

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]
└─$ 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 dan untuk menghentikannya klik CTRL + O lalu ENTER dan klik CTRL + X
 - 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".

PHP
PHP version: **8.4.11**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled** - Feature deprecated in PHP 7.4, see lab f
PHP function allow_url_fopen: **Enabled**
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

Database
Backend database: **MySQL/MariaDB**
Database username: **user**
Database password: *********
Database database: **dvwa**
Database host: **127.0.0.1**
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 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

[Create / Reset Database](#)

Damn Vulnerable Web Application (DVWA)

- Masukkan username dan password kemudian klik login

DVWA

Username

Password

[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 untuk memberhentikannya klik CTRL + C.

```
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
└─# top
```

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

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
50374	kali	20	0	2473616	119152	94116	S	22.3	5.9	0:12.25	file:// Content
1097	root	20	0	486420	125144	41320	S	8.2	6.2	8:28.79	Xorg
1450	kali	20	0	893468	54296	25920	S	2.0	2.7	1:49.79	xterm
1585	kali	20	0	377340	28836	18596	S	1.3	1.4	0:52.99	vmtoolsd
1511	kali	20	0	272316	19068	14808	S	1.0	0.9	1:03.33	wrapper-2.0
18	root	20	0	0	0	0	I	0.7	0.0	0:53.58	rcu_preempt
1509	kali	20	0	296164	25840	15592	S	0.7	1.3	1:43.83	wrapper-2.0
52843	kali	20	0	648892	60736	51316	S	0.7	3.0	0:06.45	qterminal
53480	root	20	0	10472	5628	3580	R	0.7	0.3	0:00.69	top
17	root	20	0	0	0	0	S	0.3	0.0	0:13.53	ksoftirqd/0
590	root	20	0	253140	7004	6492	S	0.3	0.3	1:03.88	vmtoolsd
1514	kali	20	0	285384	20284	16184	S	0.3	1.0	0:04.21	wrapper-2.0
1559	root	20	0	319200	8440	7544	S	0.3	0.4	0:04.25	upowerd
10651	mysql	20	0	1447224	29844	19860	S	0.3	1.5	0:18.01	mariadb
49697	kali	20	0	3137328	456280	212348	S	0.3	22.7	2:03.40	firefox-esr
50855	kali	20	0	2426688	78716	65020	S	0.3	3.9	0:01.54	Web Content
1	root	20	0	24284	11096	7596	S	0.0	0.6	0:19.75	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.49	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pool_workqueue_release
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kvfree_rcu_r
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-rCU_gp
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-sync_wq
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-slub_flushwq
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-netsns
13	root	0	-20	0	0	0	I	0.0	0.0	0:00.14	kworker/R-mm_percpu_wq
14	root	20	0	0	0	0	I	0.0	0.0	0:00.04	rcu_tasks_kthread
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
16	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
19	root	20	0	0	0	0	S	0.0	0.0	0:00.02	rcu_exp_par_gp_kthread
20	root	20	0	0	0	0	S	0.0	0.0	0:00.32	rcu_exp_gp_kthread_wor
21	root	rt	0	0	0	0	S	0.0	0.0	0:01.10	migration/0
22	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0
23	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cphup/0
24	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cphup/1
25	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/1
26	root	rt	0	0	0	0	S	0.0	0.0	0:01.55	migration/1
27	root	20	0	0	0	0	S	0.0	0.0	0:06.51	ksoftirqd/1
32	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kdevtmpfs
33	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-inet_frag_wq
34	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd
35	root	20	0	0	0	0	S	0.0	0.0	0:03.32	khungtaskd

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

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1007	root	20	0	373696	123384	61044	R	60.2	6.1	1:58.19	Xorg
3473	kali	20	0	647128	59780	50216	R	29.9	3.0	0:26.59	qterminal
6362	root	20	0	9560	5172	4916	R	25.0	0.3	0:16.65	hping3
1308	kali	20	0	886908	125036	82556	S	6.6	6.2	0:20.20	xfwm4
6359	root	20	0	22820	8412	7132	S	6.6	0.4	0:03.68	sudo
12	root	20	0	0	0	0	I	4.3	0.0	0:04.75	kworker/u128:0-events_unbound
4287	root	20	0	22284	8004	6724	S	4.3	0.4	0:02.36	sudo
1425	root	20	0	319052	10456	8280	S	3.6	0.5	0:02.31	upowerd
1367	kali	20	0	296164	47736	20788	S	2.3	2.4	0:14.25	wrapper-2.0
18	root	20	0	0	0	0	I	1.6	0.0	0:07.03	rcm_preempt
1467	kali	20	0	586056	43024	34356	S	1.6	2.1	0:12.07	km-applet
54	root	20	0	0	0	0	I	1.3	0.0	0:01.72	kworker/u128:3-events_unbound
160	root	20	0	0	0	0	R	1.0	0.3	0:01.91	kworker/u128:4-events_unbound
2110	root	20	0	10460	5692	3516	R	1.0	0.3	0:07.25	top
610	root	20	0	113796	9756	8348	S	0.7	0.5	0:08.17	vmballd
1369	kali	20	0	272316	28508	21324	S	0.7	1.4	0:08.04	wrapper-2.0
1871	kali	20	0	647124	59300	49816	S	0.7	2.9	0:07.38	qterminal
17	root	20	0	0	0	0	S	0.3	0.0	0:01.63	ksoftirqd/0
27	root	20	0	0	0	0	S	0.3	0.0	0:00.81	ksoftirqd/1
342	root	20	0	0	0	0	S	0.3	0.0	0:00.45	jbd2/sda1-8
1368	kali	20	0	485404	26628	19308	S	0.3	1.3	0:02.91	wrapper-2.0
1485	kali	20	0	374316	44372	33020	S	0.3	2.2	0:09.09	vmtoolsd
1	root	20	0	24080	14628	10548	S	0.0	0.7	0:07.26	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.04	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pool_workqueue_release
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kvfree_rcu_reclaim
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-rcu_gp
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-sync_wq
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-slub_flushwq
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-netns
9	root	20	0	0	0	0	I	0.0	0.0	0:01.28	kworker/0:0-events
13	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-mm_percpu_wq
14	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
16	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_exp_par_gp_kthread_worker/1
											rcu_exp_par_gp_kthread_worker/2

b) Scanning (Terminal 2)

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

```

(kali㉿kali)-[~/home/kali]
PS> sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# nmap -p 80 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-29 12:53 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.017s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds

# 

```

c) Eksekusi Serangan (Terminal 3)

- sudo hping3 -S -p 80 -i u10 127.0.0.1 dan untuk menghentikannya klik CTRL + C

```
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

```
[root@kali ~]# sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 236K packets, 9431K bytes)
 pkts bytes target     prot opt in     out      source          destination
 116  4640 ACCEPT     tcp  --  *      *          0.0.0.0/0        0.0.0.0/0          tcp dpt:80 limit: avg 25/min burst 100

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
```