

# **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

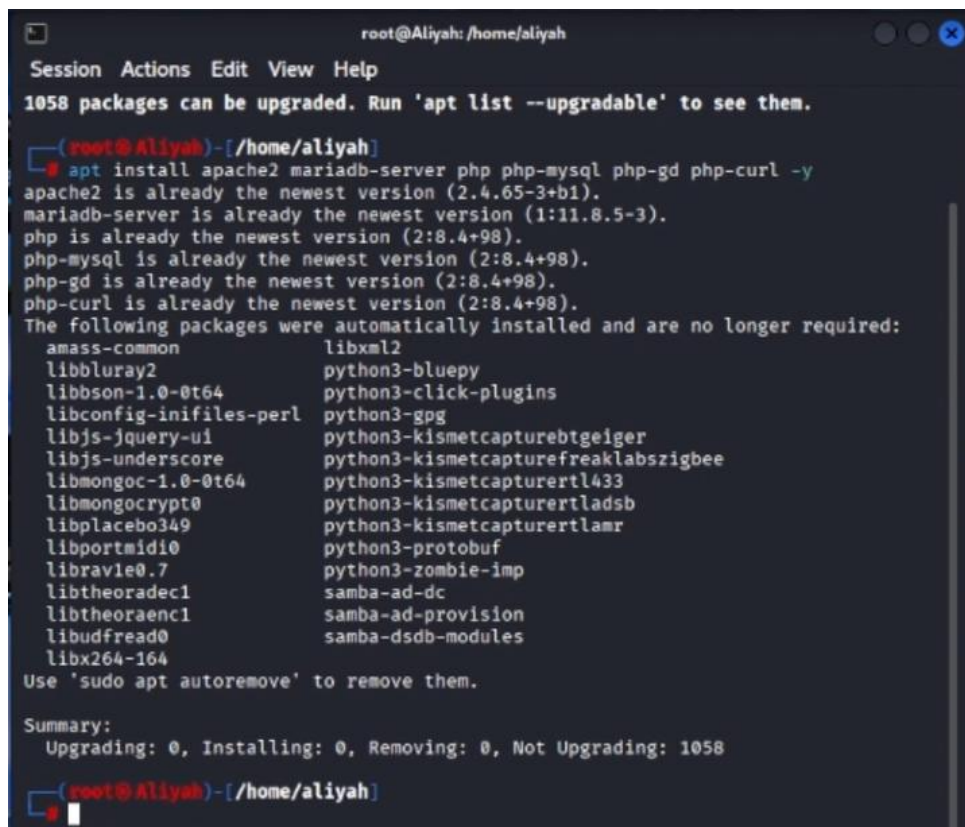
### a. Memperbarui Repositori System



```
root@Aliyah: /home/aliyah
Session Actions Edit View Help
(aliyah@Aliyah)-[~]
$ sudo su
[sudo] password for aliyah:
(root@Aliyah)-[/home/aliyah]
# apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1058 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Langkah pertama, masuk sebagai supepuser menggunakan perintah `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



```
root@Aliyah: /home/aliyah
Session Actions Edit View Help
1058 packages can be upgraded. Run 'apt list --upgradable' to see them.

(root@Aliyah)-[/home/aliyah]
# apt install apache2 mariadb-server php php-mysql php-gd php-curl -y
apache2 is already the newest version (2.4.65-3+b1).
mariadb-server is already the newest version (1:11.8.5-3).
php is already the newest version (2:8.4+98).
php-mysql is already the newest version (2:8.4+98).
php-gd is already the newest version (2:8.4+98).
php-curl is already the newest version (2:8.4+98).
The following packages were automatically installed and are no longer required:
amass-common libxml2
libbluray2 python3-bluepy
libbson-1.0-0t64 python3-click-plugins
libconfig-inifiles-perl python3-gpg
libjs-jquery-ui python3-kismetcapturebtgeiger
libjs-underscore python3-kismetcapturefreaklabszigbee
libmongoc-1.0-0t64 python3-kismetcapturertl433
libmongocrypt0 python3-kismetcapturertladsb
libplacebo349 python3-kismetcapturertlamr
libportmidi0 python3-protobuf
libravle0.7 python3-zombie-imp
libtheoradec1 samba-ad-dc
libtheoraenc1 samba-ad-provision
libudfread0 samba-dsdb-modules
libx264-164
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1058

(root@Aliyah)-[/home/aliyah]
```

Selanjutnya, kita menginstall komponen utama server yang dibutuhkan oleh DVWA atau Damn Vulnerable Web Application.

Perintah `apt install apache2 mariadb-server php php-mysql 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

```
(root@Aliyah)-[/home/aliyah]
# systemctl start apache2

(root@Aliyah)-[/home/aliyah]
# systemctl start mariadb

(root@Aliyah)-[/home/aliyah]
# 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
SW

(root@Aliyah)-[/home/aliyah]
# systemctl enable mariadb
Synchronizing state of mariadb.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable 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.

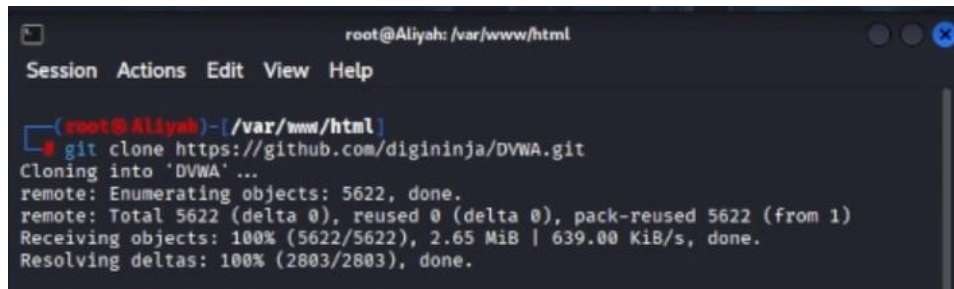
d. Berpindah ke direktori web Root

```
(root@Aliyah)-[/home/aliyah]
# cd /var/www/html

(root@Aliyah)-[/var/www/html]
#
```

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



```
root@Aliyah: /var/www/html
Session Actions Edit View Help

(root@Aliyah)-[/var/www/html]
$ 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), 2.65 MiB | 639.00 KiB/s, done.
Resolving deltas: 100% (2803/2803), done.
```

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



```
(root@Aliyah)-[/var/www/html]
$ chmod -R 777 /var/www/html/DVWA
```

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.

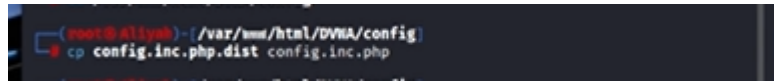
- g. Masuk ke Direktori Konfigurasi



```
(root@Aliyah)-[/var/www/html]
$ cd /var/www/html/DVWA/config
(root@Aliyah)-[/var/www/html/DVWA/config]
$
```

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



```
root@Aliyah:~/var/www/html/DVWA/config# cp config.inc.php.dist config.inc.php
```

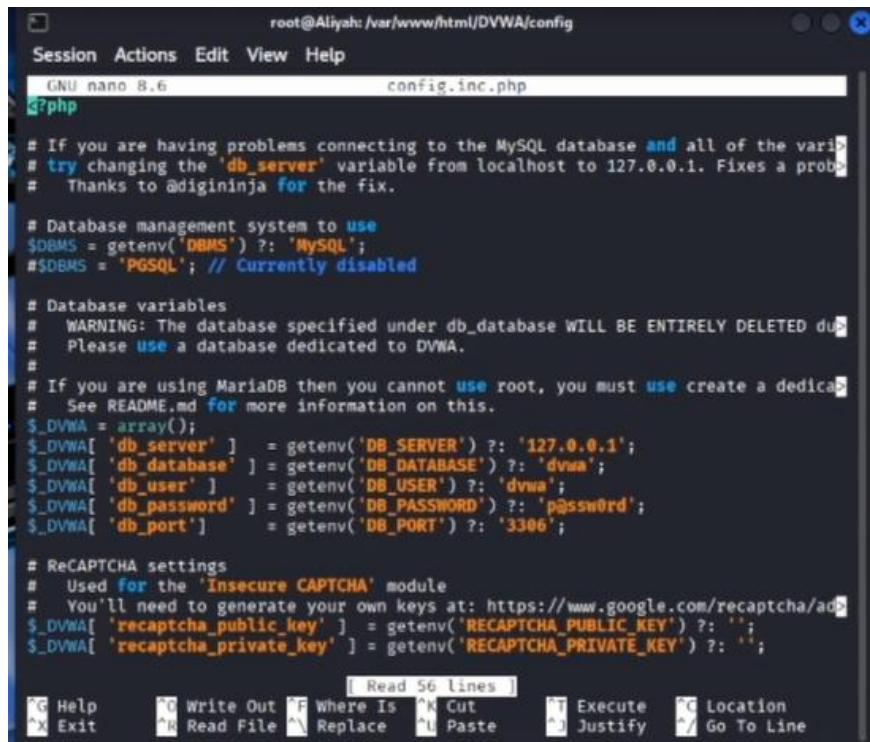
DVWA menyediakan file contoh konfigurasi bernama `config.inc.php.dist`. Kita harus menyalinnya menjadi file aktif dengan perintah `cp config.inc.php.dist config.inc.php`. File baru inilah yang nantinya akan kita edit.

#### i. Mengedit File Konfigurasi



```
root@Aliyah:~/var/www/html/DVWA/config# nano config.inc.php
```

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



```
root@Aliyah: /var/www/html/DVWA/config
Session Actions Edit View Help
GNU nano 8.6 config.inc.php
?php
# If you are having problems connecting to the MySQL database and all of the vari
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a prob
# 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 du
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedica
# 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/ad
$_DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA['recaptcha_private_key'] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

Read 56 Lines
G Help W Write Out F Where Is C Cut E Execute L Location
X Exit R Read File N Replace U Paste J Justify _ Go To Line
```

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.

```
# 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' or 'high'.
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ? 'low' : 'impossible';

# Default locale

G Help      G Write Out  F Where Is  K Cut       T Execute   C Location
X Exit      R Read File  N Replace  L Paste     J Justify   / Go To Line
```

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

```
(root@Aliyah)-[/var/www/html/DVWA/config]
# mysql -u root -p
Enter password:
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)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.007 sec)

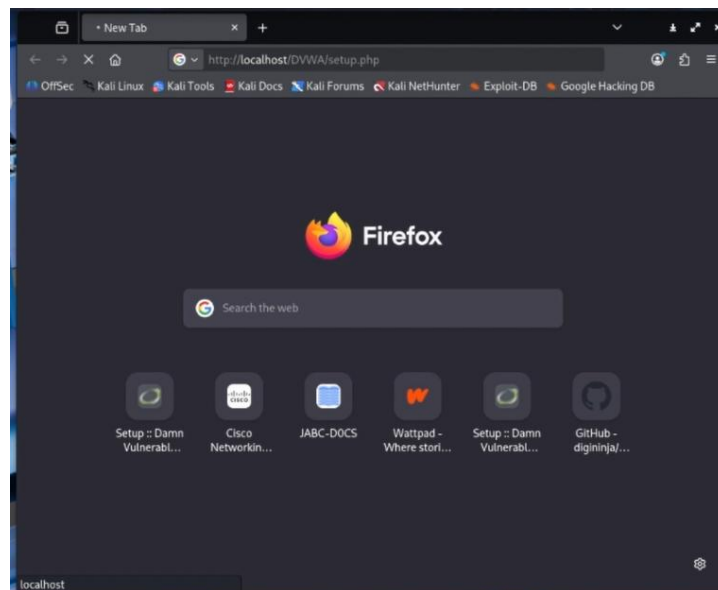
MariaDB [(none)]> CREATE USER 'dvwa'@'localhost' IDENTIFIED BY GRAND ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'IDENTIFIED BY GRAND ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost'' at line 1
MariaDB [(none)]> FLUSH PRIVILEGESD
→ ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'PRIVILEGESD' at line 1
MariaDB [(none)]> EXIT
Bye

(root@Aliyah)-[/var/www/html/DVWA/config]
```

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.

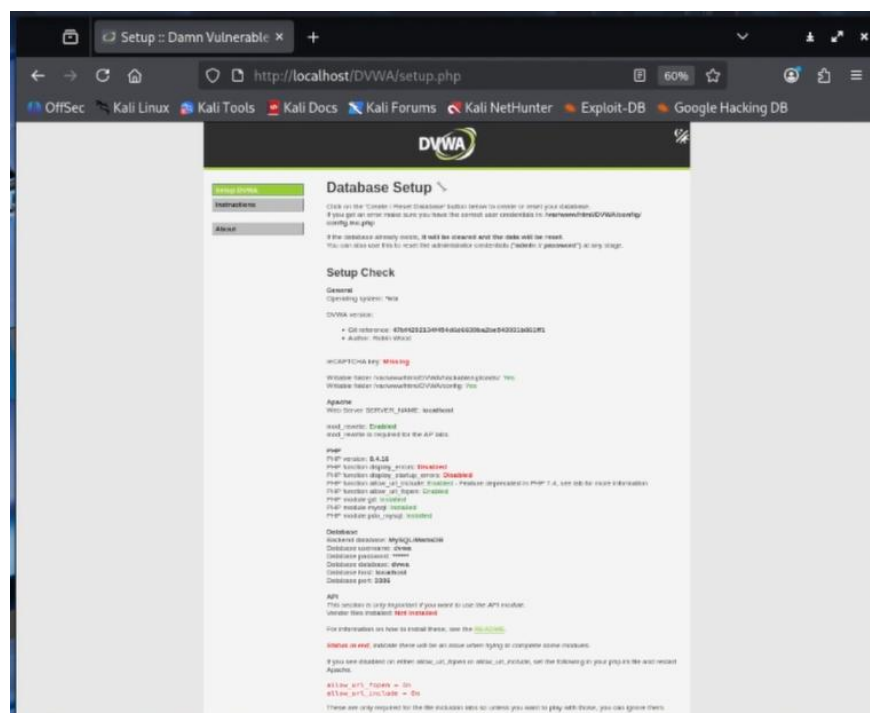


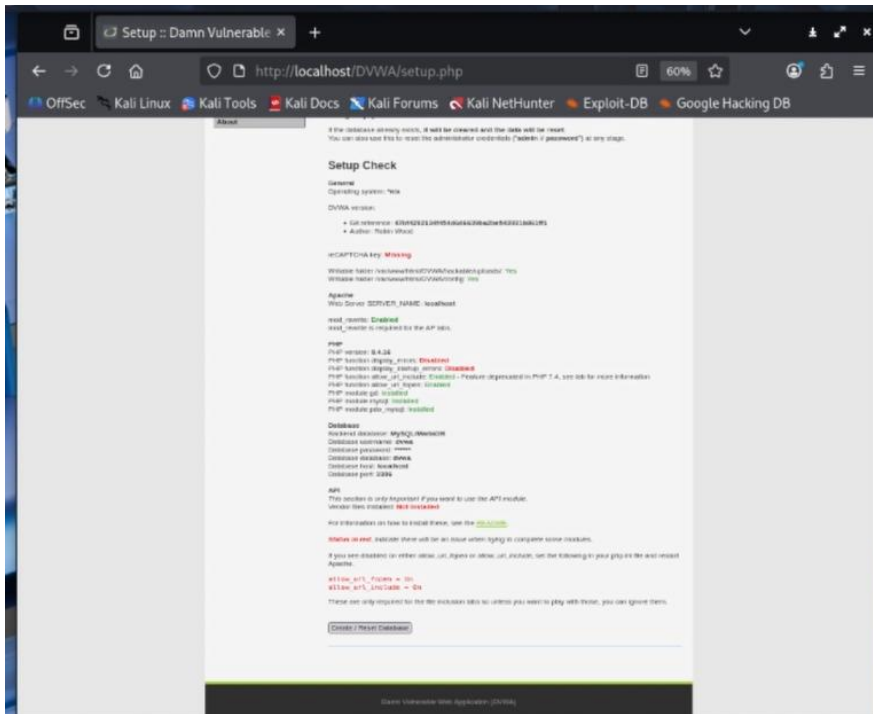
## k. Mengakses DVWA melalui Browser



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.

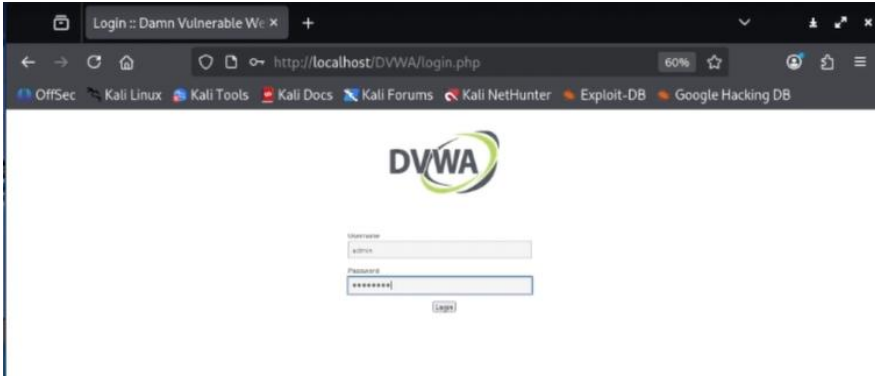
## 1. Melakukan Setup Check dan Reset Database





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.

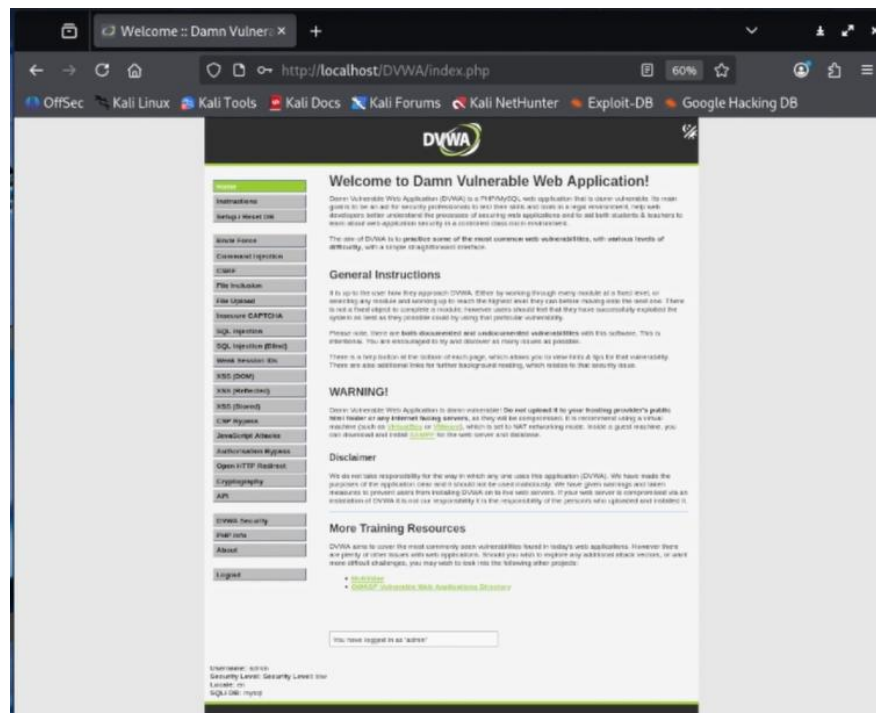
### m. Halaman Login Aplikasi



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



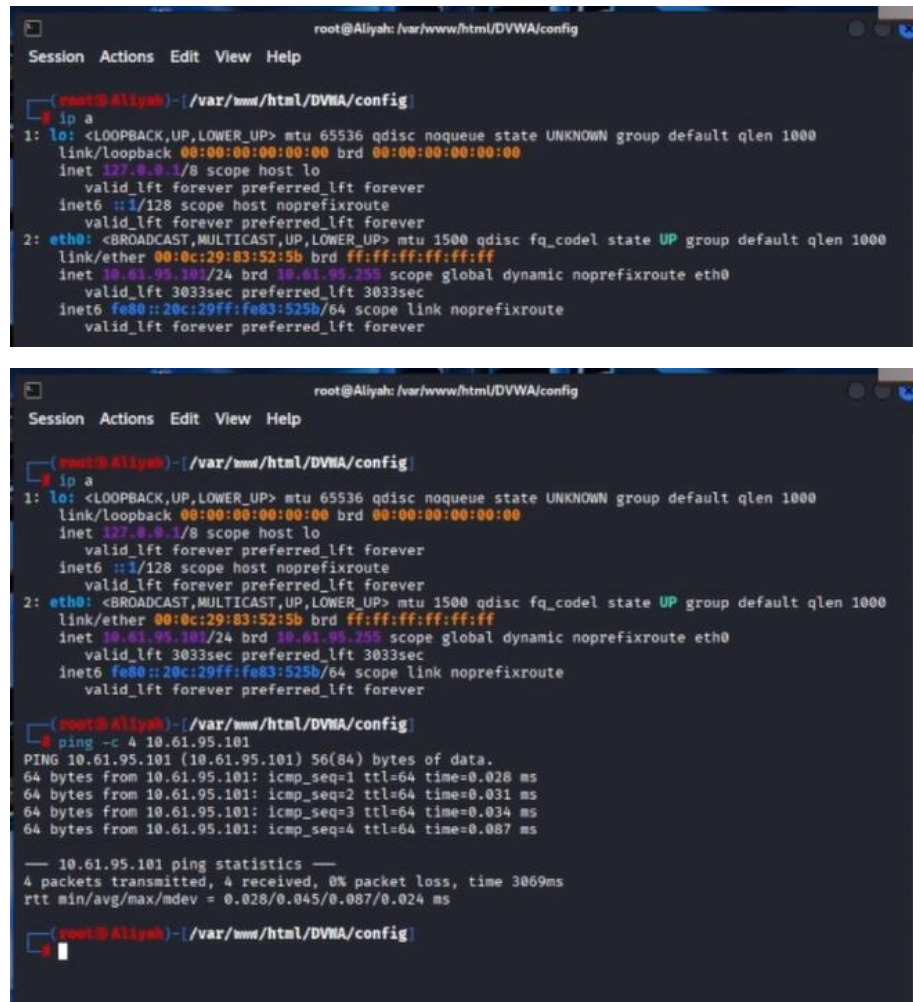
password default yaitu password. Klik **Login** untuk masuk ke dashboard utama.



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

## 2. Pengecekan Koneksi antar mesin virtual

### a. Mengecek Alamat IP Sistem



```
root@Aliyah: /var/www/html/DVWA/config

Session Actions Edit View Help

root@Aliyah: /var/www/html/DVWA/config
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 00:0c:29:83:52:5b brd ff:ff:ff:ff:ff:ff
   inet 10.61.95.101/24 brd 10.61.95.255 scope global dynamic noprefixroute eth0
       valid_lft 3033sec preferred_lft 3033sec
   inet6 fe80::20c:29ff:fe83:525b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

root@Aliyah: /var/www/html/DVWA/config
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 00:0c:29:83:52:5b brd ff:ff:ff:ff:ff:ff
   inet 10.61.95.101/24 brd 10.61.95.255 scope global dynamic noprefixroute eth0
       valid_lft 3033sec preferred_lft 3033sec
   inet6 fe80::20c:29ff:fe83:525b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

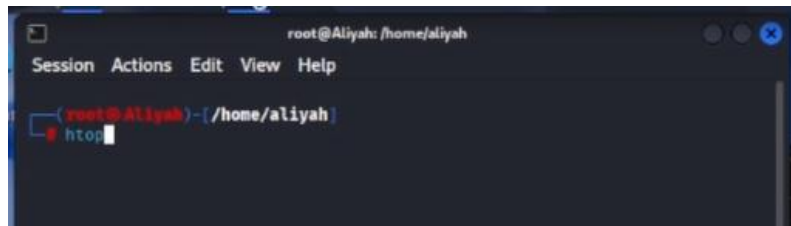
root@Aliyah: /var/www/html/DVWA/config
ping -c 4 10.61.95.101
PING 10.61.95.101 (10.61.95.101) 56(84) bytes of data:
64 bytes from 10.61.95.101: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 10.61.95.101: icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from 10.61.95.101: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 10.61.95.101: icmp_seq=4 ttl=64 time=0.087 ms

— 10.61.95.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.028/0.045/0.087/0.024 ms

root@Aliyah: /var/www/html/DVWA/config
```

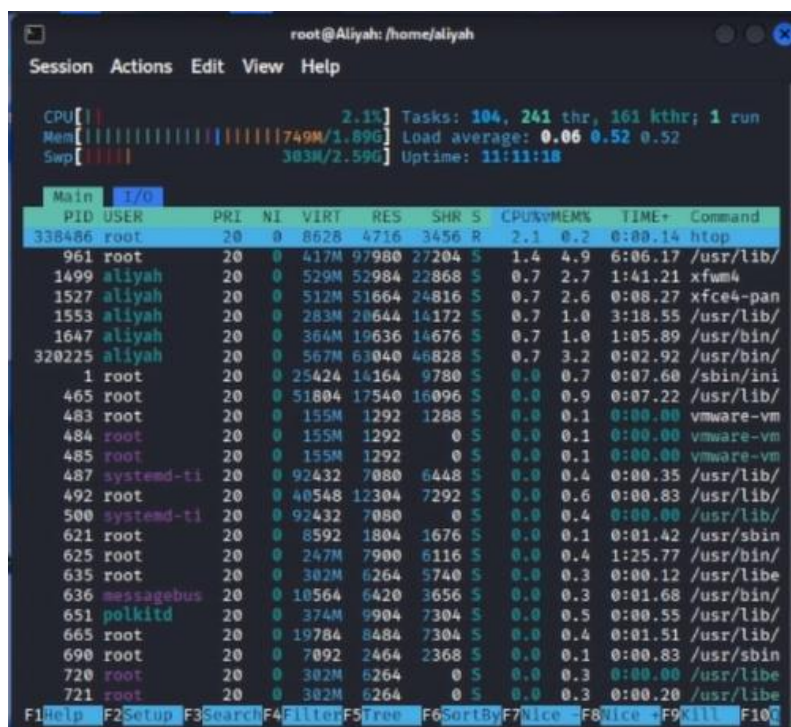
Setelah instalasi selesai, kita perlu mengetahui alamat IP lokal mesin tersebut agar bisa diakses oleh perangkat lain dalam jaringan yang sama. Perintah ip a digunakan untuk menampilkan informasi antarmuka jaringan. Terlihat pada gambar, mesin memiliki alamat IP 10.61.95.101 pada antarmuka eth0. Untuk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

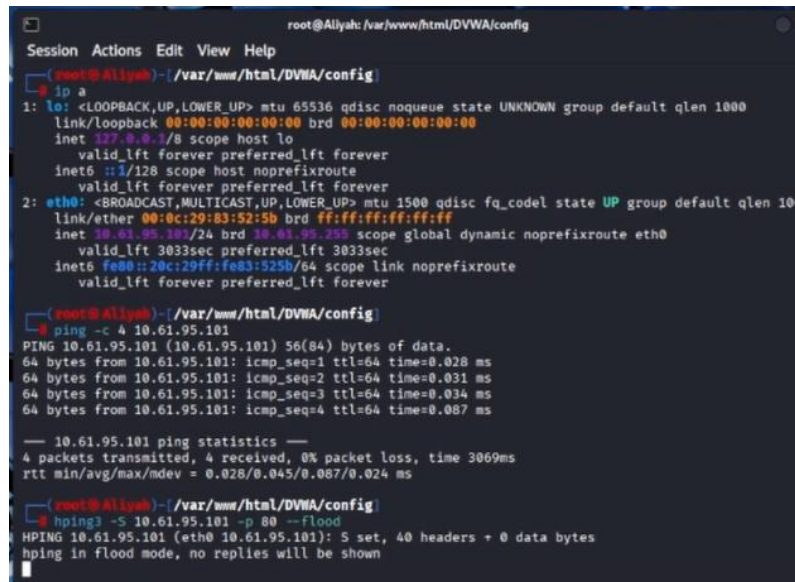
- ### c. Memantau Penggunaan Sumber Daya (CPU & RAM)



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



```
root@Aliyah: /var/www/html/DVWA/config
Session Actions Edit View Help
root@Aliyah)~[/var/www/html/DVWA/config]
# 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 00:0c:29:83:52:5b brd ff:ff:ff:ff:ff:ff
    inet 10.61.95.101/24 brd 10.61.95.255 scope global dynamic noprefixroute eth0
        valid_lft 3033sec preferred_lft 3033sec
    inet6 fe80::20c:29ff:fe83:525b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

root@Aliyah)~[/var/www/html/DVWA/config]
# ping -c 4 10.61.95.101
PING 10.61.95.101 (10.61.95.101) 56(84) bytes of data:
64 bytes from 10.61.95.101: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 10.61.95.101: icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from 10.61.95.101: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 10.61.95.101: icmp_seq=4 ttl=64 time=0.087 ms

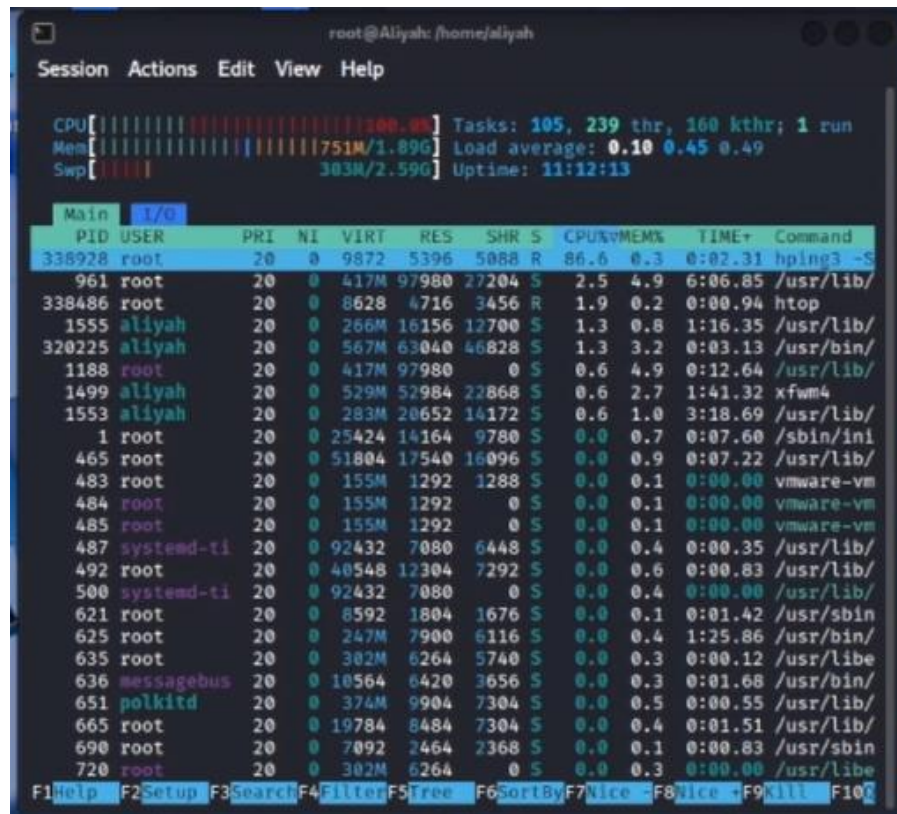
--- 10.61.95.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.028/0.045/0.087/0.024 ms

root@Aliyah)~[/var/www/html/DVWA/config]
# hping3 -S 10.61.95.101 -p 80 --flood
HPING 10.61.95.101 (eth0 10.61.95.101): 5 set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

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%)

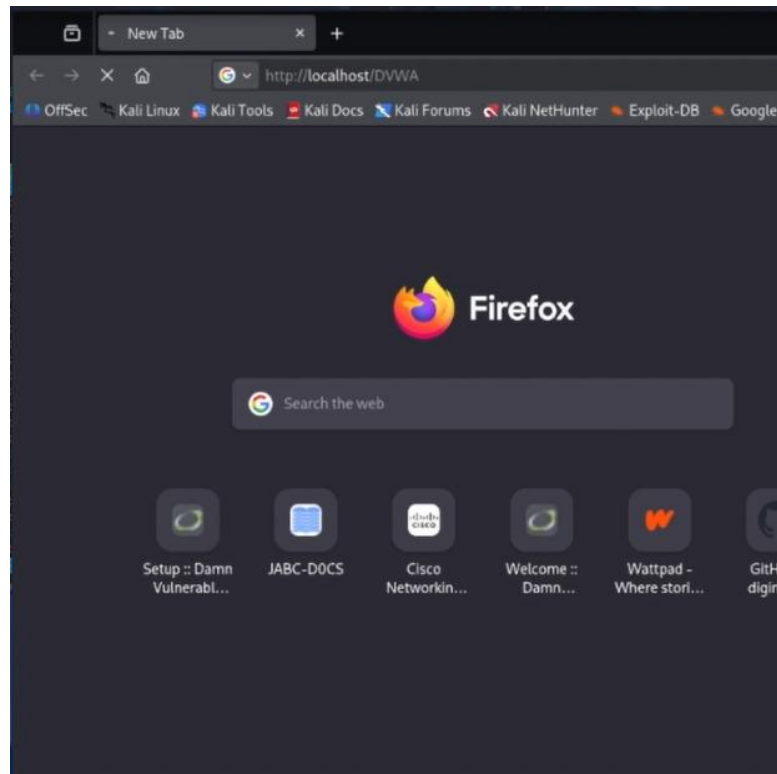


Segera setelah serangan diluncurkan, alat monitoring htop menunjukkan dampak yang drastis. Indikator bar CPU berubah menjadi warna merah penuh dan mencapai nilai 100.0%. Hal ini membuktikan bahwa proses hping3 (PID 338928) telah memakan seluruh daya komputasi yang tersedia, yang merupakan ciri khas dari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

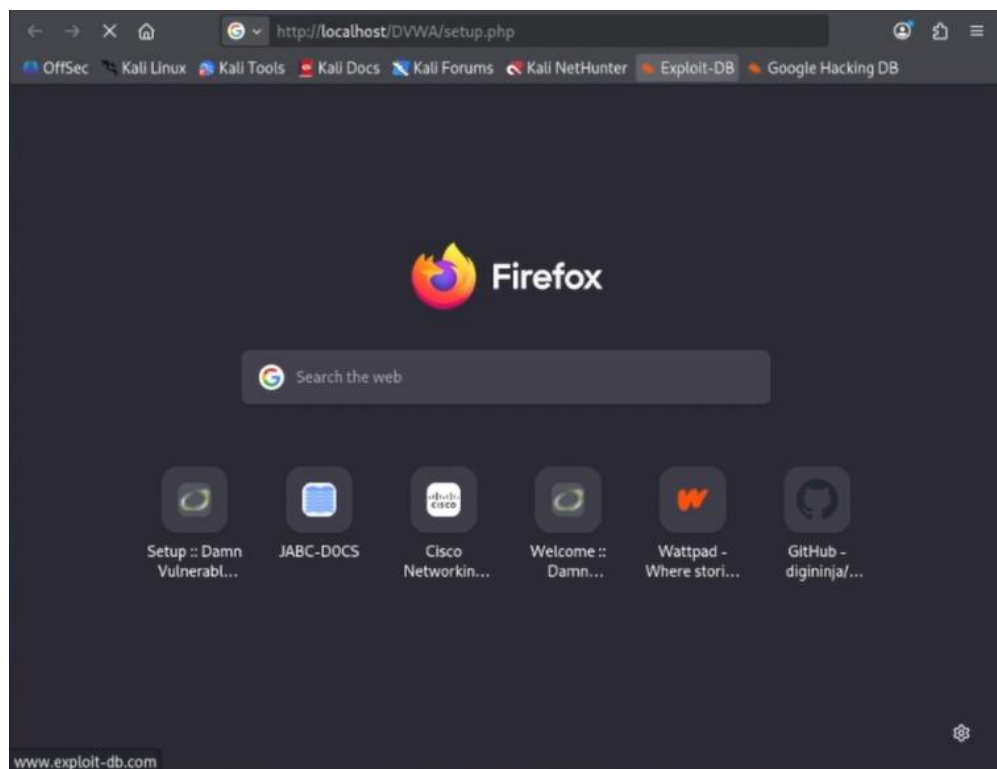
## 5. Simulasi Serangan Slowloris

```
(root@Aliyah)~# ./var/www/html/DVWA/config
# slowloris 10.61.95.101
[28-12-2025 22:30:54] Attacking 10.61.95.101 with 150 sockets.
[28-12-2025 22:30:54] Creating sockets ...
[28-12-2025 22:31:04] Sending keep-alive headers ...
[28-12-2025 22:31:04] Socket count: 4
[28-12-2025 22:31:04] Creating 146 new sockets ...
```



Setelah pengujian dengan paket SYN, dilakukan simulasi serangan Layer 7 menggunakan alat Slowloris 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)

```
(root@Aliyah)~[/var/www/html/DVWA/config]
# iptables -F
(root@Aliyah)~[/var/www/html/DVWA/config]
# iptables -X
```

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

```
(root@Aliyah)~[/var/www/html/DVWA/config]
# iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
(root@Aliyah)~[/var/www/html/DVWA/config]
# iptables -A INPUT -p tcp --dport 80 -j DROP
```

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

```
(root@Aliyah)-[/var/www/html/DVWA/config]
# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/second -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

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

```
(root@Aliyah)-[/var/www/html/DVWA/config]
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_echo_ignore_broadcasts = 1
#
```

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

```
(root@Aliyah)-[/var/www/html/DVWA/config]
# iptables -L -v -n
Chain INPUT (policy ACCEPT 29 packets, 7385 bytes)
 pkts bytes target    prot opt in     out     source                   destination
  0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0                0.0.0.0/0          tcp dpt:80
 limit: avg 25/min burst 100
  0      0 DROP      tcp  --  *      *       0.0.0.0/0                0.0.0.0/0          tcp dpt:80
  0      0 ACCEPT    icmp --  *      *       0.0.0.0/0                0.0.0.0/0          icmp type 8
 limit: avg 1/sec burst 5
  0      0 DROP      icmp --  *      *       0.0.0.0/0                0.0.0.0/0          icmp type 8

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

(root@Aliyah)-[/var/www/html/DVWA/config]
```

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)

```
(root@Aliyah)-[/var/www/html/DVWA/config]
# netstat -an | grep :80 | wc -l
2
```

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.