 (delta 0), reused 0 (delta 0), pack-reused 5622 (from 1)
Receiving objects: 100% (5622/5622), 2.64 MiB | 24.00 KiB/s, done.
Resolving deltas: 100% (2809/2809), done.
```

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

```
Resolving deltas: 100% (2809/2809), done.  
[root@Sukma]~# cd /var/www/html/DVWA/config  
[root@Sukma]~# sudo cp config.inc.php.dist config.inc.php  
  
[root@Sukma]~# cd /var/www/html/DVWA/config  
[root@Sukma]~# sudo cp config.inc.php.dist config.inc.php  
  
[root@Sukma]~# cd /var/www/html/DVWA/config  
[root@Sukma]~# sudo cp config.inc.php.dist config.inc.php  
  
[root@Sukma]~# cd /var/www/html  
[root@Sukma]~# sudo chmod -R 777 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
```

```

[root@Sukma ~]# sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 11.8.5-MariaDB-3 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT user, host FROM mysql.user WHERE user='dvwa';
+-----+-----+
| User | Host |
+-----+-----+
| dvwa | localhost |
+-----+-----+
1 row in set (0.010 sec)

MariaDB [(none)]> ALTER USER 'dvwa'@'localhost' IDENTIFIED BY 'dvwa123';
Query OK, 0 rows affected (0.044 sec)

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| dvwa |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.060 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
Query OK, 0 rows affected (0.030 sec)

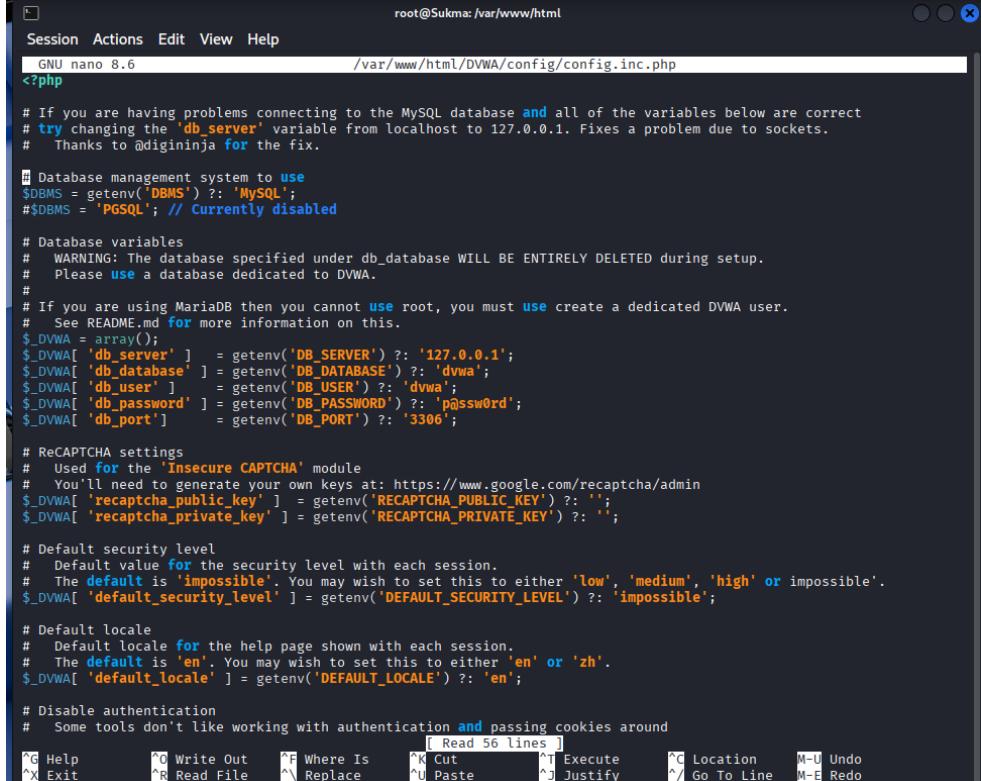
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

```

- 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



```
root@Sukma:/var/www/html
Session Actions Edit View Help
GNU nano 8.6          /var/www/html/DVWA/config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ] = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'impossible';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = getenv('DEFAULT_LOCALE') ?: 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
[ Read 56 lines ]
^G Help      ^O Write Out    ^F Where Is    ^K Cut        ^T Execute    ^C Location    M-U Undo
^X Exit      ^R Read File    ^M Replace    ^Y Paste       ^J Justify    ^L Go To Line  M-F Redo
```

`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

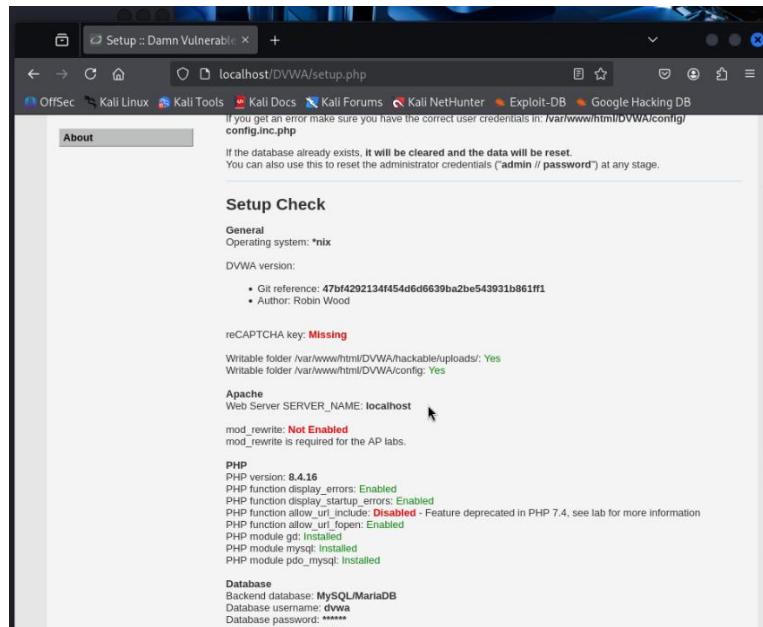
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```

- *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.

```
(root@Sukma) [/home/sukma]
# 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:bd brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
            valid_lft 527sec preferred_lft 527sec
        inet6 fe80::a00:27ff:fe98:4cbd/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

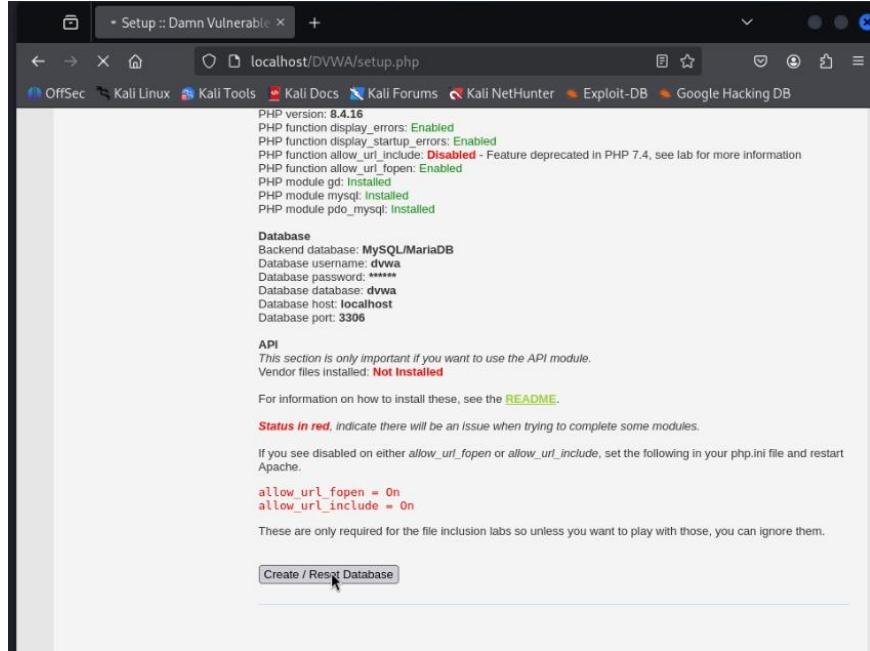
ip a digunakan untuk melihat alamat IP yang didapat pada setiap interface; di sini digunakan untuk memastikan attacker dan target berada di jaringan yang sama.

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.



The screenshot shows a web browser window titled "Setup :: Damn Vulnerable Web Application". The URL in the address bar is "localhost/DVWA/setup.php". The page content includes:

- PHP version:** 8.4.16
- PHP function display_errors:** Enabled
- PHP function display_startup_errors:** Enabled
- PHP function allow_url_include:** Disabled - Feature deprecated in PHP 7.4, see lab for more information
- PHP function allow_url_fopen:** Enabled
- PHP module gd:** Installed
- PHP module mysqli:** Installed
- PHP module pdo_mysql:** Installed

Database

Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: localhost
Database port: 3306

API

This section is only important if you want to use the API module.
Vendor files installed: Not Installed

For information on how to install these, see the [README](#).

Status in red: Indicate there will be an issue when trying to complete some modules.

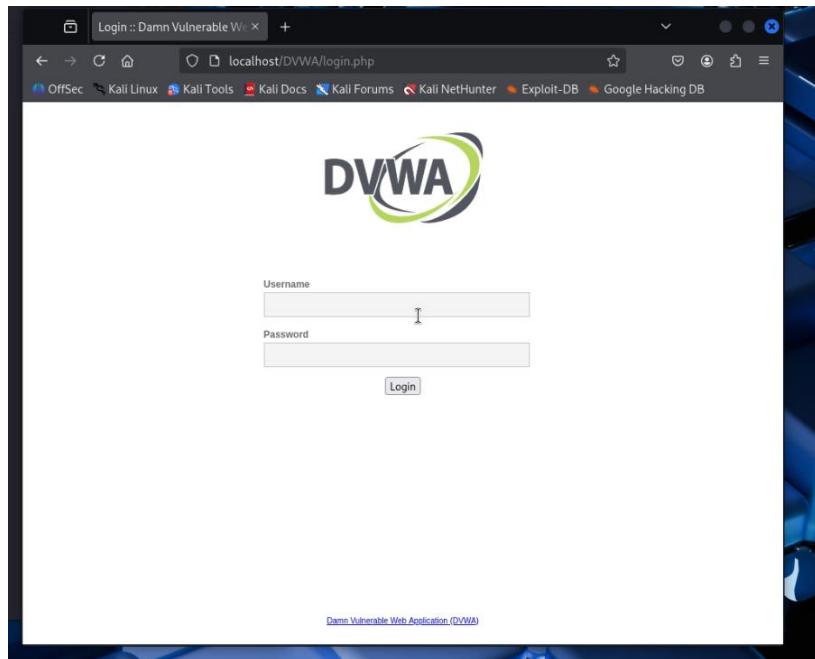
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

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



The screenshot shows a web browser window titled "Login :: Damn Vulnerable Web Application". The URL in the address bar is "localhost/DVWA/login.php". The page content includes:

DVWA

Username

Password

Damn Vulnerable Web Application (DVWA)

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

The screenshot shows a web browser window with the URL `localhost/DVWA/index.php`. The page displays a warning message: "Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database." Below this is a "Disclaimer" section stating that the application is for educational purposes only and should not be used maliciously. A "More Training Resources" section lists links to "Mutillidae" and "OWASP Vulnerable Web Applications Directory". On the left sidebar, there is a navigation menu with options like XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript Attacks, Authorisation Bypass, Open HTTP Redirect, Cryptography, API, DVWA Security, PHP Info, About, and Logout.

Ini tampilan setelah berhasil masuk, setelah itu atur DvWA security

The screenshot shows the DVWA security configuration page. The title is "DVWA Security". Under "Security Level", it says "Security level is currently: low.". A note states: "You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:". Below this is a dropdown menu with options: Low (selected), Medium, High, and Impossible. A "Submit" button is next to the dropdown. At the bottom right, there is a link: "Broken Access Control Logs - View access logs for the Broken Access Control vulnerability". On the left sidebar, there is a navigation menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript Attacks, and Authorisation Bypass.

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

6. Port Scanning dengan Nmap

```
[root@Sukma ~]# nmap -p 1-100 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-28 20:17 WITA
massdns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.000090s 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 menunjukkan port 80 terbuka.

B. Eksekusi serangan DoS dengan HPING3

1. Monitoring baseline di target.

```
[root@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

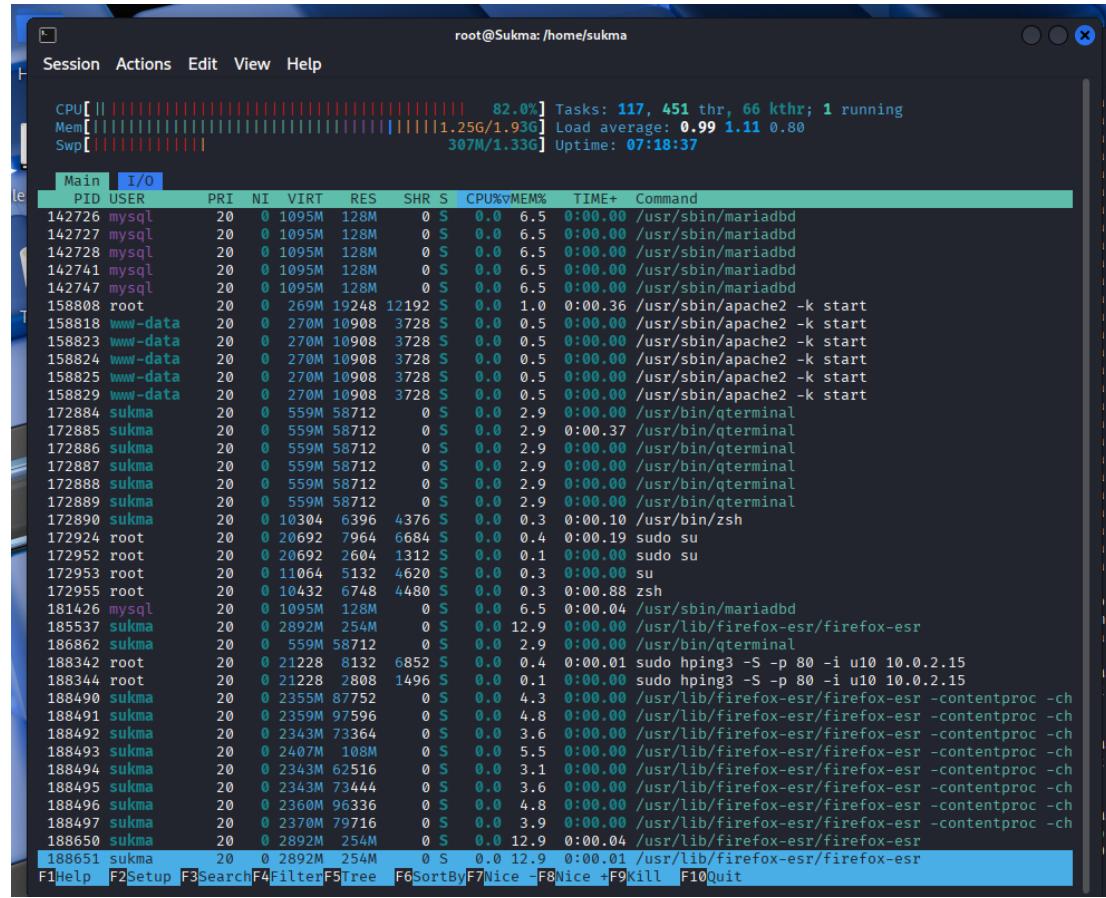
The screenshot shows the Htop terminal window with the following details:

- System statistics at the top:
 - CPU usage: 2.3%
 - Tasks: 115, 446 thr, 66 kthr; 1 running
 - Memory usage: 1.24G/1.93G Load average: 0.24 0.12 0.09
 - Swap usage: 136M/1.33G Uptime: 07:01:48
- Process list table:

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%vMEM%	TIME+ Command
678	root	20	0	437M	152M	74944	S	1.9	7.7 4:59.84 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/
179763	root	20	0	437M	152M	0	S	0.8	7.7 0:08.95 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/
690	root	20	0	437M	152M	0	S	0.8	7.7 0:08.95 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/
1072	sukma	20	0	282M	33320	21112	S	0.8	1.6 0:56.99 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
1035	sukma	20	0	210M	3352	0	S	0.4	0.2 0:04.60 /usr/bin/VBoxClient --vmsvga
1062	sukma	20	0	572M	56904	35452	S	0.4	2.8 0:07.49 xfdesktop
172883	sukma	20	0	559M	59096	49720	S	0.4	2.9 0:01.14 /usr/bin/qterminal
1	root	20	0	24800	15416	10796	S	0.0	0.8 0:04.38 /sbin/init splash
531	root	20	0	8380	4660	1772	S	0.0	0.2 0:01.57 /usr/sbin/haveged --Foreground --verbose=1
537	root	20	0	301M	7328	6560	S	0.0	0.4 0:00.07 /usr/libexec/accounts-daemon
541	messagebus	20	0	10264	7452	4380	S	0.0	0.4 0:09.09 /usr/bin/dbus-daemon --system --address=systemd:
543	polkitd	20	0	373M	10108	7544	S	0.0	0.5 0:00.17 /usr/lib/polkit-1/polkitd --no-debug --log-level=
545	root	20	0	19032	9260	8108	S	0.0	0.5 0:01.73 /usr/lib/systemd/systemd-logind
551	root	20	0	6888	2632	2504	S	0.0	0.1 0:00.11 /usr/sbin/cron -f
552	root	20	0	301M	7328	0	S	0.0	0.4 0:00.00 /usr/libexec/accounts-daemon
553	root	20	0	301M	7328	0	S	0.0	0.4 0:00.00 /usr/libexec/accounts-daemon
587	polkitd	20	0	373M	10108	0	S	0.0	0.5 0:00.72 /usr/lib/polkit-1/polkitd --no-debug --log-level=
588	polkitd	20	0	373M	10108	0	S	0.0	0.5 0:00.00 /usr/lib/polkit-1/polkitd --no-debug --log-level=
589	polkitd	20	0	373M	10108	0	S	0.0	0.5 0:00.04 /usr/lib/polkit-1/polkitd --no-debug --log-level=
591	root	20	0	328M	19188	16244	S	0.0	0.9 0:00.57 /usr/sbin/NetworkManager --no-daemon
592	root	20	0	301M	7328	0	S	0.0	0.4 0:00.01 /usr/libexec/accounts-daemon
608	root	20	0	309M	12176	10256	S	0.0	0.6 0:00.13 /usr/sbin/ModemManager
620	root	20	0	309M	12176	0	S	0.0	0.6 0:00.00 /usr/sbin/ModemManager
625	root	20	0	309M	12176	0	S	0.0	0.6 0:00.00 /usr/sbin/ModemManager
627	root	20	0	309M	12176	0	S	0.0	0.6 0:00.00 /usr/sbin/ModemManager
631	root	20	0	348M	3420	3028	S	0.0	0.2 0:00.00 /usr/sbin/VBoxService
633	root	20	0	348M	3420	0	S	0.0	0.2 0:00.00 /usr/sbin/VBoxService
634	root	20	0	348M	3420	0	S	0.0	0.2 0:00.16 /usr/sbin/VBoxService
635	root	20	0	348M	3420	0	S	0.0	0.2 0:00.47 /usr/sbin/VBoxService
636	root	20	0	348M	3420	0	S	0.0	0.2 0:06.05 /usr/sbin/VBoxService
637	root	20	0	348M	3420	0	S	0.0	0.2 0:00.00 /usr/sbin/VBoxService
638	root	20	0	348M	3420	0	S	0.0	0.2 0:00.49 /usr/sbin/VBoxService
639	root	20	0	348M	3420	0	S	0.0	0.2 0:00.84 /usr/sbin/VBoxService
640	root	20	0	348M	3420	0	S	0.0	0.2 0:00.19 /usr/sbin/VBoxService
641	root	20	0	328M	19188	0	S	0.0	0.9 0:00.00 /usr/sbin/NetworkManager --no-daemon
642	root	20	0	328M	19188	0	S	0.0	0.9 0:00.00 /usr/sbin/NetworkManager --no-daemon
644	root	20	0	328M	19188	0	S	0.0	0.9 0:00.02 /usr/sbin/NetworkManager --no-daemon
- Bottom navigation bar: F1Help, F2Setup, F3Search, F4Filter, F5Tree, F6SortBy, F7Nice -, F8Nice +, F9Kill, F10Quit

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



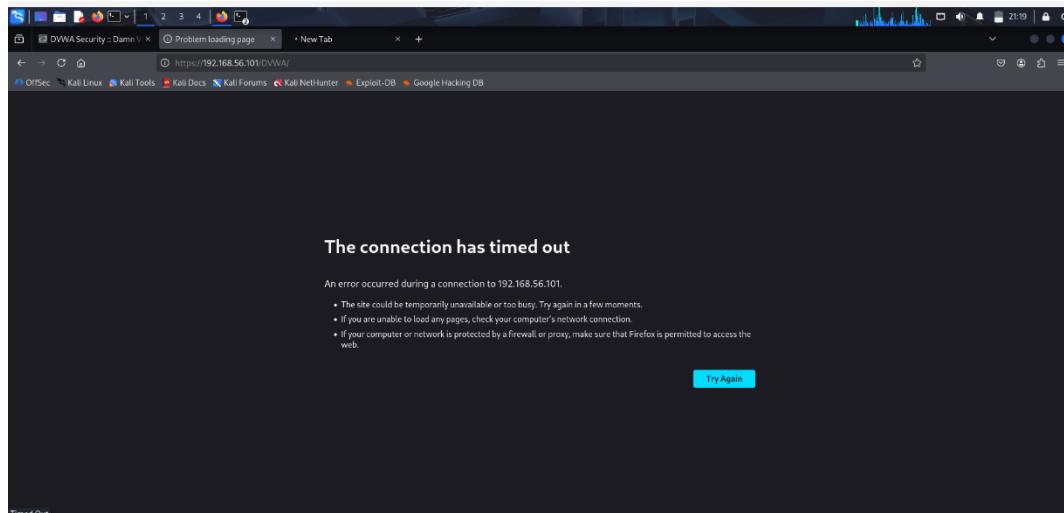
Ini peningkatan CPU 82.0% saat serangan sedang berjalan

```
(root@sukma)-[~/var/www/html]
# watch -n 1 'ss -tn state syn_RECV sport = :80 | wc -l'

(root@sukma)-[~/var/www/html]
# sudo hping3 -S -p 80 -i u10 10.0.2.15
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
```

- 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.

4. Serangan dengan slowress

```
(root@Sukma)-[~/var/www/html]
└─# sudo apt update
sudo apt install slowhttptest
# atau siapkan script slowloris.py sendiri

Hit:1 http://http.kali.org/kali kali-rolling InRelease
1437 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following package was automatically installed and is no longer required:
libconfig-inifiles-perl
Use 'sudo apt autoremove' to remove it.

Installing:
slowhttptest

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1437
Download size: 31.6 kB
Space needed: 91.1 kB / 7,579 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 slowhttptest amd64 1.9.0-1+b1 [31.6 kB]
Fetched 31.6 kB in 2s (16.3 kB/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 416694 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) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for man-db (2.13.1-1) ...
```

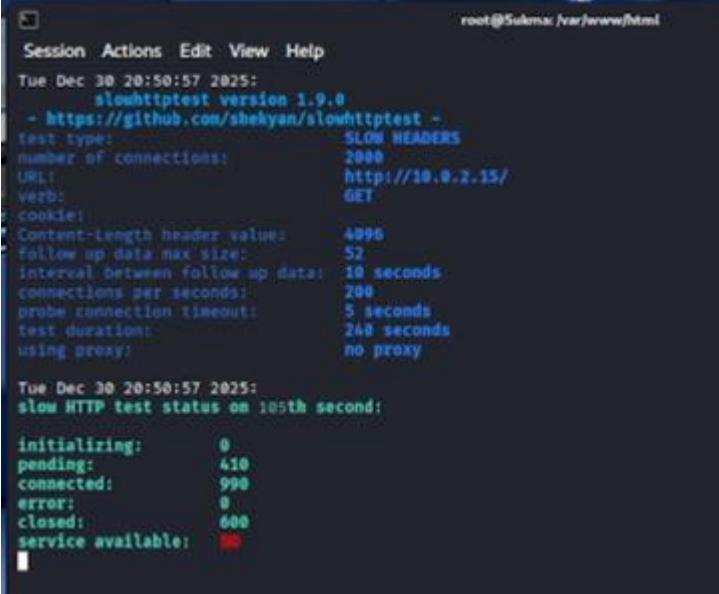
Melakukan penginstalan slowress.

```
root@Sukma:/home/sukma
Session Actions Edit View Help

CPU[██████████] 17.1% Tasks: 261, 462 thr, 67 kthr; 1 running
Mem[████████████████████████████████████████████████████████████████████████] 1.13G/1.93G Load average: 0.88 0.88 0.79
Swap[████████████████████████████████████████████████████████████████████████] 158M/1.33G Uptime: 00:46:10

Main I/O PID USER PRI NI VIRT RES SHR S CPU%MEM TIME+ Command
25569 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25570 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25571 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25572 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25573 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25574 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25575 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
25576 www-data 20 0 270M 14376 6032 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26519 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26522 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26523 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26524 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26525 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26534 sukma 20 0 1020M 6412 4396 S 0.0 0.3 0:00.16 /usr/bin/zsh
26535 sukma 20 0 567M 66296 0 S 0.0 3.3 0:00.00 /usr/bin/qterminal
26576 sukma 20 0 2904M 350M 0 S 0.0 17.8 0:00.00 /usr/lib/firefox-esr/firefox-esr
26591 sukma 20 0 2904M 350M 0 S 0.0 17.8 0:00.00 /usr/lib/firefox-esr/firefox-esr
26611 root 20 0 20692 8032 6752 S 0.0 0.4 0:00.04 sudo su
26633 root 20 0 20692 2528 1300 S 0.0 0.1 0:00.00 sudo su
26634 root 20 0 11064 5036 4524 S 0.0 0.2 0:00.00 su
26636 root 20 0 10296 6332 4316 S 0.0 0.3 0:00.07 zsh
26745 sukma 20 0 2343M 73920 0 S 0.0 3.7 0:00.00 /usr/lib/firefox-esr/firefox-esr -contentproc -ch
26829 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26838 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26839 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26848 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26849 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26850 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26851 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26860 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26861 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
26862 www-data 20 0 270M 14116 5904 S 0.0 0.7 0:00.00 /usr/sbin/apache2 -k start
```

Saat melakukan serangan di sini bisa di lihat CPU nya itu 17.1% saat kode di bawah ini di jalankan CPU nya akan menurun.

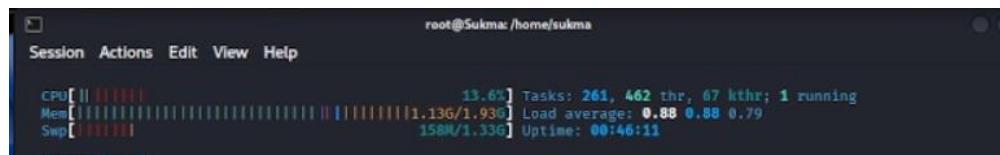


```
Session Actions Edit View Help
root@Sukma: /var/www/html
Tue Dec 30 20:50:57 2025:
slowhttptest version 1.9.0
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADERS
number of connections: 2000
URL: http://10.0.2.15/
verb: GET
cookie:
Content-length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy

Tue Dec 30 20:50:57 2025:
slow HTTP test status on 105th second:

initializing: 0
pending: 410
connected: 990
error: 0
closed: 600
service available: NO
```

Jumlah koneksi yang digunakan dalam pengujian ini adalah 2000 koneksi dengan metode HTTP GET dan tanpa menggunakan proxy. Di bagian bawah dapat dilihat statistik pada detik ke-105, di mana terdapat sekitar 990 koneksi yang masih dalam status connected dan 410 koneksi pending, sedangkan 600 koneksi sudah closed. Status service available menunjukkan nilai NO, yang berarti pada saat pengujian ini web server tidak mampu merespon permintaan secara normal dan dianggap tidak tersedia akibat serangan Slow HTTP yang sedang berlangsung.



Ini Gambaran CPU nya saat turun setelah kode di atas di jalankan.

Sementara ini saya sudah beralih menjadi user root dengan perintah sudo su, kemudian saya menjalankan perintah watch -n 1 "ss -nt sport =:80 | wc -l" untuk memonitor jumlah koneksi TCP ke port 80 setiap satu detik. Setelah itu saya menambahkan dua rule firewall iptables pada chain INPUT untuk membatasi koneksi baru ke port 80 dengan modul recent, sehingga jika satu alamat IP mencoba membuka terlalu banyak koneksi dalam waktu singkat, paketnya akan di-drop. Terakhir, saya menjalankan nmap -sV 192.168.1.100 untuk memindai host 192.168.1.100 sekaligus mendeteksi versi service yang berjalan pada port-port yang terbuka setelah aturan firewall diterapkan.