

# LAPORAN PROJECT KEAMANAN JARINGAN

## IMPLEMENTASI IDS SURICATA PADA WEB SERVER

### I. TUJUAN

Adapun tujuan praktikum :

1. Memahami konsep dan implementasi Intrusion Detection System (IDS) menggunakan Suricata pada sebuah web server.
2. Menganalisis efektivitas Suricata dalam mendeteksi dan berpotensi mencegah berbagai jenis serangan terhadap web server.
3. Memahami konsep dan implementasi firewall menggunakan Firewalld dalam mengamankan web server.
4. Membandingkan tingkat keamanan web server sebelum dan sesudah implementasi IDS Suricata dan Firewall (Firewalld) terhadap berbagai jenis serangan.

### II. DASAR TEORI

#### A. Sistem Pencegahan Intrusi (Intrusion Prevention System - IDS)

Sistem Deteksi Intrusi (IDS) adalah teknologi keamanan yang memantau aktivitas jaringan atau sistem untuk mengidentifikasi tanda-tanda ancaman siber atau pelanggaran kebijakan, lalu memberikan peringatan kepada administrator. Suricata adalah IDS open source berkinerja tinggi yang juga dapat berfungsi sebagai Sistem Pencegahan Intrusi (IPS). Ia bekerja dengan menganalisis lalu lintas jaringan secara mendalam (Deep Packet Inspection) dan menggunakan aturan berbasis tanda tangan untuk mendeteksi pola serangan yang dikenal. Meskipun utamanya berbasis tanda tangan, Suricata juga memiliki kemampuan terbatas untuk deteksi anomali melalui analisis flow dan dapat mengidentifikasi protokol secara otomatis.

Sebagai IDS, Suricata hanya akan mendeteksi serangan dan mencatatnya dalam log, sementara sebagai IPS, ia akan secara otomatis memblokir atau menjatuhkan lalu lintas berbahaya yang terdeteksi. Suricata memanfaatkan multi-threading untuk pemrosesan cepat, menghasilkan log yang komprehensif, dan sangat fleksibel dalam penyebarannya, menjadikannya alat penting untuk memantau, mendeteksi, dan mencegah berbagai ancaman dalam keamanan jaringan.

#### B. Web Server

Web server adalah komponen inti dalam arsitektur web yang berfungsi sebagai perantara antara browser pengguna dan konten situs web. Secara teknis, ini adalah perangkat lunak yang bertugas menyimpan berkas situs, memproses permintaan klien, dan mengirimkan halaman web kembali. Beberapa web server yang paling umum digunakan dan telah lama menjadi fondasi internet adalah Apache HTTP Server (Apache2) dan Nginx.

Selain web server tradisional, Caddy muncul sebagai pilihan modern yang menonjol karena kemudahan konfigurasinya dan fitur bawaan yang canggih. Keunggulan utamanya adalah manajemen sertifikat SSL/TLS otomatis melalui Let's Encrypt, yang menyederhanakan implementasi HTTPS. Caddy juga mendukung HTTP/2 secara default dan sangat serbaguna, mampu berfungsi sebagai reverse proxy, load balancer, atau file server.

Meskipun fundamental, web server sangat rentan terhadap berbagai jenis serangan siber. Ini termasuk SQL injection, Cross-Site Scripting (XSS), directory

traversal, dan serangan brute-force, serta eksploitasi kerentanan pada perangkat lunak server itu sendiri. Oleh karena itu, pengamanan web server—apakah itu Apache, Nginx, Caddy, atau lainnya—adalah hal yang sangat penting untuk melindungi data sensitif, menjaga kelangsungan layanan web, dan mencegah penyalahgunaan server.

### C. Implementasi IPS pada Web Server dengan Suricata

Sistem Deteksi Intrusi (IDS) adalah teknologi keamanan yang memantau aktivitas jaringan atau sistem untuk mengidentifikasi tanda-tanda ancaman siber atau pelanggaran kebijakan, lalu memberikan peringatan kepada administrator. Suricata adalah IDS open source berkinerja tinggi yang juga dapat berfungsi sebagai Sistem Pencegahan Intrusi (IPS). Ia bekerja dengan menganalisis lalu lintas jaringan secara mendalam (Deep Packet Inspection) dan menggunakan aturan berbasis tanda tangan untuk mendeteksi pola serangan yang dikenal. Meskipun utamanya berbasis tanda tangan, Suricata juga memiliki kemampuan terbatas untuk deteksi anomali melalui analisis flow dan dapat mengidentifikasi protokol secara otomatis.

Implementasi Suricata sebagai IDS pada web server melibatkan pemantauan lalu lintas HTTP/HTTPS yang masuk dan keluar untuk mendeteksi berbagai ancaman web seperti SQL Injection atau XSS. Ketika Suricata mendeteksi aktivitas yang cocok dengan aturan serangan, ia akan menghasilkan alert (peringatan) dan mencatatnya dalam log, yang berisi informasi penting untuk analisis forensik. Dalam mode IDS, Suricata hanya mendeteksi dan memberi peringatan, tidak secara otomatis memblokir serangan, namun tetap menyediakan visibilitas kritis dan peringatan dini bagi administrator keamanan.

### D. Firewalld

Firewalld adalah aplikasi firewall dinamis yang menyediakan manajemen firewall dengan dukungan untuk network zones untuk menetapkan tingkat kepercayaan yang berbeda untuk koneksi jaringan. Ini merupakan implementasi firewall berbasis netfilter yang umum digunakan pada sistem operasi Linux modern. Firewalld memungkinkan pengelolaan aturan firewall yang fleksibel tanpa perlu me-restart layanan firewall secara keseluruhan setiap kali ada perubahan konfigurasi. Konsep zones (seperti public, private, dmz) memudahkan administrator untuk menerapkan kebijakan keamanan yang berbeda berdasarkan lingkungan jaringan tempat antarmuka jaringan terhubung. Aturan-aturan dalam firewalld dapat berupa izin atau penolakan lalu lintas berdasarkan port, protokol, alamat sumber, dan layanan. Dalam konteks keamanan web server, firewalld dapat digunakan untuk membatasi akses hanya ke port-port yang diperlukan (misalnya, port 80 untuk HTTP dan 443 untuk HTTPS) dan membatasi akses dari jaringan yang tidak terpercaya.

### E. Port Scanning

Port scanning adalah teknik dasar dalam keamanan jaringan yang digunakan untuk mengidentifikasi port-port yang terbuka atau "mendengarkan" pada sebuah host atau server. Setiap port digital mewakili sebuah endpoint komunikasi yang diasosiasikan dengan layanan atau aplikasi tertentu (misalnya, port 80 untuk web server HTTP, port 22 untuk SSH). Proses scanning ini melibatkan pengiriman paket jaringan ke port target dan menganalisis respons yang diterima. Respons ini memungkinkan penyerang atau auditor keamanan untuk menyimpulkan status port tersebut: apakah ia "terbuka" (layanan aktif dan siap menerima koneksi), "tertutup"

(tidak ada aplikasi yang mendengarkan pada port tersebut, namun host merespons), atau "di filter" (paket diblokir oleh firewall tanpa respons yang jelas).

Tujuan port scanning bervariasi, mulai dari pemetaan jaringan untuk memahami asset yang ada, mengidentifikasi layanan yang berjalan, hingga mencari celah keamanan yang potensial. Berbagai metode scanning digunakan, seperti SYN scan (juga dikenal sebagai "half-open scan" karena tidak menyelesaikan three-way handshake TCP penuh), UDP scan, atau full connect scan. Alat seperti Nmap dan Masscan adalah contoh populer yang mengimplementasikan metode-metode ini. Meskipun port scanning sendiri bukanlah serangan, informasi yang diperoleh dari scan tersebut seringkali menjadi langkah awal penting dalam fase pengintaian (reconnaissance) dari serangan siber yang lebih kompleks, karena memberikan penyerang gambaran tentang permukaan serangan yang tersedia.

#### F. Brute Force

Brute force attack adalah metode serangan siber yang melibatkan upaya mencoba setiap kemungkinan kombinasi karakter secara sistematis untuk menebak kredensial (seperti username dan password) atau kunci enkripsi. Tujuannya adalah untuk mendapatkan akses tidak sah ke sebuah sistem, akun, atau data yang dilindungi. Serangan ini mengandalkan kekuatan komputasi untuk menghasilkan dan menguji kombinasi karakter yang tak terhitung jumlahnya hingga menemukan yang benar. Meskipun terkadang lambat dan memerlukan daya komputasi yang signifikan, brute force dapat menjadi sangat efektif jika target tidak memiliki perlindungan yang memadai, seperti kebijakan password yang lemah atau mekanisme lockout akun setelah beberapa kali percobaan gagal.

Ada beberapa variasi dari serangan brute force, termasuk dictionary attack (mencoba password dari daftar kata umum atau yang bocor), credential stuffing (menggunakan kombinasi username dan password yang bocor dari satu situs untuk mencoba masuk ke situs lain), dan reverse brute force (menggunakan satu password yang umum dan mencoba banyak username). Pencegahan terhadap serangan brute force melibatkan penggunaan password yang kuat dan kompleks, implementasi kebijakan lockout akun (misalnya, memblokir akun setelah beberapa percobaan gagal), penggunaan Multi-Factor Authentication (MFA), serta penerapan CAPTCHA atau mekanisme rate limiting untuk membatasi jumlah percobaan login dalam periode waktu tertentu.

#### G. Network Sniffing dengan Wireshark dan TCPdump

Network sniffing adalah proses menangkap dan menganalisis lalu lintas data yang mengalir melalui koneksi jaringan, memungkinkan pengamat melihat detail paket seperti protokol, alamat, port, dan muatan data. Aktivitas ini dapat digunakan baik untuk tujuan ofensif, seperti mencegat kredensial yang tidak terenkripsi, maupun defensif, seperti menganalisis pola serangan atau mendiagnosa masalah jaringan. Konsep dasarnya adalah "mendengarkan" komunikasi jaringan yang sedang berlangsung.

Untuk melakukan sniffing, dua alat utama adalah Wireshark dan tcpdump. Wireshark adalah network protocol analyzer berbasis antarmuka grafis (GUI) yang sangat populer. Ia memungkinkan pengguna untuk melihat data secara real-time, menganalisisnya secara detail dengan fitur penyaringan dan visualisasi yang kaya,

serta mendekode ribuan protokol. Ini menjadikannya alat tak ternilai untuk memahami protokol, mendiagnosis masalah keamanan atau kinerja, dan investigasi insiden.

Di sisi lain, tcpdump adalah packet analyzer berbasis baris perintah yang juga kuat dan serbaguna. Ideal untuk lingkungan tanpa GUI atau untuk otomatisasi, tcpdump dapat menangkap paket berdasarkan aturan penyaringan kompleks dan menyimpan hasilnya dalam file .pcap untuk analisis lebih lanjut. Kedua tool ini sangat efektif dalam memantau dan menganalisis komunikasi jaringan, namun penting untuk selalu diingat bahwa melakukan sniffing tanpa izin atau dasar hukum yang jelas dapat dianggap ilegal dan tidak etis.

## H. Distributed Denial of Service (DDoS)

Serangan Distributed Denial of Service (DDoS) adalah upaya jahat untuk membuat layanan online tidak tersedia dengan membanjiri target atau infrastruktur di sekitarnya dengan lalu lintas internet dari berbagai sumber yang terdistribusi secara geografis. Tujuannya adalah menguras sumber daya server atau jaringan hingga tidak mampu lagi merespons permintaan yang sah dari pengguna, sehingga mengakibatkan layanan terhenti. Berbeda dengan serangan Denial of Service (DoS) biasa yang berasal dari satu sumber, DDoS memanfaatkan banyak perangkat yang terinfeksi (botnet) untuk melancarkan serangan secara simultan, menjadikannya lebih sulit dilacak, diblokir, dan diatasi.

Salah satu indikator utama dari serangan DDoS yang sedang berlangsung adalah peningkatan drastis pada waktu respon ping ke target. Ketika server dibanjiri dengan lalu lintas palsu, ia akan kesulitan memproses permintaan, menyebabkan paket ping membutuhkan waktu lebih lama untuk mencapai server dan kembali, atau bahkan hilang sama sekali (packet loss). Selain itu, server yang menjadi target serangan DDoS akan menunjukkan peningkatan tajam pada penggunaan CPU (dan juga memori atau bandwidth) karena server mencoba memproses volume lalu lintas yang sangat besar atau menjalankan proses untuk mengelola koneksi yang dibanjiri, meskipun sebagian besar adalah lalu lintas yang tidak sah. Kombinasi ping yang lambat atau gagal serta lonjakan penggunaan CPU adalah tanda-tanda klasik bahwa server sedang berada di bawah tekanan serangan DDoS.

## I. Web Scanning

Web scanning adalah proses sistematis untuk menganalisis aplikasi web (situs web) guna mengidentifikasi kerentanan keamanan, kesalahan konfigurasi, atau informasi sensitif yang dapat dieksplorasi oleh penyerang. Berbeda dengan port scanning yang berfokus pada port terbuka di level jaringan, web scanning beroperasi pada lapisan aplikasi (Layer 7), yaitu bagaimana aplikasi web itu sendiri dibangun dan berinteraksi. Tujuan utamanya adalah untuk menemukan kelemahan umum seperti SQL Injection, Cross-Site Scripting (XSS), Broken Authentication/Authorization, Security Misconfiguration, atau directory traversal, yang semuanya dapat membahayakan data pengguna dan integritas sistem.

Proses web scanning melibatkan pengiriman berbagai permintaan HTTP/HTTPS ke server target dan menganalisis respons yang diterima. Alat-alat seperti Nikto digunakan untuk mengidentifikasi kerentanan web server yang dikenal dan konfigurasi yang tidak aman, sementara tool seperti Dirb (atau Gobuster) berfokus pada penemuan direktori dan file tersembunyi yang mungkin tidak ter-link secara langsung namun dapat mengandung informasi sensitif. Informasi yang dikumpulkan

dari web scanning ini sangat penting dalam fase pengintaian dan vulnerability assessment untuk memahami permukaan serangan sebuah aplikasi web dan merencanakan langkah-langkah mitigasi yang tepat.

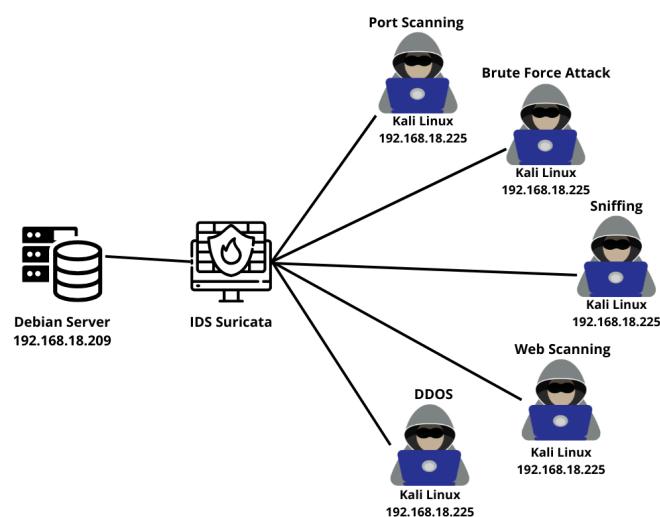
### III. PERALATAN

Adapun peralatan praktikum adalah :

1. Laptop
2. OS Kali Linux
3. OS Debian
4. Koneksi internet dan aplikasi browser

### IV. KEGIATAN PRAKTIKUM

#### Topologi



#### Konsep

Dalam praktikum ini akan dilakukan penyerangan terhadap Web Server Caddy. Penyerangan akan dilakukan lima kali dengan tools yang sudah dipilih. Beberapa penyerangan yang akan dilakukan yaitu port scanning, brute force attack, sniffing, DDOS, dan web scanning. Beberapa penyerangan yang akan dilakukan berkali-kali bertujuan untuk memberikan hasil yang akurat dan dapat dibandingkan satu sama lain. Akan dilakukan dua kali penyerangan, untuk yang pertama penyerangan secara langsung dan untuk yang kedua dilakukan penyerangan namun ditambahkan IDS Suricata untuk memantau lalu lintas jaringan yang mencurigakan dan melihat penyerangan yang dilakukan oleh penyerang.

#### Praktikum

##### A. Penyerangan

###### a. Install Web Server Caddy

1. Pastikan server Debian dan Kali Linux (penyerang) berada dalam satu jaringan yang sama. Lakukan ping antar perangkat untuk memastikan koneksi.
2. Selanjutnya install web server Caddy dengan perintah **sudo apt install caddy -y** lalu pastikan status layanan nya sudah aktif.

```

root@Debian:/var/www/html# sudo systemctl status caddy
● caddy.service - Caddy
   Loaded: loaded (/lib/systemd/system/caddy.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-06-01 21:39:08 EDT; 1h 4min ago
     Docs: https://caddyserver.com/docs/
  Process: 8260 ExecReload=/usr/bin/caddy reload --config /etc/caddy/Caddyfile --force (c
 Main PID: 5151 (caddy)
    Tasks: 11 (limit: 4631)
      Memory: 28.0M
        CPU: 2.227s
       CGroup: /system.slice/caddy.service
           └─5151 /usr/bin/caddy run --environ --config /etc/caddy/Caddyfile

Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2116768,"logger":"admin","msg":"Caddy v2.6.0 starting up on port 8260."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2149546,"logger":"admin","msg":"TLS configuration: 1 certificate(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"warn","ts":1748829280.2152522,"logger":"http","msg":"HTTP configuration: 1 site(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2154942,"logger":"http","msg":"TLS configuration: 1 certificate(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2154994,"logger":"tls","msg":"TLS configuration: 1 certificate(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.215568,"logger":"tls.ca","msg":"TLS configuration: 1 certificate(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2158773,"msg":"autosave configuration: 1 file(s) loaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.216755,"logger":"admin","msg":"Caddy successfully reloaded."}
Jun 01 21:54:40 Debian caddy[5151]: {"level":"info","ts":1748829280.2195277,"logger":"admin","msg":"Reloading caddy.service - Caddy."}
lines 1-22/22 (END)

```

- Mengedit beberapa konfigurasi web untuk proses login user pada file login.html, dashboard.php, dan auth.php.

```

farhan30@Debian:~ login
:aa GNU nano 7.2 login.html
<!DOCTYPE html>
<html><title>Login</title></head>
<body>
<form method="POST" action="/auth.php">
<label>Username:</label><input type="text" name="username"><br>
<label>Password:</label><input type="password" name="password"><br>
<button type="submit">Login</button>
</form>
</body>
</html>

```

```

farhan30@Debian:~ dashboard.php
:aa GNU nano 7.2
<?php
session_start();
if (!isset($_SESSION['login'])) {
    header("Location: /login.html");
    exit;
}
echo "Selamat datang, Admin!";
?>

```

```

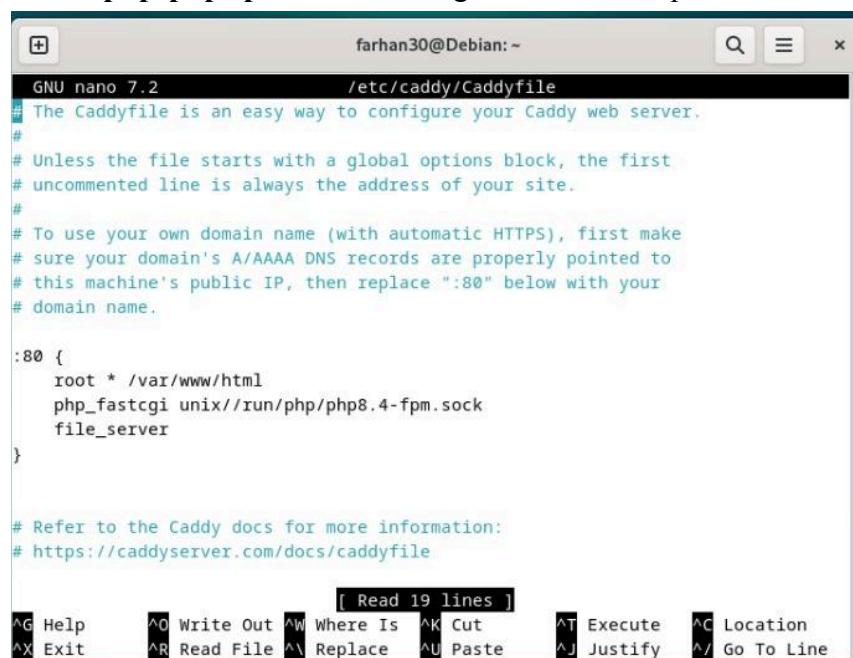
farhan30@Debian:~ auth.php
:aa GNU nano 7.2
<?php
session_start();
$user = $_POST['username'];
$pass = $_POST['password'];

if ($user === "admin" && $pass === "1234") {
    $_SESSION['login'] = true;
    header("Location: /dashboard.php");
    exit;
} else {
    echo "Login gagal.";
}
?>

```

- Mengedit konfigurasi pada Caddy file dengan menambahkan PHP-PFM, namun sebelumnya perlu menginstall PHP-FPM dengan perintah **sudo apt**

install php php-fpm. Hasil konfigurasi lalu disimpan dan direload kembali.



```
farhan30@Debian: ~
GNU nano 7.2          /etc/caddy/Caddyfile
# The Caddyfile is an easy way to configure your Caddy web server.
#
# Unless the file starts with a global options block, the first
# uncommented line is always the address of your site.
#
# To use your own domain name (with automatic HTTPS), first make
# sure your domain's A/AAAA DNS records are properly pointed to
# this machine's public IP, then replace ":80" below with your
# domain name.

:80 {
    root * /var/www/html
    php_fastcgi unix://run/php/php8.4-fpm.sock
    file_server
}

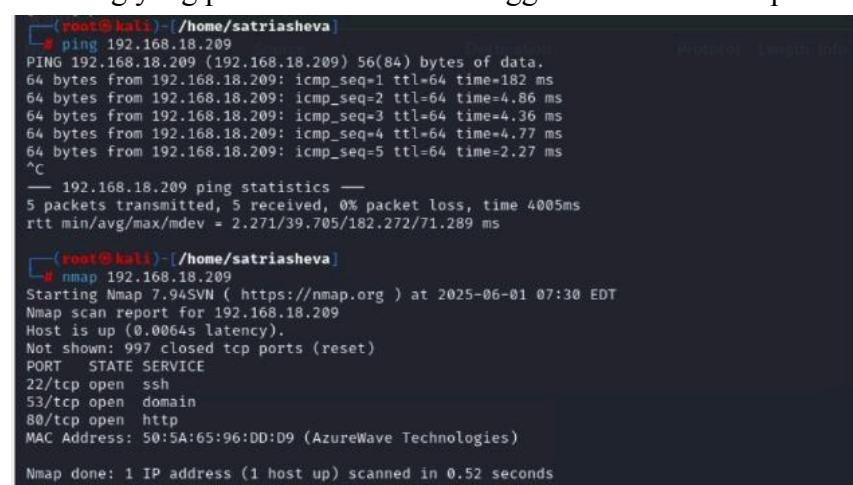
# Refer to the Caddy docs for more information:
# https://caddyserver.com/docs/caddyfile
```

5. Menjalankan web server Caddy di browser dengan ketik IP dari server Debian pada file login.html.



### b. Port Scanning

1. Penyerang melakukan port scanning pada Kali Linux terhadap port dan IP dari server Debian, dan dilakukan dengan dua tools berbeda yaitu Nmap dan Masscan.
2. Scanning yang pertama dilakukan menggunakan tools Nmap.



```
root@kali:~/home/satriasheva]
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=182 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=4.86 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=4.36 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=4.77 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=2.27 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.271/39.705/182.272/71.289 ms

root@kali:~/home/satriasheva]
# nmap 192.168.18.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 07:30 EDT
Nmap scan report for 192.168.18.209
Host is up (0.0064s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

```
(root㉿kali)-[~/home/satriasheva]
└─# nmap 192.168.18.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 07:30 EDT
Nmap scan report for 192.168.18.209
Host is up (0.0067s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

```
(root㉿kali)-[~/home/satriasheva]
└─# nmap 192.168.18.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 07:30 EDT
Nmap scan report for 192.168.18.209
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

```
(root㉿kali)-[~/home/satriasheva]
└─# nmap 192.168.18.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 07:30 EDT
Nmap scan report for 192.168.18.209
Host is up (0.0074s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

```
(root㉿kali)-[~/home/satriasheva]
└─# nmap 192.168.18.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 07:30 EDT
Nmap scan report for 192.168.18.209
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

### 3. Scanning yang kedua dilakukan menggunakan tools Masscan.

```
(root㉿kali)-[~/home/satriasheva]
└─# masscan -p80 192.168.18.209
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-01 11:33:17 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.18.209
```

```
(root㉿kali)-[~/home/satriasheva]
└─# masscan 192.168.18.209 -p80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-01 11:33:50 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.18.209
```

```
(root㉿kali)-[~/home/satriasheva]
└─# masscan 192.168.18.209 -p80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-01 11:34:15 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.18.209
```

```
[root@kali] ~[~/home/satriasheva]
# masscan 192.168.18.209 -p80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-01 11:34:30 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.18.209
```

```
[root@kali] ~[~/home/satriasheva]
# masscan 192.168.18.209 -p80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-01 11:34:44 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.18.209
```

### c. Brute Force

- Brute force untuk mencari username dan password user dilakukan dengan menggunakan dua tools yang berbeda, yaitu Hydra dan Medusa.
- Menginstall tools Hydra dan Medusa terlebih dahulu di Kali Linux.
- Membuat word list username bernama **username.txt** yang berisi list username yang akan dicoba.

```
root@kali: /home/satriasheva
username.txt *
GNU nano 7.2
ameng
admin
dafa
asep
abi
favian
rakha
leyan
arung
uhuy
keneo
farhab
kursi
yuli
ali
aldi
rakhana
```

- Membuat word list password bernama **password.txt** yang berisi list password yang akan dicoba.

```
root@kali: /home/satriasheva
password.txt *
GNU nano 7.2
admin123
12345
123
kera10
senggel122
poltek123
haha123
rakha123
pnm127
127187hs
korsai291
kipas5757
rumah12
lantai12
keramik12
uiuiii12
yfywqn21
yugubu12
126bjjhj
```

- Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username admin dan password admin123 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi.

```
[root@kali] ~[~/home/satriasheva]
# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username='USER'&password='PASS':Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:53:47
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:/1:p:1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username='USER'&password='PASS':Login
[80][http-post-form] host: 192.168.18.209 login: admin password: admin123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:53:48
```

6. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username dafa dan password senggel122 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi

```
[root@kali] ~ /home/satriasheva
# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username='USER'&password='PASS':Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:43:43
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1::1:p1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username='USER'&password='PASS':Login
[80][http-post-form] host: 192.168.18.209 login: dafa password: senggel122
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:44:44
```

7. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username abi dan password kera10 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi

```
[root@kali] ~ /home/satriasheva
# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username='USER'&password='PASS':Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:56:02
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1::1:p1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username='USER'&password='PASS':Login
[80][http-post-form] host: 192.168.18.209 login: abi password: kera10
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:56:03
```

8. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username asep dan password asep123 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi

```
[root@kali] ~ /home/satriasheva
# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username='USER'&password='PASS':Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:57:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1::1:p1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username='USER'&password='PASS':Login
[80][http-post-form] host: 192.168.18.209 login: asep password: asep123
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:57:25
```

9. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username ameng dan password 123 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi

```
[root@kali] ~ /home/satriasheva
# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username='USER'&password='PASS':Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:58:14
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1::1:p1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username='USER'&password='PASS':Login
[80][http-post-form] host: 192.168.18.209 login: ameng password: 123
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:58:14
```

10. Selanjutnya, menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username admin dan password admin123 berhasil dengan perintah **medusa -h 192.168.18.209 -u admin -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi

```
[root@kali]~[/home/satriasheva]
# 2025-06-04 05:40:43 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: admin (1 of 1,
2025-06-04 05:40:43 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: admin Password: admin123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

11. Melakukan menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username dafa dan password senggel122 berhasil dengan perintah **medusa -h 192.168.18.209 -u dafa -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi

```
[root@kali]~[/home/satriasheva]
# 2025-06-04 05:39:02 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: dafa (1 of 1
2025-06-04 05:39:02 ACCOUNT FOUND: [http] Host: 192.168.10.209 User: dafa Password: senggel122 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

12. Melakukan menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username abi dan password kera10 berhasil dengan perintah **medusa -h 192.168.18.209 -u abi -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi

```
[root@kali]~[/home/satriasheva]
# 2025-06-04 05:42:43 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: abi (1 of 1
2025-06-04 05:42:43 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: abi Password: kera10 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

13. Melakukan menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username asep dan password asep123 berhasil dengan perintah **medusa -h 192.168.18.209 -u asep -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi

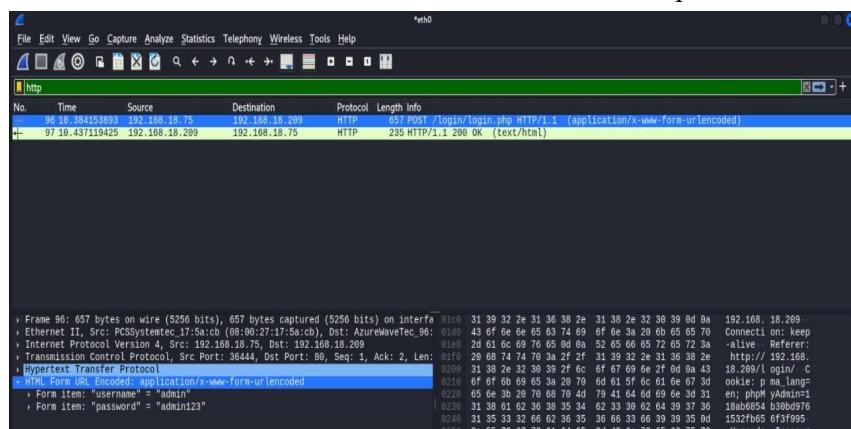
```
[root@kali]~[/home/satriasheva]
# 2025-06-04 05:45:37 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: asep (1 of 1
2025-06-04 05:45:37 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: asep Password: asep123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

14. Melakukan menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username ameng dan password 123 berhasil dengan perintah **medusa -h 192.168.18.209 -u ameng -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi

```
[root@kali]~[/home/satriasheva]
# 2025-06-04 05:44:55 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: ameng (1 of 1
2025-06-04 05:44:55 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: ameng Password: 123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

#### d. Sniffing

1. Sniffing dilakukan melalui dua tools yang berbeda, yaitu melalui Wireshark dan tcpdump.
2. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode HTTP POST adalah username: **admin** dan password: **admin123**.



3. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **dafa** dan password: **senggel122**.

No.	Time	Source	Destination	Protocol	Length	Info
11.5	12:00:00.8392	192.168.18.75	192.168.18.209	HTTP	654	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
12.5	13:04:06.4946	192.168.18.209	192.168.18.75	HTTP	226	200 OK (text/html)
18.13	3:26:17:66:78	192.168.18.75	192.168.18.209	HTTP	658	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
19.13	33:26:61:11:18	192.168.18.209	192.168.18.75	HTTP	234	200 OK (text/html)

```

Frame 18: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_17:5a:cb (08:00:27:17:5a:cb), Dst: AzureWaveTec_96 (01:00:43:6f:6e:66)
Internet Protocol Version 4, Src: 192.168.18.75, Dst: 192.168.18.209
Transmission Control Protocol, Src Port: 55854, Dst Port: 80, Seq: 589, Ack: 162, Len: 658
Hypertext Transfer Protocol
    HTML Form URL Encoded: application/x-www-form-urlencoded
        Form item: "username" = "dafa"
        Form item: "password" = "senggel122"

```

4. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **abi** dan password: **kera10**.

No.	Time	Source	Destination	Protocol	Length	Info
28.10	4:02:54:69:78	192.168.18.75	192.168.18.209	HTTP	653	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
30.10	4:07:18:19:22	192.168.18.209	192.168.18.75	HTTP	233	200 OK (text/html)

```

Frame 28: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_17:5a:cb (08:00:27:17:5a:cb), Dst: AzureWaveTec_96 (01:00:43:6f:6e:66)
Internet Protocol Version 4, Src: 192.168.18.75, Dst: 192.168.18.209
Transmission Control Protocol, Src Port: 55854, Dst Port: 80, Seq: 1, Ack: 1, Len: 653
Hypertext Transfer Protocol
    HTML Form URL Encoded: application/x-www-form-urlencoded
        Form item: "username" = "abi"
        Form item: "password" = "kera10"

```

5. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **asep** dan password: **12345**.

No.	Time	Source	Destination	Protocol	Length	Info
http2	1:17:44:6255	192.168.18.209	192.168.18.75	HTTP	163	HTTP/1.1 404 Not Found
http3	.897662945	192.168.18.75	192.168.18.209	HTTP	656	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
175.29	.911054352	192.168.18.209	192.168.18.75	HTTP	226	200 OK (text/html)
177.30	.351211392	192.168.18.75	192.168.18.209	HTTP	439	GET /favicon.ico HTTP/1.1
179.30	.362826721	192.168.18.209	192.168.18.75	HTTP	163	HTTP/1.1 404 Not Found
211.39	.941882396	192.168.18.75	192.168.18.209	HTTP	653	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
213.39	.956229962	192.168.18.209	192.168.18.75	HTTP	226	200 OK (text/html)
216.40	.375977373	192.168.18.75	192.168.18.209	HTTP	439	GET /favicon.ico HTTP/1.1
218.40	.681517314	192.168.18.209	192.168.18.75	HTTP	163	HTTP/1.1 404 Not Found
232.40	.681517314	192.168.18.75	192.168.18.209	HTTP	439	GET /favicon.ico HTTP/1.1
234.45	.686050569	192.168.18.209	192.168.18.75	HTTP	163	HTTP/1.1 404 Not Found
446.53	.483947099	192.168.18.75	192.168.18.209	HTTP	657	POST /login/login.php HTTP/1.1 (application/x-www-form-urlencoded)
447.53	.494226483	192.168.18.209	192.168.18.75	HTTP	226	200 OK (text/html)
455.54	.352096733	192.168.18.75	192.168.18.209	HTTP	439	GET /favicon.ico HTTP/1.1
457.54	.363409574	192.168.18.209	192.168.18.75	HTTP	163	HTTP/1.1 404 Not Found

```

Frame 73: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_17:5a:cb (08:00:27:17:5a:cb), Dst: AzureWaveTec_96 (01:00:43:6f:6e:66)
Internet Protocol Version 4, Src: 192.168.18.75, Dst: 192.168.18.209
Transmission Control Protocol, Src Port: 55854, Dst Port: 80, Seq: 1, Ack: 2, Len: 653
Hypertext Transfer Protocol
    HTML Form URL Encoded: application/x-www-form-urlencoded
        Form item: "username" = "asep"
        Form item: "password" = "12345"

```

6. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **ameng** dan password: **123**.

The screenshot displays a Wireshark interface with the following details:

- Network Interface:** \*eth0
- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Includes icons for file operations, search, and zoom.
- Selected Protocol:** http
- Packets List:** Shows two captured packets:
  - Packet 24: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface eth0 at 08:27:17.5a:cb from source 192.168.18.269 to destination 192.168.18.209 via Ethernet II, Src: PCSSystemtec\_17:5a:cb (08:27:17:5a:cb), Dst: AzureWaveTec\_96 (08:00:27:17:5a:cb). Protocol: HTTP. Length: 652. Info: 652 POST /login/login.php HTTP/1.1 (text/html).
  - Packet 26: 235 bytes on wire (1920 bits), 235 bytes captured (1920 bits) on interface eth0 at 08:27:17.5a:cb from source 192.168.18.269 to destination 192.168.18.209 via Ethernet II, Src: PCSSystemtec\_17:5a:cb (08:27:17:5a:cb), Dst: AzureWaveTec\_96 (08:00:27:17:5a:cb). Protocol: HTTP. Length: 235. Info: 235 HTTP/1.1 200 OK (text/html)
- Details Pane:** Shows the structure of the selected packet (Frame 24).
  - Frame 24: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface eth0 at 08:27:17.5a:cb from source 192.168.18.269 to destination 192.168.18.209 via Ethernet II, Src: PCSSystemtec\_17:5a:cb (08:27:17:5a:cb), Dst: AzureWaveTec\_96 (08:00:27:17:5a:cb).
  - Internet Protocol Version 4, Src: 192.168.18.75, Dst: 192.168.18.209
  - Transmission Control Protocol, Src Port: 43284, Dst Port: 80, Seq: 1, Ack: 1, Len: 652
  - Hypertext Transfer Protocol
  - HTTP Form URL Encoded; application/x-www-form-urlencoded
    - Form item: "username" = "Ameng"
    - Form item: "password" = "123"
- Bytes Pane:** Displays the raw hex and ASCII data for the selected frame.

7. Sniffing melalui tcpdump yang dilakukan pada saat user login ke web server dengan perintah **sudo tcpdump -r login\_form.pcap -X**.

8. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **admin** dan password: **admin123**.

```
0x0230: 3738 3135 3332 6662 3635 3666 3366 3939 761512fb656f3f99
0x0240: 3508 0455 7067 2761 6465 2d49 6e73 6565 5 ..Upgrade-Insec
0x0250: 7572 653d 5265 7175 6573 7473 3a20 318d ure-Requests-1.
0x0260: 7573 6575 7385 2766 6166 653d 6184 6659 4 ..username=admin
0x0270: 6e26 7061 7373 7767 7264 3d61 646d 696e nopassword=admin
0x0280: 2132 33 .....123
06:17:89 67:0085 IP 192.168.16.209.45706: Flags [P..], seq 1:170, ack 591, win 505, options [nop,nop,T5 val 3680335072 ecr 45167245
0x0000: 4500 00dd 94cc 4009 4006 fee8 c08 12d1 E.....@.R..;
0x0010: c0a8 124b 0050 b2ba 08c3 b3b6 3b88 ....K.P.....];
0x0020: 8018 01ff b2d1 0000 0101 080a db5d 74e0 .....L.....];
0x0030: 1aeb f976 4854 5450 2f31 2e31 2023 3038 ...vHTTP/1.1.200
0x0040: 20af shrd 0a31 67fc 7465 6e74 2f54 7978 OK Content-Typ
```

9. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **dafa** dan password: **senggel122**.

```
0#0x20: 3736 3135 3332 6662 3635 3666 3369 3939 7f6332fb65bb199
0#0x240: 358d 0a55 7667 7261 6465 2649 6673 5653 5 ..Request-Insec
0#0x250: 7572 6526 5265 7175 6573 7473 3249 3108 ure-Requests:.1.
0#0x260: 0a4d 0a75 7365 7266 616d 653d 6461 6661 ...username=dafa
0#0x270: 2670 6173 7377 6f72 643d 7365 6667 6765 6password=sengge
0#0x280: 6c31 3232 l122
06:19:04: 256537 [192.168.16.108]:443 [http://192.168.16.108:443] Flags [P..], seq 1:169, ack 592, win 505, options [nop,nop,TSL val 3680449853 ecr 45178
0#0x000: 458b 00dc b3a8 4004 4006 e02a c0a8 12d4 E.....@.0.*.**.
0#0x010: c0ab 1248 0050 8d4e b012 b860 ad99 984a B.P.K.N....` .. J
0#0x020: 8018 01ff c5bd 0000 0101 00ba d5f7 353d .....-*.-
0#0x030: 1ae9 9224 4854 5450 2f71 2e31 2832 3030 ... HTTP/1.1.200
0#0x040: 2fa4 f4bd 0a43 6f6e 7465 6e74 2454 2970 OK Content-Typ
```

10. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **abi** dan password: **kera10**.

```
0x0240: 3568 0a55 7067 7261 6465 2d49 6e73 6561 ..5..Upgrade-Insec
0x0250: 7572 652d 5265 7175 6573 7473 3a20 310d ..ure-Requests:1.
0x0260: 0a60 075 7365 26e6 616d 6561 6162 6926 ...username=a1b
0x0270: 0a60 075 7365 26e6 616d 6561 6162 6926 ...password=keral
06:19:11.961466 IP [REDACTED] 192.168.16.209.443 -> 192.168.16.75.36744, seq 1:168, ack 587, win 501, options [nop,nop,TS val 3680487553 ecr 4518246
0x0000: 4500 00b8 b400 4006 024 c0a8 12d1 E ..D..B..$.....
0x0010: c088 12ba 0058 8d4e b012 5908 ad90 9a95 ..K.P.N......
0x0020: 0818 01f5 def1 0000 01a8 080a db5f c881 ..... .....
0x0030: iaee 4bd8 4854 5450 2f31 2e31 2032 3030 ..K.HTTP/1.1.200
```

11. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **asep** dan password: **asep123**.

```
0x023d: 3736 3135 3332 6662 3635 3666 3366 3939 761532bf656f3f99
0x0240: 350d 0a55 7067 7261 6465 2049 6e73 6563 5..Upgrade-Insec
0x0250: 7572 652d 5265 7175 6573 7473 3a20 310d ure-Requests:.1.
0x0260: 0a0d 0a75 7365 726e 616d 653d 6173 6570 ...username=asep
0x0270: 2670 6173 7377 6f72 643d 6173 6570 3132 6password=asep12
0x0280: 33
                                3
06:20:34.896482 IP 192.168.18.209.http > 192.168.18.75.36174: Flags [P.], seq 321:489, ack 1767, win 501, options [nop,nop,TS val 36805402 OK
OK
0x0000: 4500 a000 b394 4008 e016 c0a8 12d1 E.....@.0.0.....
0x0010: c0a8 12a4 0000 8d4c b012 baef ad90 9632 ...K.P.N.....|
0x0020: 8018 01f5 d3f2 0000 0101 080a db60 9632 ...`2
0x0030: 1aef 1b42 4854 5450 2f31 2e31 2032 3030 ...BHHTP/1.1.200
```

12. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **ameng** dan password: **123**.

#### e. DDOS melalui Kali Linux

1. Melihat ping ke IP server terlebih dahulu sebelum dilakukan DDOS.

```
[root@ersahayuning13]~# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

2. Cek kondisi CPU dengan perintah top untuk memantau.

```
[+] farhan30@Debian: ~ %Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem: 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
  1 root 20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
  2 root 20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
  3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
  4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
  5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
  6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
11 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
12 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
13 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
14 root 20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0
```

```
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem: 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

 PID USER      PR  NI    VIRT    RES   SHR S %CPU %MEM TIME+ COMMAND
 1659 farhan30  20   0 3859216 282448 108576 S 18.8  7.0 32:04.97 gnome-shell
19806 root    20   0  11608 5004 3104 R  6.2  0.1 0:00.02 top
  1 root       20   0 102952 12628  8840 S  0.0  0.3 0:06.96 systemd
  2 root       20   0      0      0   0 S  0.0  0.0 0:00.03 kthreadd
  3 root       0 -20     0      0   0 I  0.0  0.0 0:00.00 rcu_gp
  4 root       0 -20     0      0   0 I  0.0  0.0 0:00.00 rcu_par_gp
  5 root       0 -20     0      0   0 I  0.0  0.0 0:00.00 slub_flushwq
  6 root       0 -20     0      0   0 I  0.0  0.0 0:00.00 netns
10 root     0 -20     0      0   0 I  0.0  0.0 0:00.00 mm_percpu_wq
 11 root       20   0      0      0   0 I  0.0  0.0 0:00.00 rcu_tasks_kthread
 12 root       20   0      0      0   0 I  0.0  0.0 0:00.00 rcu_tasks_rude_kthread
 13 root       20   0      0      0   0 I  0.0  0.0 0:00.00 rcu_tasks_trace_kthread
14 root     20   0      0      0   0 S  0.0  0.0 0:00.33 ksoftirqd/0
```

```
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem: 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

 PID USER      PR  NI    VIRT    RES   SHR S %CPU %MEM TIME+ COMMAND
 1659 farhan30 20  0 3859216 282448 108576 S 18.8  7.0 32:04.97 gnome-shell
19886 root    20  0 11608  5004 3104 R  6.2  0.1 0:00.62 top
  1 root      20  0 102952 12628 8840 S  0.0  0.3 0:06.96 systemd
  2 root      20  0      0      0  0 S  0.0  0.0 0:00.03 kthreadd
  3 root      0 -20     0      0  0 I  0.0  0.0 0:00.00 rcu_gp
  4 root      0 -20     0      0  0 I  0.0  0.0 0:00.00 rcu_par_gp
  5 root      0 -20     0      0  0 I  0.0  0.0 0:00.00 slab_flushwq
  6 root      0 -20     0      0  0 I  0.0  0.0 0:00.00 netns
10 root     0 -20     0      0  0 I  0.0  0.0 0:00.00 mm_percpu_wq
 11 root      20  0      0      0  0 I  0.0  0.0 0:00.00 rcu_tasks_kthread
 12 root      20  0      0      0  0 I  0.0  0.0 0:00.00 rcu_tasks_rude_kthread
 13 root      20  0      0      0  0 I  0.0  0.0 0:00.00 rcu_tasks_trace_kthread
 14 root      20  0      0      0  0 I  0.0  0.0 0:00.00 rcu_tasks_stay_kthred
```

```

farhan30@Debian:~%
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mib Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
Mib Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
1 root 20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
11 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
12 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
13 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
14 root 20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0

farhan30@Debian:~%
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mib Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
Mib Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
1 root 20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
11 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
12 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
13 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
14 root 20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0

```

### 3. Melakukan DDOS dengan perintah hping3 -S -p 80 --flood 192.168.18.209.

```

[root@ersahayuning13]# sudo hping3 -S -p 80 --flood 192.168.18.209 [AzureWave Technologies]
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and Service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13]# 

[root@ersahayuning13]# sudo hping3 -S -p 80 --flood 192.168.18.209 [AzureWave Technologies]
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and Service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13]# 

[root@ersahayuning13]# sudo hping3 -S -p 80 --flood 192.168.18.209 [AzureWave Technologies]
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and Service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13]# 

```

```

[root@ersahayuning13] ~
# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hpPing in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and Service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13] ~
# 

```

4. Cek kondisi CPU kembali dengan top setelah dilakukan DDOS. Kondisi CPU tidak ada perubahan signifikan.

```

farhan30@Debian:~
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
  1 root    20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
  2 root    20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
  3 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
  4 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
  5 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
  6 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
  10 root   0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
  11 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
  12 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
  13 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
  14 root   20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0

farhan30@Debian:~
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
  1 root    20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
  2 root    20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
  3 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
  4 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
  5 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
  6 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
  10 root   0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
  11 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
  12 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
  13 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
  14 root   20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0

farhan30@Debian:~
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1659 farhan30 20 0 3859216 282448 108576 S 18.8 7.0 32:04.97 gnome-shell
19806 root 20 0 11608 5004 3104 R 6.2 0.1 0:00.02 top
  1 root    20 0 102952 12628 8840 S 0.0 0.3 0:06.96 systemd
  2 root    20 0 0 0 0 S 0.0 0.0 0:00.03 kthreadd
  3 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
  4 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
  5 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 slab_flushwq
  6 root    0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
  10 root   0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
  11 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
  12 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
  13 root   20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
  14 root   20 0 0 0 0 S 0.0 0.0 0:03.32 ksoftirqd/0

```

%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
Mib Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache  
Mib Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0

5. Lihat ping nya kembali setelah dilakukan DDOS apakah ada perubahan atau tidak. Tidak ada perubahan yang signifikan pada hasil respon time pada ping.

```

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
From 192.168.18.209: icmp_seq=15 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

```

```
[root@arsahayuning11] ~
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[root@arsahayuning11] ~
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3
```

#### **f. Web Scanning**

1. Penyerang melakukan web scanning pada Kali Linux terhadap aplikasi web dari server Debian, dengan menggunakan dua tools yang berbeda yaitu Nikto dan Dirb.
  2. Web Scanning yang pertama dilakukan menggunakan tools Nikto.

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# nikto -h http://192.168.18.209
- Nikto v2.5.0

+ Target IP:          192.168.18.209
+ Target Hostname:   192.168.18.209
+ Target Port:        80
+ Start Time:        2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+: The Anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+: The Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use -C all to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/jun/536
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/jun/536
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: 9 errors(s) and 8 warning(s) reported on remote host
+ End Time:           2025-06-07 03:24:14 (GMT+4) (18s seconds)

+ 1 host(s) tested
```

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# nikto -h http://192.168.18.209
- Nikto v2.5.0

+ Target IP:          192.168.18.209
+ Target Hostname:   192.168.18.209
+ Target Port:        80
+ Start Time:        2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+: The Anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+: The Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use -C all to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/jun/536
+ /phpMyAdmin/db_details/importdcsl.php?submit_show=true&do=import&dcopath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/jun/536
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: 9 errors(s) and 8 warning(s) reported on remote host
+ End Time:           2025-06-07 03:24:14 (GMT+4) (18s seconds)

+ 1 host(s) tested
```

### 3. Web scanning yang kedua dilakukan dengan tools Dirb.

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any information on the login page using the default credentials. Let's break down the sqlmap output and discuss the potential

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any information on the login page using the default credentials. Let's break down the sqlmap output and discuss the potential

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any information on the login page using the default credentials. Let's break down the sqlmap output and discuss the potential

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://192.168.18.209 / ---
+ http://192.168.18.209 /login (CODE:308|SIZE:0)
+ http://192.168.18.209 /phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any information to extract. Let's try to access the login page using the direct URL.

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://192.168.18.209 / ---
+ http://192.168.18.209 /login (CODE:308|SIZE:0)
+ http://192.168.18.209 /phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209 /phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any information to extract. Let's try to access the login page using the direct URL.

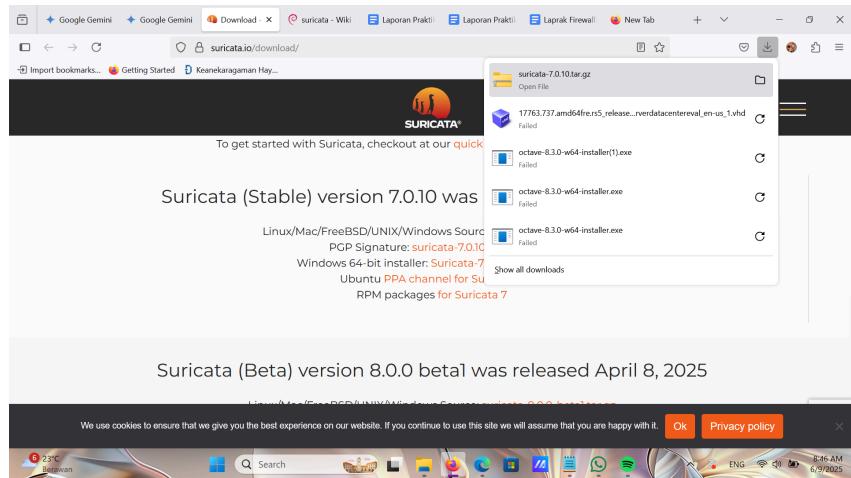
## B. Pertahanan

### a. Instalasi Suricata dan Membuat Tampilan GUI Suricata

- Suricata di install pada server Debian, diawali dengan melakukan update dan install dependensi yang diperlukan.

```
b ...
Unpacking libnetfilter-queue-dev:amd64 (1.0.5-3) ...
Selecting previously unselected package libnspr4-dev.
Preparing to unpack .../6-libnspr4-dev_2%3a4.35-1_amd64.deb ...
Unpacking libnspr4-dev (2:4.35-1) ...
Selecting previously unselected package libnss3-dev:amd64.
Preparing to unpack .../7-libnss3-dev_2%3a3.87.1-1+deb12u1_amd64.
deb ...
Unpacking libnss3-dev:amd64 (2:3.87.1-1+deb12u1) ...
Setting up libnspr4-dev (2:4.35-1) ...
Setting up libnfnetlink-dev:amd64 (1.0.2-2) ...
Setting up libmagic-dev:amd64 (1:5.44-3) ...
Setting up liblz4-dev:amd64 (1.9.4-1) ...
Setting up libnetfilter-queue1:amd64 (1.0.5-3) ...
Setting up libnetfilter-queue-dev:amd64 (1.0.5-3) ...
Setting up libnss3-dev:amd64 (2:3.87.1-1+deb12u1) ...
Setting up libcap-ng-dev:amd64 (0.8.3-1+b3) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u10) ...
root@Debian:/home/farhan30#
```

- Mengunduh file dari web resmi Suricata, file kemudian di ekstraksi dan memulai proses instalasi Suricata.



- Membuat direktori log untuk menyimpan log aktivitas yang akan ditangkap dan disimpan oleh Suricata.

```
root@Debian:/var/log# cd suricata
root@Debian:/var/log/suricata# ls
certs  eve.json  fast.log  files  stats.log  suricata.log
root@Debian:/var/log/suricata# nano eve.json
root@Debian:/var/log/suricata# nano fast.log
root@Debian:/var/log/suricata#
```

- Mengedit beberapa konfigurasi di dalam file konfigurasi suricata.yaml seperti OME\_NET dan EXTERNAL\_NET, lokasi rule, runmode, interface, dan output log.

```
GNU nano 7.2          suricata.yaml
%YAML 1.1
---
# Suricata configuration file. In addition to the comments describing
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml

# This configuration file generated by Suricata 7.0.10.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
    # more specific is better for alert accuracy and performance
address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
Search:
```

- Memulai layanan suricata dan memastikan nya sudah di enable dan status aktif.

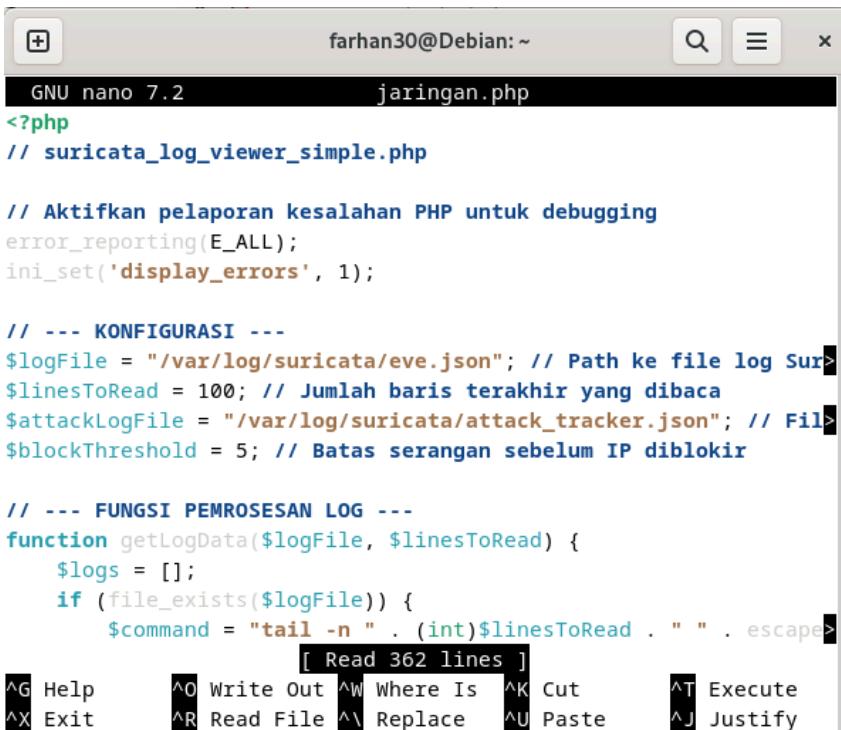
```

depcomp      Makefile.in
doc          missing
root@Debian:/home/farhan30/Downloads/suricata-7.0.10# nano suricata.yaml
root@Debian:/home/farhan30/Downloads/suricata-7.0.10# sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS daemon
   Loaded: loaded (/etc/systemd/system/suricata.service; enabled)
   Active: active (running) since Sun 2025-06-08 20:49:12 EDT; 1min 29.401s
     Main PID: 644 (Suricata-Main)
        Tasks: 8 (limit: 4631)
       Memory: 907.0M
          CPU: 1min 29.401s
        CGroup: /system.slice/suricata.service
                  └─644 /usr/bin/suricata -c /etc/suricata/suricata.yaml

Jun 08 20:49:12 Debian systemd[1]: Started suricata.service - Su>
Jun 08 20:49:12 Debian suricata[644]: Info: conf-yaml-loader: Co>
Jun 08 20:49:12 Debian suricata[644]: i: suricata: This is Suricat>
Jun 08 20:50:29 Debian suricata[644]: W: af-packet: enp0s3: AF_P>
Jun 08 20:50:30 Debian suricata[644]: i: threads: Threads create>
lines 1-15/15 (END)

```

- Membuat tampilan GUI untuk Suricata pada file jaringan.php, menampilkan Timestamp, jenis event, Source IP Port, Dest IP, Protocol, dan Details lalu kemudian ditampilkan pada browser dengan **192.168.18.209/jaringan.php**.



```

farhan30@Debian: ~
GNU nano 7.2          jaringan.php
<?php
// suricata_log_viewer_simple.php

// Aktifkan pelaporan kesalahan PHP untuk debugging
error_reporting(E_ALL);
ini_set('display_errors', 1);

// --- KONFIGURASI ---
$logFile = "/var/log/suricata/eve.json"; // Path ke file log Suricata
$linesToRead = 100; // Jumlah baris terakhir yang dibaca
$attackLogFile = "/var/log/suricata/attack_tracker.json"; // File log serangan
$blockThreshold = 5; // Batas serangan sebelum IP diblokir

// --- FUNGSI PEMROSESAN LOG ---
function getLogData($logFile, $linesToRead) {
    $logs = [];
    if (file_exists($logFile)) {
        $command = "tail -n " . (int)$linesToRead . " " . escapeapeshift($logFile);
        $logs = shell_exec($command);
    }
    return $logs;
}

function escapeapeshift($string) {
    $string = str_replace("\\", "\\\\", $string);
    $string = str_replace("'", "\\'", $string);
    return $string;
}

// --- TAMPILAN LOG ---
echo "

|               |
|---------------|
| " . \$log . " |
|---------------|

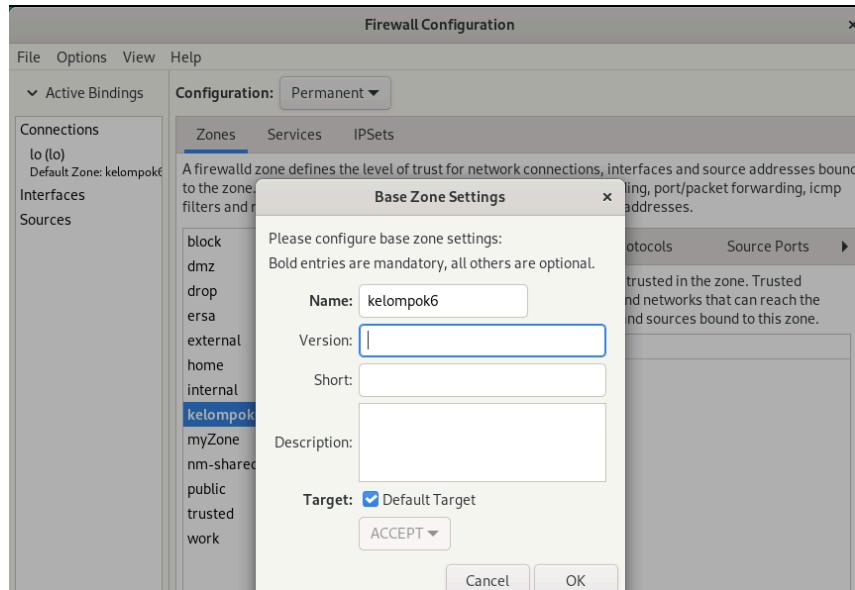
";


```

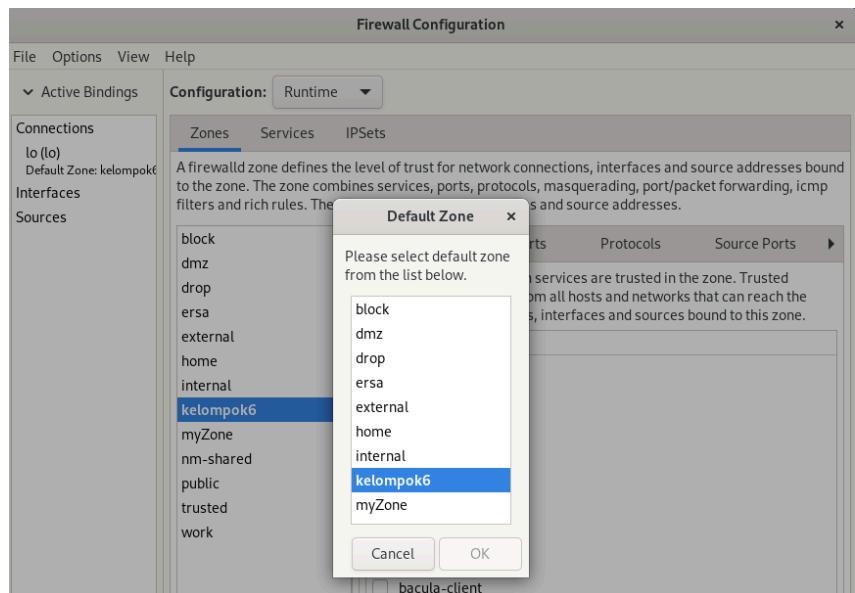
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

### b. Instalasi FirewallD

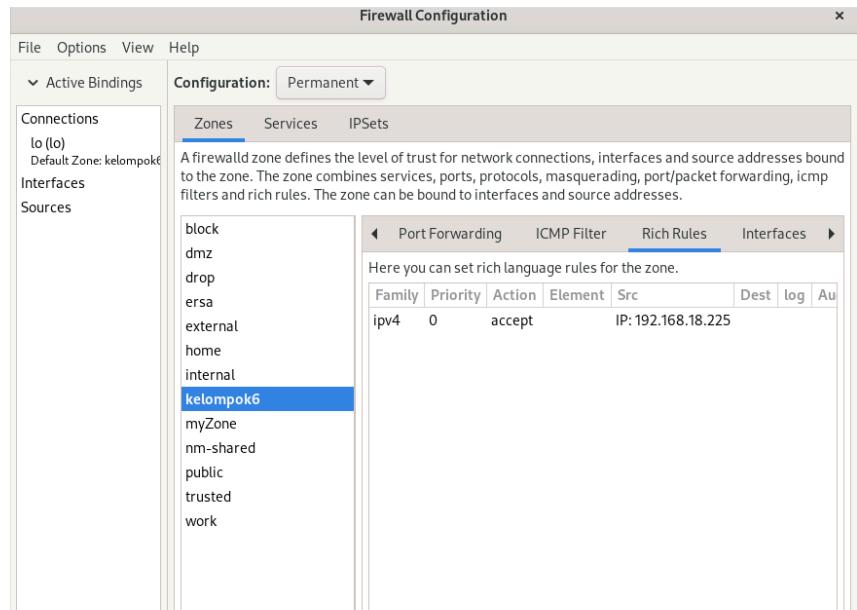
- Menginstall GUI FirewallD pada server Debian dengan perintah **sudo apt install firewall-config**.
- Menjalankan GUI FirewallD dengan perintah **sudo firewall-config**.
- Mengatur Configuration menjadi **Permanent** dan membuat zone baru yaitu **kelompok6** dengan klik icon Plus (+). Firewalld direload kembali pada menu **Options**, lalu pilih **Reload Firewalld**.



- Mengubah Default Zone pada menu **Options** dan pilih **Change Default Zone**. Gunakan zone **kelompok6** yang baru dibuat, lalu reload kembali firewalld-nya.



- Menambahkan Rich Rule pada FirewallD untuk memblokir IP penyerang, dengan memilih action **accept** dan memasukkan IP penyerang ke bagian **src**. FirewallD di reload kembali untuk menyimpan perubahan.



### c. Port Scanning

1. Penyerang melakukan scanning pada Kali Linux terhadap port dan IP dari server Debian,
2. Scanning yang pertama dilakukan menggunakan tools Nmap

```
(root@ersahayuning13)-[~/home/ersahayuning13]
└# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

[root@ersahayuning13]-[~/home/ersahayuning13]
└#
```

```
(root@ersahayuning13)-[~/home/ersahayuning13]
└# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

[root@ersahayuning13]-[~/home/ersahayuning13]
└#
```

```
(root@ersahayuning13)-[~/home/ersahayuning13]
└# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

[root@ersahayuning13]-[~/home/ersahayuning13]
└#
```

```
(root@ersahayuning13)-[~/home/ersahayuning13]
└# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

[root@ersahayuning13]-[~/home/ersahayuning13]
└#
```

```

└─[root@ersahayuning13]~[/home/ersahayuning13]
# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

```

```

└─[root@ersahayuning13]~[/home/ersahayuning13]
# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 50:5A:65:96:DD:D9 (AzureWave Technologies)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds

```

3. Tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 saat melakukan scanning Nmap

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Suricata Log Viewer

Menampilkan 100 baris log terakhir dari /var/log/suricata/www.json.  
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

#### 4. Scanning yang kedua dilakukan menggunakan tools masscan

```
(root@ersahayuning13)-[/home/ersahayuning13]
# masscan -p80 192.168.18.213
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-08 08:59:09 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]

(root@ersahayuning13)-[/home/ersahayuning13]
# masscan -p80 192.168.18.213
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-08 08:59:09 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]

(root@ersahayuning13)-[/home/ersahayuning13]
# masscan -p80 192.168.18.213
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-08 08:59:09 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]

(root@ersahayuning13)-[/home/ersahayuning13]
# masscan -p80 192.168.18.213
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-08 08:59:09 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
```

#### 5. Tampilan log pada gui Suricata juga sama, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan scanning Masscan.

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4406-0400	tls	192.168.18.225:4079 4	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tls	192.168.18.225:4077 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tls	192.168.18.225:4077 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

## d. Brute Force

1. Brute force dilakukan untuk mencari username dan password user dilakukan dengan menggunakan dua tools yang berbeda, yaitu Hydra dan Medusa. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallD.
2. Membuat word list username bernama **username.txt** yang berisi list username yang akan dicoba.

The terminal window shows the file 'username.txt' containing a list of usernames:

```
root@kali:/home/satriasheva
username.txt *
al meng
admin
dafa
asep
abi
favian
rakha
leyan
arung
uhuy
ke neo
farhab
kursi
yuli
ali
aldi
rak han
```

3. Membuat word list password bernama **password.txt** yang berisi list password yang akan dicoba.

The terminal window shows the file 'password.txt' containing a list of passwords:

```
root@kali:/home/satriasheva
password.txt *
admin123
12345
123
kerat0
senggel122
poltek123
haha123
rakha123
pmn127
127187hs
korsa1291
kipas5757
rumah12
lantai12
keramik31
uiiiii12
yfwqn21
yugubu12
126bjjhj
```

4. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server caddy untuk setiap username admin, dafa, abi, asep, dan ameng dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"** dimana hasilnya berhasil melewati autentikasi.

The terminal windows show the execution of Hydra against three different user accounts:

- Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).**  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:53:47  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:/p1), -1 try per task  
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username="USER"&password="PASS":Login  
[80][http-post-form] host: 192.168.18.209 login: admin password: admin123  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:53:48
- Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).**  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:54:43  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:/p1), -1 try per task  
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username="USER"&password="PASS":Login  
[80][http-post-form] host: 192.168.18.209 login: dafa password: senggel122  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:54:44
- Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).**  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:56:02  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:/p1), -1 try per task  
[DATA] attacking http-post-form://192.168.18.209:80/login/login.php:username="USER"&password="PASS":Login  
[80][http-post-form] host: 192.168.18.209 login: abi password: kerat0  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:56:03

```
[root@kali:~/home/satriasheva]
# hydra -l username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php?username=%USER%&password=%PASS%:Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:57:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:/Login/login.php?username=%USER%&password=%PASS%:Login
[80][http-post-form] host: 192.168.18.209 login: asep password: asep123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:57:25
```

```
[root@kali:~/home/satriasheva]
# hydra -l username.txt -P password.txt 192.168.18.209 http-post-form "/Login/login.php?username=%USER%&password=%PASS%:Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 05:58:14
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), -1 try per task
[DATA] attacking http-post-form://192.168.18.209:/Login/login.php?username=%USER%&password=%PASS%:Login
[80][http-post-form] host: 192.168.18.209 login: ameng password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 05:58:14
```

5. Selanjutnya, melihat tampilan log pada gui Suricata juga sama, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan brute force dengan hydra pada masing masing username

192.168.18.213/jaringan.php						
Date	Type	Source IP	Dest IP	Protocol	Port	Details
2025-06-08T05:16:59.43	fileinfo	192.168.18.213.80	192.168.18.225.4659	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42	tts	192.168.18.225.4661	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39	http	192.168.18.225.4660	192.168.18.213.80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39	alert	192.168.18.225.4660	192.168.18.213.80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38	tts	192.168.18.225.4659	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36	tts	192.168.18.225.4658	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

192.168.18.213/jaringan.php						
Date	Type	Source IP	Dest IP	Protocol	Port	Details
2025-06-08T05:16:59.43	fileinfo	192.168.18.213.80	192.168.18.225.4659	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42	tts	192.168.18.225.4661	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39	http	192.168.18.225.4660	192.168.18.213.80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39	alert	192.168.18.225.4660	192.168.18.213.80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38	tts	192.168.18.225.4659	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36	tts	192.168.18.225.4658	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

192.168.18.213/jaringan.php						
Date	Type	Source IP	Dest IP	Protocol	Port	Details
2025-06-08T05:16:59.43	fileinfo	192.168.18.213.80	192.168.18.225.4659	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42	tts	192.168.18.225.4661	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39	http	192.168.18.225.4660	192.168.18.213.80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39	alert	192.168.18.225.4660	192.168.18.213.80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38	tts	192.168.18.225.4659	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36	tts	192.168.18.225.4658	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

192.168.18.213/jaringan.php						
Date	Type	Source IP	Dest IP	Protocol	Port	Details
2025-06-08T05:16:59.43	fileinfo	192.168.18.213.80	192.168.18.225.4659	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42	tts	192.168.18.225.4661	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39	http	192.168.18.225.4660	192.168.18.213.80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39	alert	192.168.18.225.4660	192.168.18.213.80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38	tts	192.168.18.225.4659	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36	tts	192.168.18.225.4658	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

6. Menjalankan tool Medusa untuk melakukan brute-force terhadap formulir login HTTP di web server caddy untuk setiap username admin, dafa, abi, asep, dan ameng dengan perintah **medusa -h 192.168.18.209 -u admin -P password.txt -M http** dimana hasilnya berhasil melewati autentikasi.

```

[root@kali]~[/home/satriasheva]
# 2025-06-04 05:40:43 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: admin (1 of 1, 2025-06-04 05:40:43 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: admin Password: admin123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http

[root@kali]~[/home/satriasheva]
# 2025-06-04 05:39:02 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: dafa (1 of 1, 2025-06-04 05:39:02 ACCOUNT FOUND: [http] Host: 192.168.10.209 User: dafa Password: senggel122 [SUCCESS].
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http

[root@kali]~[/home/satriasheva]
# 2025-06-04 05:42:43 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: abi (1 of 1, 2025-06-04 05:42:43 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: abi Password: kera10 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http

[root@kali]~[/home/satriasheva]
# 2025-06-04 05:45:37 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: asep (1 of 1, 2025-06-04 05:45:37 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: asep Password: asep123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http

[root@kali]~[/home/satriasheva]
# 2025-06-04 05:44:55 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: ameng (1 of 1, 2025-06-04 05:44:55 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: ameng Password: 123 [SUCCESS]
[1] + done medusa -h 192.168.18.209 -u admin -P password.txt -M http

```

7. Selanjutnya, melihat tampilan log pada gui Suricata juga sama, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan brute force dengan medusa pada masing masing username.

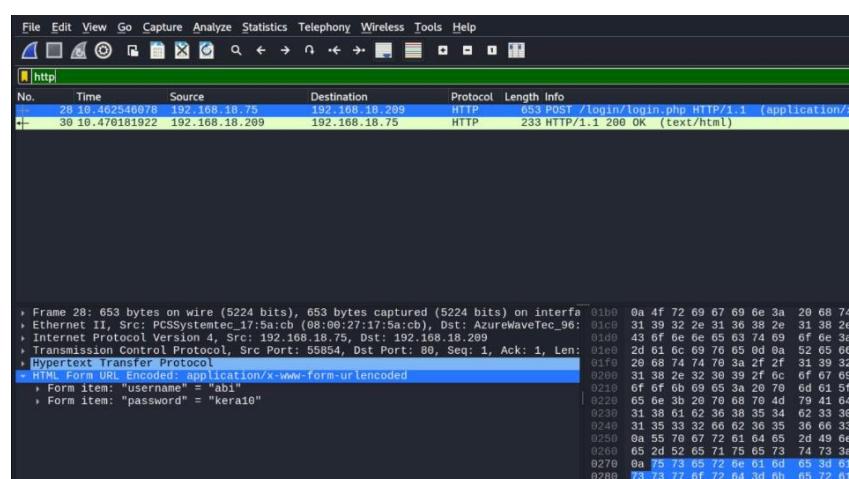
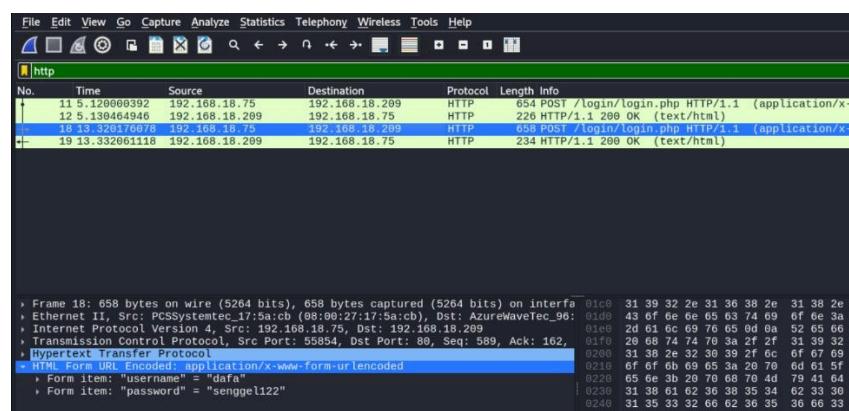
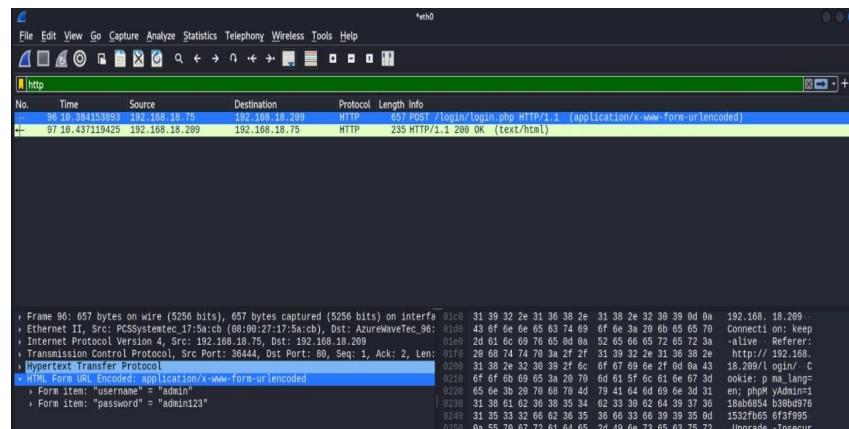
7945-0400	8						
2025-06-08T05:16:59:36	ts	192.168.18.225.4658 6	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A	
8974-0400							
2025-06-08T05:16:59:33	http	192.168.18.225.4659 2	192.168.18.213.80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	
8354-0400							
2025-06-08T05:16:59:33	alert	192.168.18.225.4659 7575-0400	192.168.18.213.80	TCP	http	Sigature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1	
9978-0400							
2025-06-08T05:16:59:32	fileinfo	192.168.18.213.80	192.168.18.225.4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A	
9944-0400							

7945-0400	8						
2025-06-08T05:16:59:36	ts	192.168.18.225.4658 6	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A	
8974-0400							
2025-06-08T05:16:59:33	http	192.168.18.225.4659 2	192.168.18.213.80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	
8354-0400							
2025-06-08T05:16:59:33	alert	192.168.18.225.4659 7575-0400	192.168.18.213.80	TCP	http	Sigature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1	
9978-0400							
2025-06-08T05:16:59:32	fileinfo	192.168.18.213.80	192.168.18.225.4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A	
9944-0400							
7945-0400	8						
2025-06-08T05:16:59:36	ts	192.168.18.225.4658 6	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A	
8974-0400							
2025-06-08T05:16:59:33	http	192.168.18.225.4659 2	192.168.18.213.80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	
8354-0400							
2025-06-08T05:16:59:33	alert	192.168.18.225.4659 7575-0400	192.168.18.213.80	TCP	http	Sigature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1	
9978-0400							
2025-06-08T05:16:59:32	fileinfo	192.168.18.213.80	192.168.18.225.4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A	
9944-0400							
7945-0400	8						
2025-06-08T05:16:59:36	ts	192.168.18.225.4658 6	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A	
8974-0400							
2025-06-08T05:16:59:33	http	192.168.18.225.4659 2	192.168.18.213.80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	
8354-0400							
2025-06-08T05:16:59:33	alert	192.168.18.225.4659 7575-0400	192.168.18.213.80	TCP	http	Sigature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1	
9978-0400							
2025-06-08T05:16:59:32	fileinfo	192.168.18.213.80	192.168.18.225.4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A	
9944-0400							

## e. Sniffing

- Sniffing dilakukan melalui dua tools yang berbeda, yaitu melalui wireshark dan tcpdump. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallD.

2. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** untuk setiap username: admin, dafa, abi, asep, dan ameng.



Frame 73: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \*eth0

Frame 24: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \*eth0

Protocol: Hypertext Transfer Protocol (HTTP)

HTTP Form URL Encoded: application/x-www-form-urlencoded

Form item: "username" = "asep"

Form item: "password" = "12345"

3. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan bahwa IP penyerang 192.168.18.225 tercatat tetapi tidak tercatat sebagai alert sehingga tidak berwarna orange pada saat dilakukan sniffing dengan Wireshark.

Suricata Log Viewer

Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.

Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:12:54.61	flow	192.168.18.225:5174	192.168.18.213:443	TCP	tls	State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (126B)
1913-0400		4				
2025-06-08T05:12:54.55	flow	192.168.18.225:5169	192.168.18.213:443	TCP	http	State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
3612-0400		4				
2025-06-08T05:12:53.66	tts	192.168.18.225:3706	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
1938-0400		8				
2025-06-08T05:12:53.63	tts	192.168.18.225:3706	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
6036-0400		6				
2025-06-08T05:12:53.59	tts	192.168.18.225:3705	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
7643-0400		6				

Suricata Log Viewer

Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.

Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)

Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:12:54.61	flow	192.168.18.225:5174	192.168.18.213:443	TCP	tls	State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (126B)
1913-0400		4				
2025-06-08T05:12:54.55	flow	192.168.18.225:5169	192.168.18.213:443	TCP	http	State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
3612-0400		4				
2025-06-08T05:12:53.66	tts	192.168.18.225:3706	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
1938-0400		8				
2025-06-08T05:12:53.63	tts	192.168.18.225:3706	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
6036-0400		6				
2025-06-08T05:12:53.59	tts	192.168.18.225:3705	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
7643-0400		6				

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:12:54.61	flow	192.168.18.225.5174	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (1285B)
1913-0400		4				
2025-06-08T05:12:54.55	flow	192.168.18.225.5169	192.168.18.213.443	TCP	http	State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
3612-0400		4				
2025-06-08T05:12:53.66	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
1938-0400		8				
2025-06-08T05:12:53.63	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
6036-0400		6				
2025-06-08T05:12:53.59	tts	192.168.18.225.3705	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
7643-0400		6				

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:12:54.61	flow	192.168.18.225.5174	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (1285B)
1913-0400		4				
2025-06-08T05:12:54.55	flow	192.168.18.225.5169	192.168.18.213.443	TCP	http	State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
3612-0400		4				
2025-06-08T05:12:53.66	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
1938-0400		8				
2025-06-08T05:12:53.63	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
6036-0400		6				
2025-06-08T05:12:53.59	tts	192.168.18.225.3705	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
7643-0400		6				

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:12:54.61	flow	192.168.18.225.5174	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (1285B)
1913-0400		4				
2025-06-08T05:12:54.55	flow	192.168.18.225.5169	192.168.18.213.443	TCP	http	State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
3612-0400		4				
2025-06-08T05:12:53.66	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
1938-0400		8				
2025-06-08T05:12:53.63	tts	192.168.18.225.3706	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
6036-0400		6				
2025-06-08T05:12:53.59	tts	192.168.18.225.3705	192.168.18.213.443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
7643-0400		6				

4. Selanjutnya sniffing melalui tcpdump yang dilakukan pada saat user login ke web server dengan perintah **sudo tcpdump -r login\_form.pcap -X** untuk setiap username: admin, dafa, abi, asep, dan ameng.

```
(root@kali:~/home/satriasheva]# sudo tcpdump -r login_form.pcap -X
reading from file login_form.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:17:09.628950 IP 192.168.18.75.45706 -> 192.168.18.209.http: Flags [P..], seq 3015063865:3015064456, ack 3636703928, win 502, options [nop,nop,TS val 3680335072 ecr 4516724]
: HTTP: POST /login_form.php HTTP/1.1
0x0000: 4500 0283 c52c 0000 4006 acdb c0a8 124b E.....@.....
0x0010: c0a8 12d1 b18a 0050 b2bc 3929 d8c2 b2b8 .....@.....
0x0020: 8018 01f6 a8e2 0000 0101 080a laeb f976 .....@.....
0x0030: db5d 74b8 504f 5354 202f 6ccf 6769 6e2f J...POST.../login.php,HTTP/1
0x0040: 6c6f 6769 6e2e 7068 7028 4854 5456 2f31 1...Host: 192.168.18.209
0x0050: 2e31 0d0a 486f 7374 3a20 3139 322e 3136 1...Content-Type: application/x-www-form-urlencoded
0x0240: 3736 3135 3332 6662 3635 3666 3366 3920 761532fb56f3ff99
0x0250: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5...Upgrade-Insec
0x0260: 7572 652d 5265 7175 6573 7473 3a20 310d ure-Requests:1.
0x0270: 0a0d 0a75 7365 7266 616d 653d 6164 6d69 ...username=admin
0x0278: 6e26 7061 7373 776f 7264 3d61 646d 698e npassword=admin
0x0280: 3132 33 123
06:17:09.670085 IP 192.168.18.209.http -> 192.168.18.75.45706: Flags [P..], seq 1:170, ack 591, win 505, options [nop,nop,TS val 3680335072 ecr 4516724]
0x0000: 4500 00d5 94c5 4000 4006 fee8 c0a8 12d1 E.....@.....
0x0010: c0a8 12d4 0050 b2b8 d28a b3b6 3d08a ...K.P.N.....
0x0020: 8018 01f9 21d1 0000 0101 080a db5d 74e0 .....jt.
0x0030: lae9 f976 4854 5456 2f31 2e31 2832 3030 ...vHTTP/1.1:200
0x0040: 2047 5d0d 6a51 6765 4f6d 7465 4f74 2044 7970 ..OK..Content-Type: application/x-www-form-urlencoded
0x0240: 3736 3135 3332 6662 3635 3666 3366 3920 761532fb56f3ff99
0x0250: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5...Upgrade-Insec
0x0260: 7572 652d 5265 7175 6573 7473 3a20 310d ure-Requests:1.
0x0270: 0a0d 0a75 7365 7266 616d 653d 6164 6d69 ...username=dfa
0x0278: 6e26 7061 7373 776f 7264 3d61 646d 698e npassword=sengge
0x0280: 6c31 3232 l122
06:19:04.256557 IP 192.168.18.209.http -> 192.168.18.75.45706: Flags [P..], seq 1:169, ack 592, win 505, options [nop,nop,TS val 3680449853 ecr 4516724]
0x0000: 4500 00d5 94c5 4000 4006 fee8 c0a8 12d1 E.....@.....
0x0010: c0a8 12d4 0050 b2b8 d28a b3b6 3d08a ...K.P.N.....
0x0020: 8018 01f9 21d1 0000 0101 080a db5d 74e0 .....jt.
0x0030: lae9 f976 4854 5456 2f31 2e31 2832 3030 ...vHTTP/1.1:200
0x0040: 2047 5d0d 6a51 6765 4f6d 7465 4f74 2044 7970 ..OK..Content-Type: application/x-www-form-urlencoded
0x0240: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5...Upgrade-Insec
0x0250: 7572 652d 5265 7175 6573 7473 3a20 310d ure-Requests:1.
0x0260: 0a0d 0a75 7365 7266 616d 653d 6164 6d69 ...username=abi
0x0270: 7061 7373 776f 7264 3d6b 6572 6131 30 password=kera10
06:19:41.961466 IP 192.168.18.209.http -> 192.168.18.75.45706: Flags [P..], seq 1:168, ack 587, win 501, options [nop,nop,TS val 3680487553 ecr 4518246]
0x0000: 4500 00db 3b38 4000 4006 e024 c0a8 12d1 E.....@.....
0x0010: c0a8 12d4 0050 8d4e b012 b908 ad90 9a95 ...K.P.N.....
0x0020: 8018 01f5 def1 0000 0101 080a db5f c881 .....-..
0x0030: lae9 abd8 4854 5456 2f31 2e31 2832 3030 ..K.HTTP/1.1:200
0x0040: 2047 5d0d 6a51 6765 4f6d 7465 4f74 2044 7970 ..OK..Content-Type: application/x-www-form-urlencoded
0x0240: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5...Upgrade-Insec
0x0250: 7572 652d 5265 7175 6573 7473 3a20 310d ure-Requests:1.
0x0260: 0a0d 0a75 7365 7266 616d 653d 6164 6d69 ...username=ameng
0x0270: 7061 7373 776f 7264 3d6b 6572 6131 30 password=kera10
06:19:41.961466 IP 192.168.18.209.http -> 192.168.18.75.45706: Flags [P..], seq 1:168, ack 587, win 501, options [nop,nop,TS val 3680487553 ecr 4518246]
```

```

0x0230: 3736 3135 3332 6662 3635 3666 3366 3939 761532fb656f3f99
0x0240: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5 ..Upgrade-Insec
0x0250: 7572 652d 5265 7175 7473 3a20 310d ure-Requests::1.
0x0260: 0a0d 0a75 7365 7261 616d 653d 6173 6570 ...username=asep
0x0270: 2670 6173 7377 6f72 643d 6173 6570 3132 &password=asep12
0x0280: 33 3

06:20:34.896482 IP 192.168.18.209.http > 192.168.18.75.36174: Flags [P.], seq 321:489, ack 1767, win 501, options [nop,nop,TS val 36805402
OK
0x0000: 4500 00dd b394 4000 4006 e01a c0a8 12d1 E.....@.0.....
0x0010: c0a8 124b 0050 8d4e b012 baef ad90 a17c ...K.P.N.....
0x0020: 8018 01f5 d3f2 0000 0101 080a db60 9632 ...K.P.N.....
0x0030: laef 1b42 4854 5450 2f31 2e31 2032 3030 ...BHTTP/1.1.200

0x0230: 3736 3135 3332 6662 3635 3666 3366 3939 761532fb656f3f99
0x0240: 350d 0a55 7067 7261 6465 2d49 6e73 6563 5 ..Upgrade-Insec
0x0250: 7572 652d 5265 7175 7473 3a20 310d ure-Requests::1.
0x0260: 0a0d 0a75 7365 7261 616d 653d 6173 6570 ...username=asep
0x0270: 2670 6173 7377 6f72 643d 6173 6570 3132 &password=asep12
0x0280: 33 3

06:21:41.791544 IP 192.168.18.209.http > 192.168.18.75.36174: Flags [P.], seq 161:330, ack 1174, win 501, options [nop,nop,TS val 3680607197 ecr 4519
OK
0x0000: 4500 00dd b394 4000 4006 e00e c0a8 12d1 E.....@.0.....
0x0010: c0a8 124b 0050 8d4e b012 bc37 ad90 a612 ...K.P.N.....
0x0020: 8018 01f5 abd2 0000 0101 080a db61 9b0d ...K.P.N.....
0x0030: 1-e0-300-4554-5450-3e31-3e31-3e31-3e30 ...HTTP/1.1.200

```

5. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan bahwa IP penyerang 192.168.18.225 tercatat tetapi tidak tercatat sebagai alert sehingga tidak berwarna orange pada saat dilakukan sniffing dengan tcpdump.

Activities Firefox ESR Jun 8 05:16						
		Suricata Log Viewer (Simple)		Suricata Log Viewer (Simple)		
<a href="#">Restore Session</a> <a href="#">192.168.18.213/jaringan.php</a> 80%						
2025-06-08T05:16:19.92	flow	192.168.18.225.3511 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1485B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3518 0	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1482B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3519 6	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1476B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.89	flow	192.168.18.225.5909 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 9 (817B), Pkts(C->S): 11 (10988B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3606 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (561B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3595 2	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (580B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.87	stats	N/A/N/A	N/A/N/A	N/A		Uptime: 1234s, Total Flows: 17212, Alerts Detected: 186
2025-06-08T05:16:18.95	flow	192.168.18.225.3499 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1413B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:18.95	flow	192.168.18.225.5554	192.168.18.213.1	TCP		State: closed, Pkts(S->C): 1 (74B), Pkts(C->S): 1 (54B)

Activities Firefox ESR Jun 8 05:16						
		Suricata Log Viewer (Simple)		Suricata Log Viewer (Simple)		
<a href="#">Restore Session</a> <a href="#">192.168.18.213/jaringan.php</a> 80%						
2025-06-08T05:16:19.92	flow	192.168.18.225.3511 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1485B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3518 0	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1482B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3519 6	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1476B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.89	flow	192.168.18.225.5909 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 9 (817B), Pkts(C->S): 11 (10988B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3606 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (561B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3595 2	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (580B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.87	stats	N/A/N/A	N/A/N/A	N/A		Uptime: 1234s, Total Flows: 17212, Alerts Detected: 186
2025-06-08T05:16:18.95	flow	192.168.18.225.3499 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1413B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:18.95	flow	192.168.18.225.5554	192.168.18.213.1	TCP		State: closed, Pkts(S->C): 1 (74B), Pkts(C->S): 1 (54B)

Activities Firefox ESR Jun 8 05:16						
		Suricata Log Viewer (Simple)		Suricata Log Viewer (Simple)		
<a href="#">Restore Session</a> <a href="#">192.168.18.213/jaringan.php</a> 80%						
2025-06-08T05:16:19.92	flow	192.168.18.225.3511 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1485B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3518 0	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1482B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3519 6	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1476B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.89	flow	192.168.18.225.5909 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 9 (817B), Pkts(C->S): 11 (10988B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3606 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (561B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3595 2	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (580B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.87	stats	N/A/N/A	N/A/N/A	N/A		Uptime: 1234s, Total Flows: 17212, Alerts Detected: 186
2025-06-08T05:16:18.95	flow	192.168.18.225.3499 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1413B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:18.95	flow	192.168.18.225.5554	192.168.18.213.1	TCP		State: closed, Pkts(S->C): 1 (74B), Pkts(C->S): 1 (54B)

Activities Firefox ESR Jun 8 05:16						
		Suricata Log Viewer (Simple)		Suricata Log Viewer (Simple)		
<a href="#">Restore Session</a> <a href="#">192.168.18.213/jaringan.php</a> 80%						
2025-06-08T05:16:19.92	flow	192.168.18.225.3511 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1485B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3518 0	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1482B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.92	flow	192.168.18.225.3519 6	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 10 (1476B), Pkts(C->S): 10 (2952B)
2025-06-08T05:16:19.89	flow	192.168.18.225.5909 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 9 (817B), Pkts(C->S): 11 (10988B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3606 4	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (561B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.89	flow	192.168.18.225.3595 2	192.168.18.213.80	TCP	http	State: closed, Pkts(S->C): 6 (580B), Pkts(C->S): 5 (794B)
2025-06-08T05:16:19.87	stats	N/A/N/A	N/A/N/A	N/A		Uptime: 1234s, Total Flows: 17212, Alerts Detected: 186
2025-06-08T05:16:18.95	flow	192.168.18.225.3499 4	192.168.18.213.443	TCP	tts	State: closed, Pkts(S->C): 9 (1413B), Pkts(C->S): 10 (2991B)
2025-06-08T05:16:18.95	flow	192.168.18.225.5554	192.168.18.213.1	TCP		State: closed, Pkts(S->C): 1 (74B), Pkts(C->S): 1 (54B)

Suricata Log Viewer (Simple)						
		Jun 8 05:16				
		192.168.18.213[jaringan.php]				
2025-06-08T05:16:19.92	flow	192.168.18.225.3511	192.168.18.213:443	TCP	tts	State: closed, Pkts(S->C): 10 (1485B), Pkts(C->S): 10 (2991B)
7887-0400		4				
2025-06-08T05:16:19.92	flow	192.168.18.225.3518	192.168.18.213:443	TCP	tts	State: closed, Pkts(S->C): 9 (1402B), Pkts(C->S): 10 (2952B)
7815-0400		0				
2025-06-08T05:16:19.92	flow	192.168.18.225.3519	192.168.18.213:443	TCP	tts	State: closed, Pkts(S->C): 10 (1476B), Pkts(C->S): 10 (2952B)
7513-0400		6				
2025-06-08T05:16:19.89	flow	192.168.18.225.5900	192.168.18.213:80	TCP	http	State: closed, Pkts(S->C): 9 (817B), Pkts(C->S): 11 (10988B)
0982-0400		4				
2025-06-08T05:16:19.89	flow	192.168.18.225.3600	192.168.18.213:80	TCP	http	State: closed, Pkts(S->C): 6 (561B), Pkts(C->S): 5 (794B)
0947-0400		4				
2025-06-08T05:16:19.89	flow	192.168.18.225.3595	192.168.18.213:80	TCP	http	State: closed, Pkts(S->C): 6 (580B), Pkts(C->S): 5 (794B)
0838-0400		2				
2025-06-08T05:16:19.87	stats	N/A/N/A	N/A/N/A	N/A		Uptime: 1234s, Total Flows: 17212, Alerts Detected: 186
6412-0400						
2025-06-08T05:16:18.95	flow	192.168.18.225.3499	192.168.18.213:443	TCP	tts	State: closed, Pkts(S->C): 9 (1413B), Pkts(C->S): 10 (2991B)
3757-0400		4				
2025-06-08T05:16:18.95	flow	192.168.18.225.5554	192.168.18.213:1	TCP		State: closed, Pkts(S->C): 1 (748), Pkts(C->S): 1 (548)

## f. DDOS

- Melihat ping ke ip server terlebih dahulu sebelum dilakukan DDOS.

```
(root@ersahayuning13) [~]
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

```
(root@ersahayuning13) [~]
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

```
(root@ersahayuning13) [~]
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

```
(root@ersahayuning13) [~]
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

```
[root@ersahayuning13] ~
# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

```
[root@ersahayuning13:~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=12.5 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=6.01 ms
64 bytes from 192.168.18.209: icmp_seq=4 ttl=64 time=5.76 ms
64 bytes from 192.168.18.209: icmp_seq=5 ttl=64 time=6.18 ms
^C
--- 192.168.18.209 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4223ms
rtt min/avg/max/mdev = 5.757/11.883/28.933/8.896 ms
```

2. Cek kondisi CPU dengan perintah top untuk memantau.

System Resource Usage Report												
Memory		CPU		Swap		Disk I/O		Network		System		Total
MiB	Mem	MiB	Swap	MiB	Free	MiB	Used	MiB	Free	MiB	Used	MiB
MiB	Mem : 3915.3 total, 1503.1 free, 1578.4 used, 1079.2 buff/cache											
MiB	Swap: 975.0 total, 785.5 free, 189.5 used, 2336.9 avail Mem											
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND	
1659	farhan30	20	0	3863376	282444	108576	S	12.5	7.0	32:04.43	gnome-shell	
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.95	systemd	
2	root	20	0		0	0	S	0.0	0.0	0:00.03	kthreadd	
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp	
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp	
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq	
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns	
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq	
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread	
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread	
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread	
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksftoirqd/0	
15	root	20	0	0	0	0	I	0.0	0.0	0:31.75	rcu_preempt	

farhan30@Debian: ~										
MiB Mem :		3915.3	total,	1503.1	free,	1578.4	used,	1079.2	buff/cache	
MiB Swap:		975.0	total,	785.5	free,	189.5	used,	2336.9	avail Mem	
<hr/>										
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
1659	farhan30	20	0	3863376	282444	108576	S	12.5	7.0	32:04.43 gnome-shell
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.95 systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03 kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32 ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:31.75 rcu_preempt

farhan30@Debian: ~

MiB Mem : 3915.3 total, 1503.1 free, 1578.4 used, 1079.2 buff/cache										
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.9 avail Mem										
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
1659	farhan30	20	0	3863376	282444	108576	S	12.5	7.0	32:04.43 gnome-shell
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.95 systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03 kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32 ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:31.75 rcu_preempt
...	...	...	...	...	...	...	...	...	...	...

farhan30@Debian: ~

MiB Mem : 3915.3 total, 1503.1 free, 1578.4 used, 1079.2 buff/cache										
MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.9 avail Mem										
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
1659	farhan30	20	0	3863376	282444	108576	S	12.5	7.0	32:04.43 gnome-shell
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.95 systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03 kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32 ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:31.75 rcu_preempt
...	...	...	...	...	...	...	...	...	...	...

### 3. Melakukan DDOS dengan perintah hping3 -S -p 80 --flood 192.168.18.209

```
(root@ersahayuning13) [~]
# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13] -[~] (1 up) scanned in 22.67 seconds
#
```

```
(root@ersahayuning13) [~]
# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13] -[~] (1 up) scanned in 22.67 seconds
#
```

```
(root@ersahayuning13) [~] (AzureWave Technologies)
# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.18.209 hping statistic --
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and service detection performed. Please report any incorrect results at https://nmap.org
[root@ersahayuning13] -[~] (1 up) scanned in 22.67 seconds
#
```

```
(root@ersahayuning13)-[~] ~ AzureWave Technologies
└─# sudo hping3 -S -p 80 --flood 192.168.18.209 specific OS details
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.18.209 hping statistic —
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and service detection performed. Please report any incorrect results at https://nmap.org/report.html
[root@ersahayuning13]-[~] it up) scanned in 22.67 seconds
└─#
```

```
(root@ersahayuning13)-[~] ~ AzureWave Technologies
└─# sudo hping3 -S -p 80 --flood 192.168.18.209 specific OS details
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.18.209 hping statistic —
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
OS and service detection performed. Please report any incorrect results at https://nmap.org/report.html
[root@ersahayuning13]-[~] it up) scanned in 22.67 seconds
└─#
```

4. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan DDOS dengan hping3 karena request yang berlebihan.

2025-06-08T05:16:59.38 7945-0400	tts	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tts	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7375-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9944-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 8	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.38 7945-0400	tts	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tts	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7375-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9944-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 8	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.38 7945-0400	tts	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tts	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7375-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9944-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 8	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.38 7945-0400	tts	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tts	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7375-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, Category: Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9944-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 8	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

5. Hasil ping ketika dilakukan DDOS, respon time nya tidak ada perubahan signifikan.

```

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

[~]# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 192.168.18.209: icmp_seq=10 Destination Host Unreachable
From 192.168.18.209: icmp_seq=11 Destination Host Unreachable
From 192.168.18.209: icmp_seq=12 Destination Host Unreachable
From 192.168.18.209: icmp_seq=13 Destination Host Unreachable
From 192.168.18.209: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.18.209: icmp_seq=18 ttl=64 time=242 ms
64 bytes from 192.168.18.209: icmp_seq=21 ttl=64 time=106 ms
64 bytes from 192.168.18.209: icmp_seq=22 ttl=64 time=83.8 ms
64 bytes from 192.168.18.209: icmp_seq=25 ttl=64 time=236 ms
64 bytes from 192.168.18.209: icmp_seq=26 ttl=64 time=183 ms
^C
192.168.18.209 ping statistics ---
46 packets transmitted, 21 received, +6 errors, 54.3478% packet loss, time 45500ms
rtt min/avg/max/mdev = 27.336/118.656/241.690/58.312 ms, pipe 3

```

6. Kondisi CPU pada saat dilakukan DDOS juga tidak meningkat signifikan, masih sama seperti pada saat belum dilakukan DDOS.

farhan30@Debian:~

MiB Mem : 3915.3 total, 1503.1 free, 1578.4 used, 1079.2 buff/cache  
 MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.9 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3863376	282444	108576	S	12.5	7.0	32:04.43	gnome-shell
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.95	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:31.75	rcu_preempt
...	...	...	...	...	...	...	...	...	...	...	...

farhan30@Debian:~

%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
 MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache  
 MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0
...	...	...	...	...	...	...	...	...	...	...	...

farhan30@Debian:~

%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
 MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache  
 MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0
...	...	...	...	...	...	...	...	...	...	...	...

farhan30@Debian:~

%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
 MiB Mem : 3915.3 total, 1502.4 free, 1579.1 used, 1079.2 buff/cache  
 MiB Swap: 975.0 total, 785.5 free, 189.5 used. 2336.2 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0
...	...	...	...	...	...	...	...	...	...	...	...

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1659	farhan30	20	0	3859216	282448	108576	S	18.8	7.0	32:04.97	gnome-shell
<b>19806</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>11608</b>	<b>5004</b>	<b>3104</b>	<b>R</b>	<b>6.2</b>	<b>0.1</b>	<b>0:00.02</b>	<b>top</b>
1	root	20	0	102952	12628	8840	S	0.0	0.3	0:06.96	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:03.32	ksoftirqd/0

## g. Web Scanning

- Penyerang melakukan web scanning pada Kali Linux terhadap aplikasi web dari server Debian, dengan menggunakan dua tools yang berbeda yaitu nikto dan dirb. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallID.
- Web Scanning yang pertama dilakukan menggunakan tools nikto

```
[root@kali] ~[home/satriasheva/sqlmap-dev]
└─# nikto -h http://192.168.18.209
[Nikto v2.5.6]

+ Target IP:      192.168.18.209
+ Target Hostname: 192.168.18.209
+ Target Port:    80
+ Start Time:    2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/: Right click interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ 0/0 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:      2025-06-07 03:24:14 (GMT+4) (184 seconds)

+ 1 host(s) tested
[root@kali] ~[home/satriasheva/sqlmap-dev]
```

```
[root@kali] ~[home/satriasheva/sqlmap-dev]
└─# nikto -h http://192.168.18.209
[Nikto v2.5.6]

+ Target IP:      192.168.18.209
+ Target Hostname: 192.168.18.209
+ Target Port:    80
+ Start Time:    2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/: Right click interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ 0/0 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:      2025-06-07 03:24:14 (GMT+4) (184 seconds)

+ 1 host(s) tested
[root@kali] ~[home/satriasheva/sqlmap-dev]
```

```
[root@kali] ~[home/satriasheva/sqlmap-dev]
└─# nikto -h http://192.168.18.209
[Nikto v2.5.6]

+ Target IP:      192.168.18.209
+ Target Hostname: 192.168.18.209
+ Target Port:    80
+ Start Time:    2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/: Right click interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ 0/0 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:      2025-06-07 03:24:14 (GMT+4) (184 seconds)

+ 1 host(s) tested
[root@kali] ~[home/satriasheva/sqlmap-dev]
```

```
[root@kali] ~[home/satriasheva/sqlmap-dev]
└─# nikto -h http://192.168.18.209
[Nikto v2.5.6]

+ Target IP:      192.168.18.209
+ Target Hostname: 192.168.18.209
+ Target Port:    80
+ Start Time:    2025-06-07 03:22:30 (GMT+4)

+ Server: Caddy
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /phpMyAdmin/: Uncommon header 'x-ob-mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/db_details_importtocsrl.php?submit_show=true&do=import&docpath.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/: Right click interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ 0/0 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:      2025-06-07 03:24:14 (GMT+4) (184 seconds)

+ 1 host(s) tested
[root@kali] ~[home/satriasheva/sqlmap-dev]
```

```
[root@bal1 ~]# /home/satriashew/sqlmap-dev
[*] nikto -h http://192.168.18.209
Nikto v2.5.0

[+] Target IP:          192.168.18.209
[+] Target Hostname:    192.168.18.209
[+] Threads:           400 (-)
[+] Timeout:            15 (-)
[+] Threads:           400 (-)
[+] Start Time:         2025-06-07 03:22:30 (GMT-4)

[+] Server:             Caddy
[+] This is the anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
[+] The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/vulnerabilities/x-content-type-options-xss-vulnerability
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] /phpmyadmin/db_details_importdbcscl.php?submit_show=true&db=importdbcscl...// Uncommon header 'x-0b_mode' found, with contents: 1
[+] /full/directoryclosure/2003/Jun/38/
[+] /phpmyadmin/db_details_importdbcscl.php?submit_show=true&db=importdbcscl...// phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/38/
[+] /phpmyadmin/db_details_importdbcscl.php?submit_show=true&db=importdbcscl...// phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/38/
[+] /Login/: This might be interesting.
[+] /phpMyAdmin/: phpMyAdmin directory found
[+] /phpMyAdmin/index.php: phpMyAdmin index page
[+] /phpMyAdmin/index.php?submit_show=true: phpMyAdmin index page
[+] 8102 requests | 0 errors(s) & 0 item(s) reported on remote host
[+] End Time:           2025-06-07 03:24:14 (GMT-4) (104 seconds)

[+] 1 host(s) tested
```

3. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan web scanning yang berlebihan dengan tools Nikto.

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.09 4406-0400	tts	192.168.18.225:4079 4	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:39.04 8322-0400	tts	192.168.18.225:4077 8	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:38.99 4430-0400	tts	192.168.18.225:4077 2	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.09 4406-0400	tts	192.168.18.225:4079 4	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:39.04 8322-0400	tts	192.168.18.225:4077 8	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:38.99 4430-0400	tts	192.168.18.225:4077 2	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		<p>Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic Protocol Command Decode Action: allowed, GID: 1, Rev: 2</p>
2025-06-08T05:14:39.09 4406-0400	tts	192.168.18.225:4079 4	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:39.04 8322-0400	tts	192.168.18.225:4077 8	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>
2025-06-08T05:14:38.99 4430-0400	tts	192.168.18.225:4077 2	192.168.18.213:443	TCP		<p>TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A</p>

Suricata Log Viewer						
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.						
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)						
Timestamp	Event Type	Source IP:Port	Dest IP:Port	Protocol	App Proto	Details
2025-06-08T05:14:39.74 1520-0400	alert	192.168.18.213:N/A	192.168.18.225:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic protocol unknown code Action allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.74 1297-0400	alert	192.168.18.225:N/A	192.168.18.213:N/A	ICMP		Signature: SURICATA ICMPv4 unknown code, Severity: 3, Category: Generic protocol Command Decode Action allowed, GID: 1, Rev: 2
2025-06-08T05:14:39.09 4405-0400	tts	4	192.168.18.225:4079	192.168.18.213:443	TCP	TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.04 8322-0400	tts	8	192.168.18.225:4079	192.168.18.213:443	TCP	TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.99 4430-0400	tts	2	192.168.18.225:4077	192.168.18.213:443	TCP	TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

#### 4. Web scanning yang kedua dilakukan dengan tools Dirb.

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential findings.

Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any interesting results on the http://192.168.18.209/ page using the common wordlist. Let's analyze the messages:

- + http://192.168.18.209/login (CODE:308|SIZE:0)
- + http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://192.168.18.209 ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential findings.

Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any interesting results on the http://192.168.18.209/ page using the common wordlist. Let's analyze the messages:

- + http://192.168.18.209/login (CODE:308|SIZE:0)
- + http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://192.168.18.209 ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential findings.

Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any interesting results on the http://192.168.18.209/ page using the common wordlist. Let's analyze the messages:

- + http://192.168.18.209/login (CODE:308|SIZE:0)
- + http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpmyadmin2 (CODE:200|SIZE:18935)
- + http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential findings.

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any注入点 (Injection Points) on the http://192.168.18.209/ page using the current wordlist. Let's break down what the messages mean:

```
(root㉿kali)-[~/home/satriasheva/sqlmap-dev]
# dirb http://192.168.18.209

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jun 7 03:34:04 2025
URL_BASE: http://192.168.18.209/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.18.209/ ---
+ http://192.168.18.209/login (CODE:308|SIZE:0)
+ http://192.168.18.209/phpmyadmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)
+ http://192.168.18.209/phpMyAdmin2 (CODE:200|SIZE:18935)

END_TIME: Sat Jun 7 03:34:53 2025
DOWNLOADED: 4612 - FOUND: 5
```

Let's break down the sqlmap output and discuss the potential findings.

#### Understanding the sqlmap Output

The output from sqlmap indicates that it could not find any注入点 (Injection Points) on the http://192.168.18.209/ page using the current wordlist. Let's break down what the messages mean:

5. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan web scanning yang berlebihan dengan tools Dirb.

2025-06-08T05:16:59.43 9532-0400	fileInfo	192.168.18.213:80	192.168.18.225:4659 2	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		
2025-06-08T05:16:59.42 7730-0400	tls	192.168.18.225:4661 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.39 6653-0400	http	192.168.18.225:4660 2	192.168.18.213:80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/bookNSE.html)		
2025-06-08T05:16:59.39 6231-0400	alert	192.168.18.225:4660 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C When Application Attacks Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1		
2025-06-08T05:16:59.38 7945-0400	tls	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.36 8974-0400	tls	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/bookNSE.html)		
2025-06-08T05:16:59.33 7575-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1		
2025-06-08T05:16:59.32 9978-0400	fileInfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		
2025-06-08T05:16:59.32 0044-0400	fileInfo	192.168.18.213:80	192.168.18.225:4657 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		

2025-06-08T05:16:59.43 9532-0400	fileInfo	192.168.18.213:80	192.168.18.225:4659 2	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		
2025-06-08T05:16:59.42 7730-0400	tls	192.168.18.225:4661 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.39 6653-0400	http	192.168.18.225:4660 2	192.168.18.213:80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/bookNSE.html)		
2025-06-08T05:16:59.39 6231-0400	alert	192.168.18.225:4660 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1		
2025-06-08T05:16:59.38 7945-0400	tls	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.36 8974-0400	tls	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A		
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/bookNSE.html)		
2025-06-08T05:16:59.33 7575-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1		
2025-06-08T05:16:59.32 9978-0400	fileInfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		
2025-06-08T05:16:59.32 0044-0400	fileInfo	192.168.18.213:80	192.168.18.225:4657 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A		

Suricata Log - 192.168.18.213/jaringan.php						
2025-06-08T05:16:59.43 9532-0400	fileinfo	192.168.18.213:80	192.168.18.225:4659 2	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42 7730-0400	tls	192.168.18.225:4661 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39 6653-0400	http	192.168.18.225:4660 2	192.168.18.213:80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39 6231-0400	alert	192.168.18.225:4660 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38 7945-0400	tls	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tls	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7575-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
Suricata Log - 192.168.18.213/jaringan.php						
2025-06-08T05:16:59.43 9532-0400	fileinfo	192.168.18.213:80	192.168.18.225:4659 2	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42 7730-0400	tls	192.168.18.225:4661 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39 6653-0400	http	192.168.18.225:4660 2	192.168.18.213:80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39 6231-0400	alert	192.168.18.225:4660 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38 7945-0400	tls	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tls	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7575-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
Suricata Log - 192.168.18.213/jaringan.php						
2025-06-08T05:16:59.43 9532-0400	fileinfo	192.168.18.213:80	192.168.18.225:4659 2	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.42 7730-0400	tls	192.168.18.225:4661 2	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.39 6653-0400	http	192.168.18.225:4660 2	192.168.18.213:80	TCP		HTTP Request: GET 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.39 6231-0400	alert	192.168.18.225:4660 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.38 7945-0400	tls	192.168.18.225:4659 8	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.36 8974-0400	tls	192.168.18.225:4658 6	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.33 8354-0400	http	192.168.18.225:4659 2	192.168.18.213:80	TCP		HTTP Request: OPTIONS 192.168.18.213/ Status: 200, User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
2025-06-08T05:16:59.33 7575-0400	alert	192.168.18.225:4659 2	192.168.18.213:80	TCP	http	Signature: ET SCAN Possible Nmap User-Agent Observed, Severity: 1, C Web Application Attack Action: allowed, GID: 1, Rev: 5 Potensi Serangan Nmap dari: 192.168.18.225 Attack Count: 1
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4658 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.32 9978-0400	fileinfo	192.168.18.213:80	192.168.18.225:4657 0	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

## V. ANALISA DAN KESIMPULAN

### Analisa

Dari serangkaian pengujian penyerangan yang dilakukan terhadap web server yang telah diimplementasikan Suricata sebagai IDS dan Firewalld sebagai firewall, terlihat pola deteksi yang konsisten untuk berbagai jenis serangan aktif. Seluruh percobaan penyerangan yang melibatkan port scanning, brute-force, Distributed Denial of Service (DDoS), dan web scanning berhasil memicu alert berwarna pada log GUI Suricata. Hal ini menunjukkan efektivitas Suricata dalam mengidentifikasi aktivitas-aktivitas mencurigakan yang secara aktif mencoba mengeksploitasi atau membanjiri server atau mencari kerentanan. Deteksi ini didasarkan pada kecocokan pola lalu lintas serangan yang tidak biasa atau bersifat ofensif dengan aturan (signatures) yang telah didefinisikan dalam basis data Suricata. Namun, pada aktivitas percobaan sniffing yang dilakukan dengan Wireshark dan tcpdump tidak terdeteksi sebagai alert berwarna oranye. Hal ini dikarenakan sniffing pada dasarnya merupakan aktivitas pasif, penyerang hanya mendengarkan atau mengamati lalu lintas yang sudah mengalir di jaringan, tanpa secara aktif mengirimkan paket yang melanggar aturan atau memanipulasi server dengan cara yang terdeteksi sebagai serangan

oleh IDS berbasis tanda tangan. Proses login pengguna, meskipun berisi kredensial sensitif, dianggap sebagai lalu lintas aplikasi yang sah. Suricata dirancang untuk mendeteksi pola serangan yang melanggar keamanan.

### Kesimpulan

Secara keseluruhan, implementasi Suricata sebagai IDS dan Firewalld sebagai firewall pada web server menunjukkan efektivitas yang sesuai harapan dalam mendeteksi dan memblokir serangan aktif seperti port scanning, brute-force, DDoS, dan web scanning, dengan Suricata berhasil memicu alert yang relevan. Namun, pengujian network sniffing menegaskan bahwa aktivitas pasif ini tidak terdeteksi sebagai alert oleh IDS berbasis tanda tangan karena sifatnya yang hanya mengamati lalu lintas, bukan menyerang secara aktif. Oleh karena itu, meskipun Suricata dan Firewalld terbukti kuat untuk deteksi dan pencegahan ancaman aktif, keamanan web server yang komprehensif memerlukan strategi multi-lapis, termasuk enkripsi data sensitif (HTTPS) dan solusi tambahan untuk mendeteksi reconnaissance pasif, melengkapi kapabilitas yang telah ditunjukkan.

## VI. DAFTAR PUSTAKA

Maulana dan A. F. Rochman, "Keamanan Secara Berlapis Menggunakan OSSEC dan Honeytrap Cowrie," *Jurnal Sistem Komputer dan Informatika (SISFOKOM)*, vol. 4, no. 2, hal. 110-117, 2023. [Online]. Tersedia: <https://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/1246/801>

P. Y. Pinontoan dan I. Sembiring, "Implementasi dan Analisis Deteksi Serangan Jaringan pada Web Server NFT Menggunakan Suricata," *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 4, no. 1, hal. 65-78, 2024.

<https://ejurnal.unima.ac.id/index.php/edutik/article/download/9428/5045>