ETHICAL HACKING AND PENETRATION TESTING I

Dosen pengampuh : RUNAL REZKIAWAN, S.kom., M.T

OLEH

Nama : ALAMSYAH SAHLAN

Nim : 105841111823

Kelas : 5A

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

LAPORAN PRAKTIKUM

SIMULASI DOS ATTACK & MITIGASI

1. Referensi & Sumber Daya

Berikut adalah referensi yang digunakan dalam praktikum ini:

- Download DVWA: https://github.com/digininja/DVWA.git
- Panduan Instalasi DVWA: Sesuai dokumen "DVWA Installation".
- Penggunaan hping3: Alat untuk simulasi paket TCP/IP.

2. Langkah-Langkah Praktikum

1) Instalasi Target (DVWA)

Tahap ini bertujuan untuk membangun lingkungan server yang rentan.

a) **Persiapan Direktori:**

- sudo apt update: Memperbarui daftar paket aplikasi agar sistem siap.

```
┌──(kali㉿kali)-[/home/kali]
└─PS> sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1453 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- cd /var/www/html: Berpindah ke direktori root web server Apache.

```
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html
```

- sudo git clone https://github.com/digininja/DVWA.git: Mengunduh kode sumber DVWA dari GitHub.

```
┌──(root㉿kali)-[/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 | 400.00 KiB/s, done.
Resolving deltas: 100% (2809/2809), done.
```

b) **Konfigurasi dan Izin:**

- cd /var/www/html/DVWA/config: Masuk ke folder pengaturan.

```
┌──(root㉿kali)-[/var/www/html]
└─# cd /var/www/html/DVWA/config
```

- sudo cp config.inc.php.dist config.inc.php: Menyalin file contoh konfigurasi menjadi file konfigurasi aktif.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo cp config.inc.php.dist config.inc.php
```

- sudo chmod -R 777 /var/www/html/DVWA/: Memberikan izin akses penuh ke folder DVWA agar aplikasi bisa menulis log dan data.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo chmod -R 777 /var/www/html/DVWA/
```

c) **Setup Database (MariaDB):**

- sudo mysql -u root -p: Masuk ke konsol database sebagai pengguna root.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://gi

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)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.023 sec)

MariaDB [(none)]> CREATE USER IF NOT EXISTS 'user' IDENTIFIED BY 'pass';
Query OK, 0 rows affected, 1 warning (0.199 sec)

MariaDB [(none)]> GRANT ALL ON dvwa.* TO 'user';
Query OK, 0 rows affected (0.157 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.091 sec)

MariaDB [(none)]> EXIT;
Bye
```

  - ✓ CREATE DATABASE dvwa;: Membuat database baru bernama dvwa.
  - ✓ CREATE USER 'user' IDENTIFIED BY 'pass';: Membuat akun pengguna database dengan password pass.
  - ✓ GRANT ALL ON dvwa.* TO 'user';: Memberikan izin penuh kepada user untuk mengelola database dvwa.
  - ✓ FLUSH PRIVILEGES;: Memperbarui hak akses sistem.

- ✓ EXIT;: untuk keluar

d) **Edit File Konfigurasi:**

- sudo nano /var/www/html/DVWA/config/config.inc.php: Membuka editor teks untuk mengatur koneksi database.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo nano /var/www/html/DVWA/config/config.inc.php
```

- Ubah db_user menjadi 'user' dan db_password menjadi 'pass' agar sesuai dengan kredensial database yang baru dibuat.
  - Sebelum di ubah

```
$_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';
```

  - Sesudah di ubah

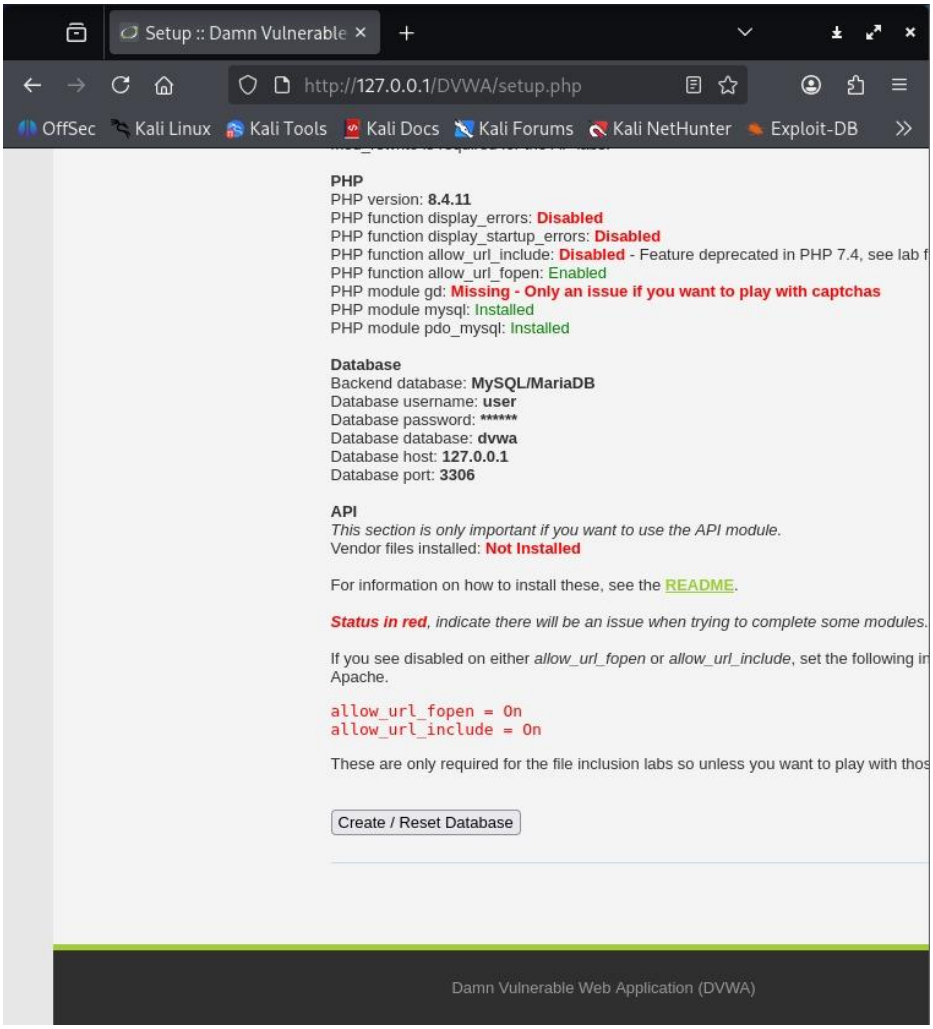
```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

e) **Aktivasi Layanan:**

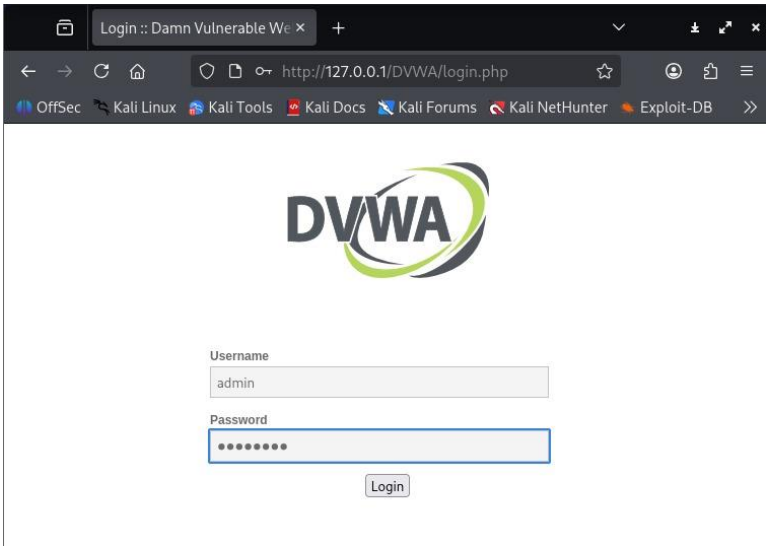
- sudo service apache2 restart: Memulai ulang web server agar perubahan konfigurasi terbaca.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo service apache2 restart
```

- Akses http://127.0.0.1/DVWA/setup.php di Firefox, lalu klik "Create / Reset Database".



- Masukkan username dan password kemudian klik login



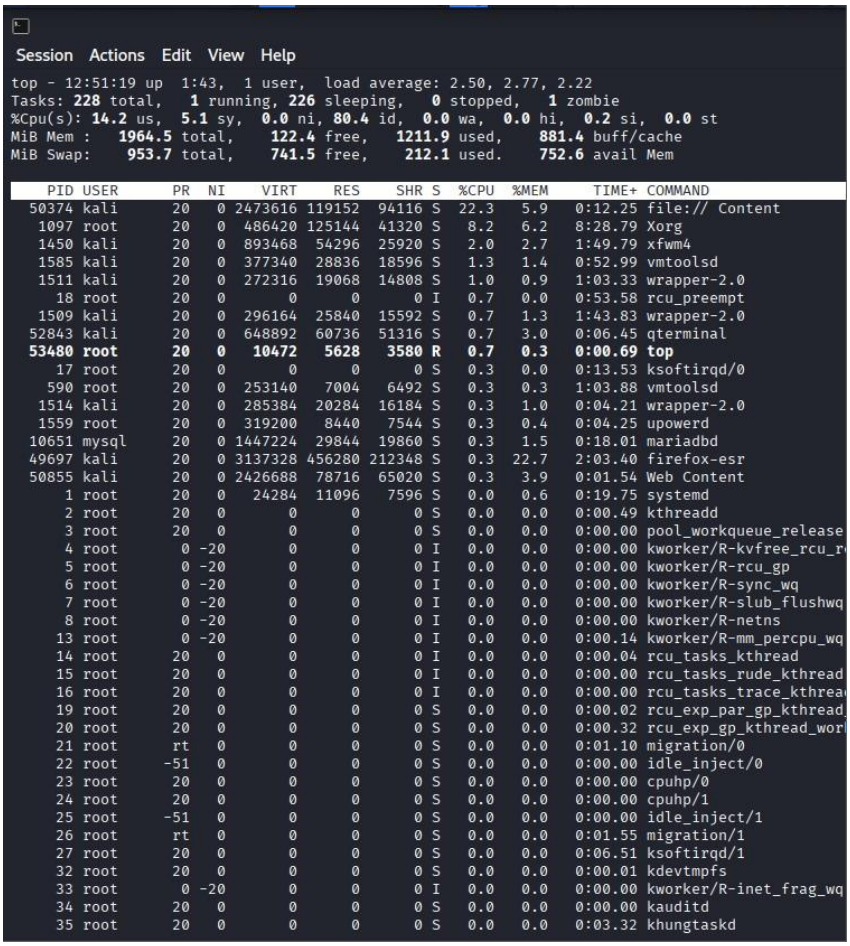
2) Simulasi Serangan (DoS)

Tahap ini menunjukkan bagaimana serangan membebani sumber daya server.

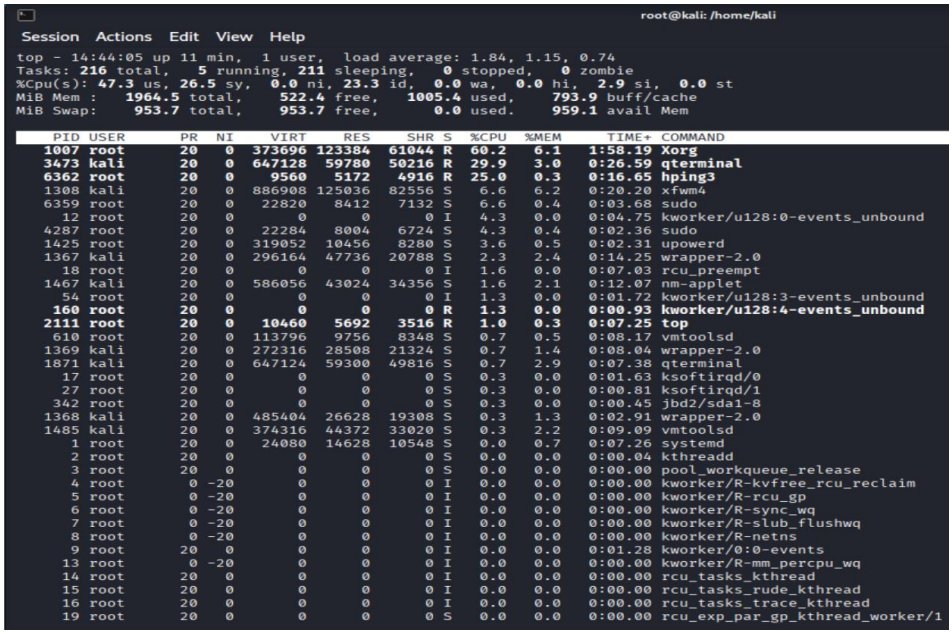
a) **Monitoring (Terminal 1):**

- top: Menampilkan penggunaan CPU dan RAM secara *real-time*. Digunakan untuk melihat lonjakan beban akibat serangan dan unutk memberhentikannya klik CTRL + C.

- kondisi komputer sebelum diserang di mana **%id (idle)** sebesar **80.4%** berarti CPU masih santai dan tidak bekerja keras

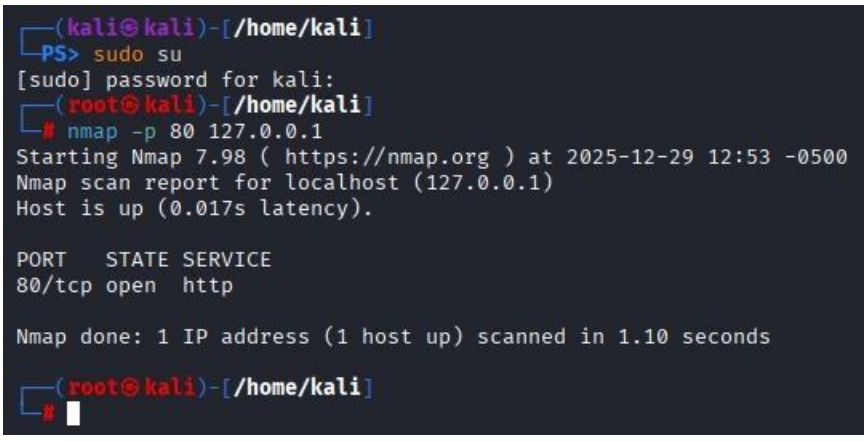


- kondisi komputer saat diserang di mana kondisinya akan turun mendekati 0%, menandakan CPU tidak lagi memiliki waktu luang.



b) **Scanning (Terminal 2):**

- nmap -p 80 127.0.0.1: Memastikan port 80 (HTTP) terbuka sebelum serangan dimulai.



c) **Eksekusi Serangan (Terminal 3):**

- sudo hping3 -S -p 80 -i u10 127.0.0.1 dan untuk menghentikannya klik CTRL + O lalu ENTER dan klik CTRL + X

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo hping3 -S -p 80 -i u10 127.0.0.1
```

```
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53465 win=0 rtt=37.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53466 win=0 rtt=37.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53467 win=0 rtt=37.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53468 win=0 rtt=37.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53469 win=0 rtt=36.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53470 win=0 rtt=36.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53471 win=0 rtt=36.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53472 win=0 rtt=5.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53473 win=0 rtt=6.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53474 win=0 rtt=5.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53475 win=0 rtt=5.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53476 win=0 rtt=17.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53477 win=0 rtt=17.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53478 win=0 rtt=17.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53479 win=0 rtt=16.9 ms
^C
── 127.0.0.1 hping statistic ──
53484 packets transmitted, 53480 packets received, 1% packet loss
round-trip min/avg/max = 0.1/23.1/1576.9 ms
```

  - ✓ -S: Mengirim paket SYN (awal jabat tangan TCP).
  - ✓ -p 80: Menargetkan port web.
  - ✓ -i u10: Interval pengiriman paket setiap 10 mikrodetik (sangat cepat).

3) Mitigasi (Firewall)

Tahap ini menunjukkan cara menangkal atau membatasi serangan.

a) **Penerapan Aturan:**

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

```
┌──(root㉿kali)-[/home/kali]
└─# sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

  - ✓ -A INPUT: Menambahkan aturan pada jalur masuk data.
  - ✓ -p tcp --dport 80: Hanya berlaku untuk protokol TCP di port 80.
  - ✓ -m limit --limit 25/minute: Membatasi rata-rata hanya 25 paket yang diterima per menit.

- ✓ --limit-burst 100: Mengizinkan lonjakan maksimal hingga 100 paket sebelum pembatasan ketat diberlakukan.

b) **Verifikasi Mitigasi:**

- sudo iptables -L -n -v: Menampilkan daftar aturan firewall beserta jumlah paket (pkts) yang berhasil ditangkap oleh aturan tersebut. Dengan jumlah paket 116 dan total data 4640