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 mendiagnosis 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 dieksploitasi 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.

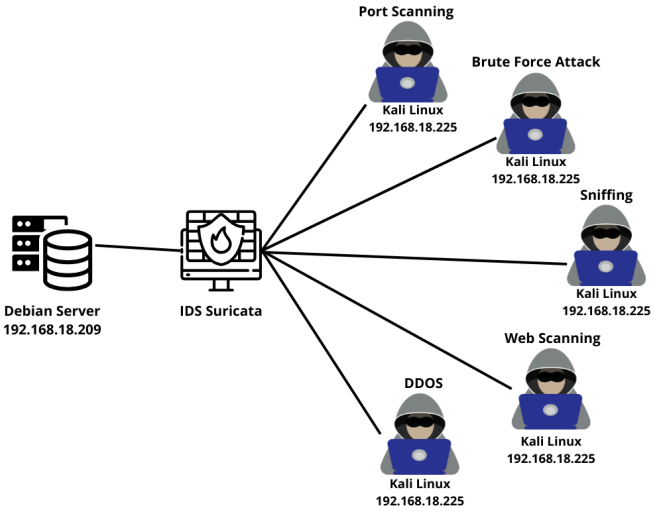
III. PERALATAN

Adapun peralatan praktikum adalah :

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

IV. KEGIATAN PRAKTIKUM

Topologi



Konsep

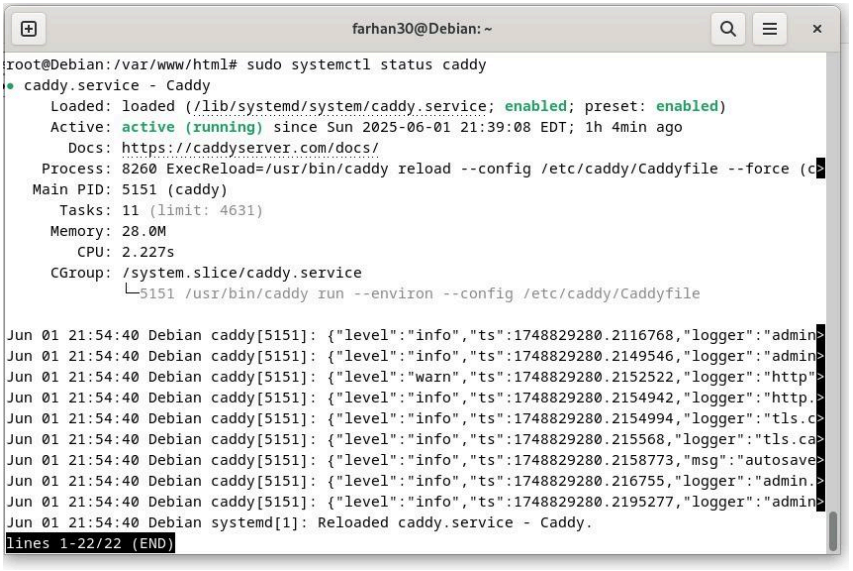
Dalam praktikum ini akan dilakukan penyerangan terhadap Web Server Caddy. Penyerangan akan dilakukan lima kali dengan tools yang sudah dipilih. Beberapa penyerangan yang akan dilakukan yaitu port scanning, brute force attack, sniffing, DDOS, dan web scanning. Beberapa penyerangan yang akan dilakukan 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

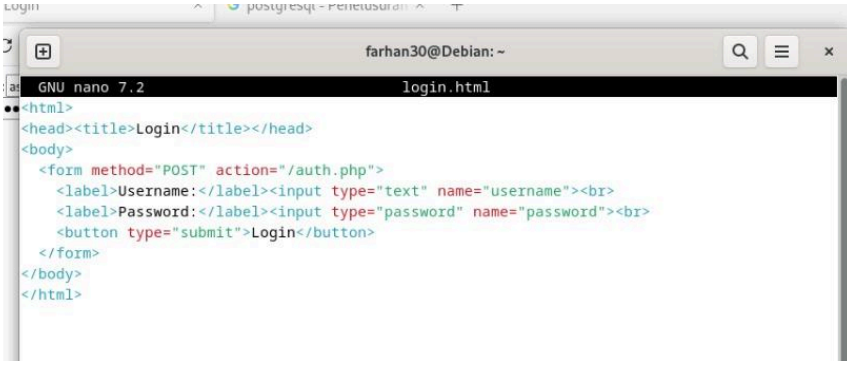
A. Penyerangan

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 konektivitas.
2. Selanjutnya install web server Caddy dengan perintah **sudo apt install caddy -y** lalu pastikan status layanan nya sudah aktif.

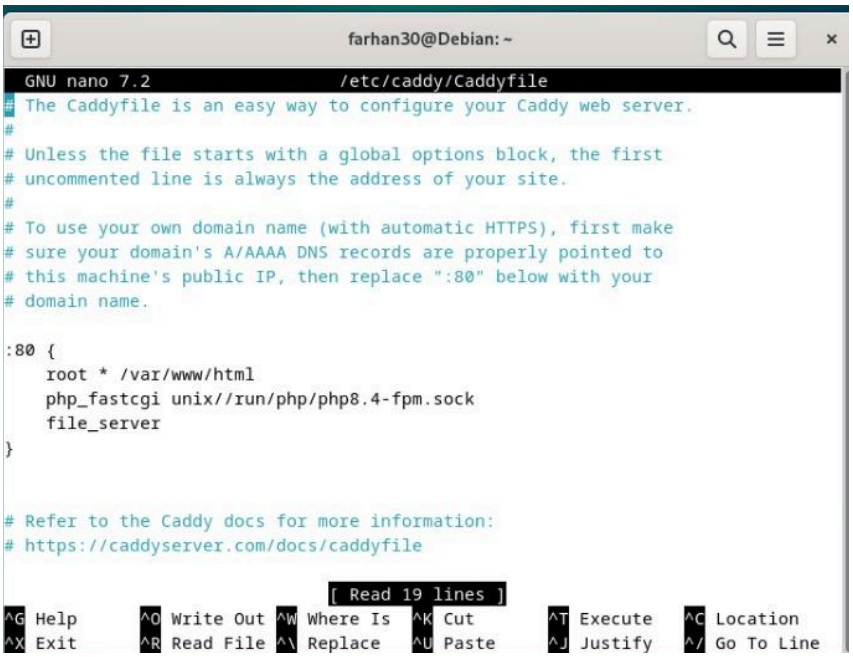


3. Mengedit beberapa konfigurasi web untuk proses login user pada file login.html, dashboard.php, dan auth.php.

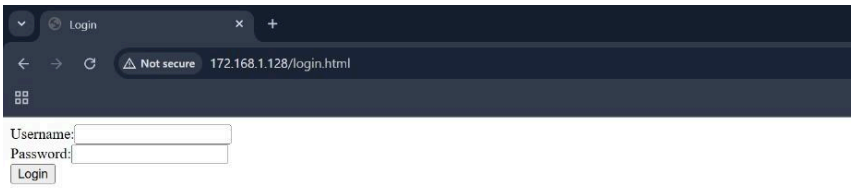


4. Mengedit konfigurasi pada Caddy file dengan menambahkan PHP-PFM, namun sebelumnya perlu menginstall PHP-FPM dengan perintah **sudo apt**

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

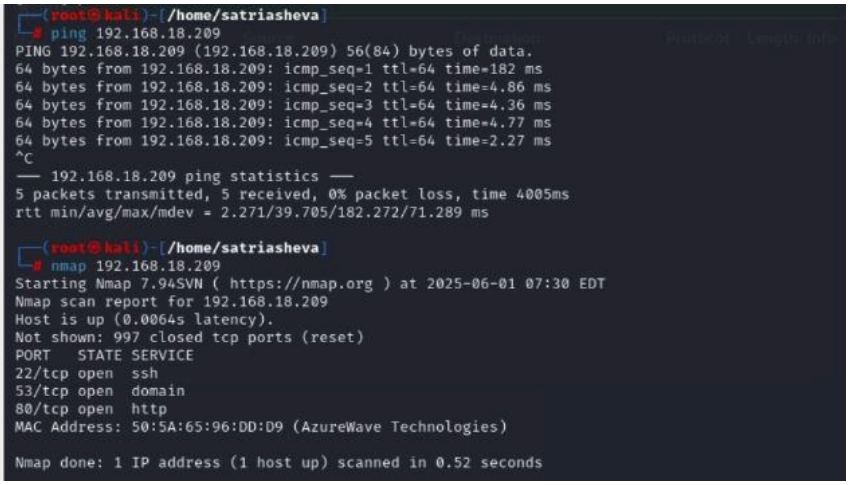


5. Menjalankan web server Caddy di browser dengan ketik IP dari server Debian pada file login.html.



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]
└─# 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

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

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

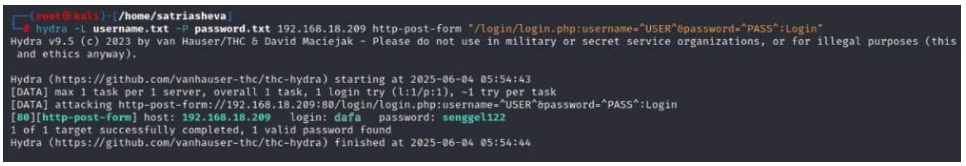
4. Membuat word list password bernama **password.txt** yang berisi list password yang akan dicoba.

```
root@kali: /home/satriasheva
File  Actions  Edit  View  Help
  GNU nano 7.2                                    password.txt *
admin123
12345
123
kera10
senggel122
poltek123
haha123
rakha123
pnm127
127187hs
korsa1291
kipas5757
rumah12
lantai12
keramik31
uiiiii12
yfywqn21
yugubuu12
126bjjhj
```

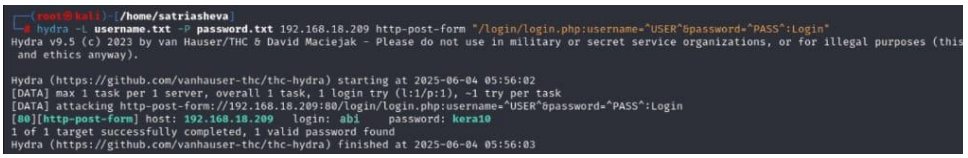
5. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server caddy dengan username admin dan password admin123 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login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

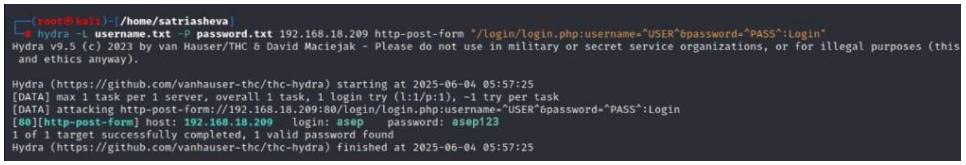
6. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username dafa dan password senggel122 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login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



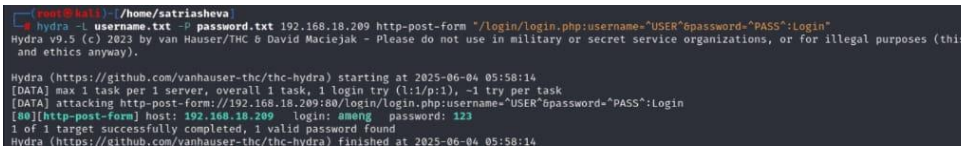
7. Melakukan menjalankan tool Hydra untuk melakukan brute-force terhadap formulir login HTTP di web server Caddy dengan username abi dan password kera10 berhasil dengan perintah **hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/auth.php:username=^USER^&password=^PASS^:Login gagal"**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



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



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



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

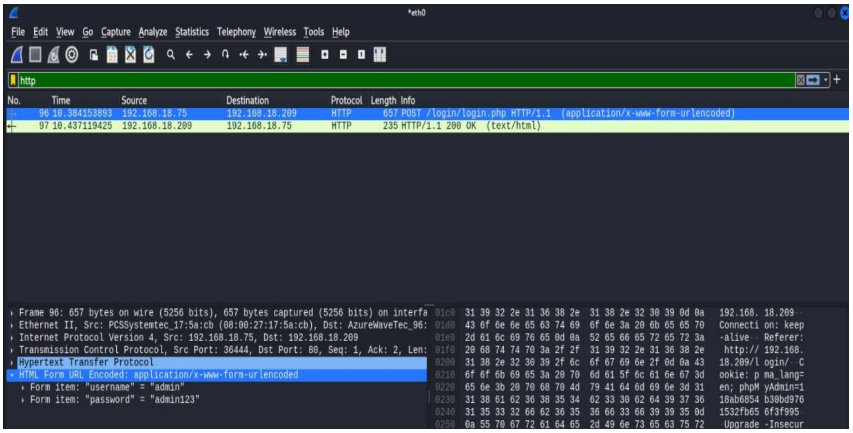
```
┌──(root㉿kali)-[/home/satriasheva]
└─# 2025-06-04 05:45:37 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: asep (1 of 1,
2025-06-04 05:45:37 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: asep Password: asep123 [SUCCESS]

[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

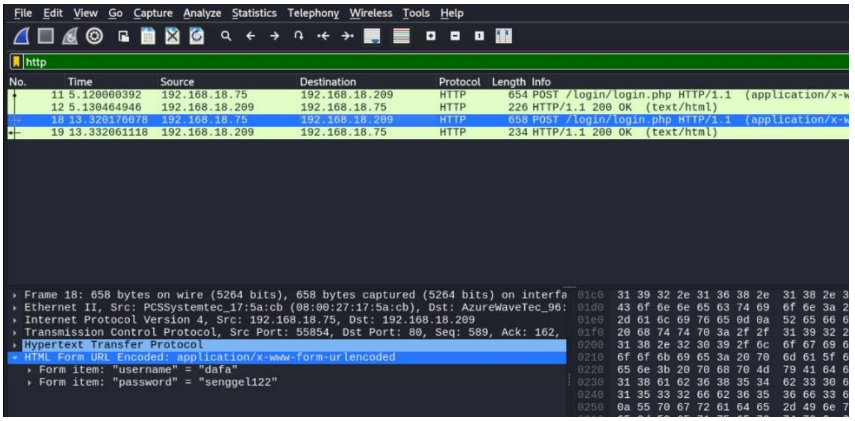
```
┌──(root㉿kali)-[/home/satriasheva]
└─# 2025-06-04 05:44:55 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: ameng (1 of 1
2025-06-04 05:44:55 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: ameng Password: 123 [SUCCESS]

[1]  + done       medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

d. Sniffing

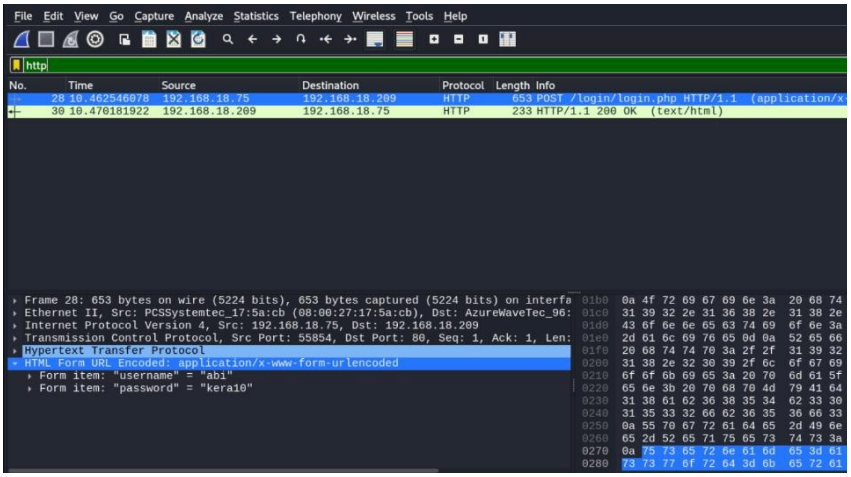
1. Sniffing dilakukan melalui dua tools yang berbeda, yaitu melalui Wireshark dan tcpdump.
2. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **admin** dan password: **admin123**.



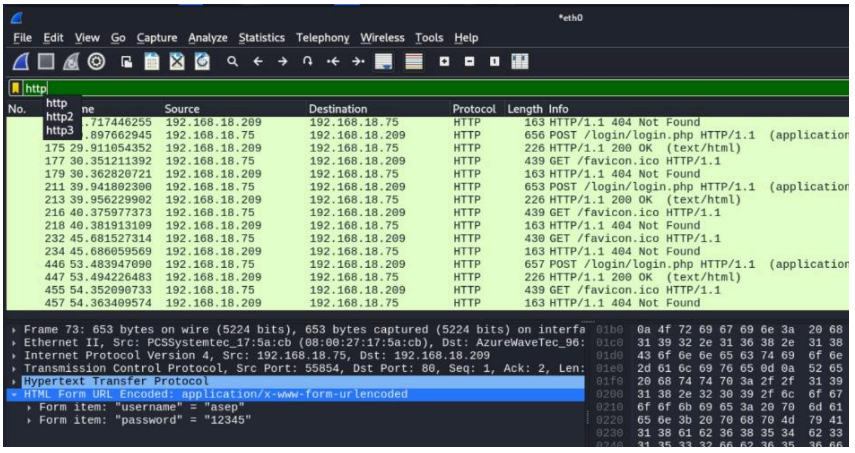
3. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **dafa** dan password: **senggel122**.



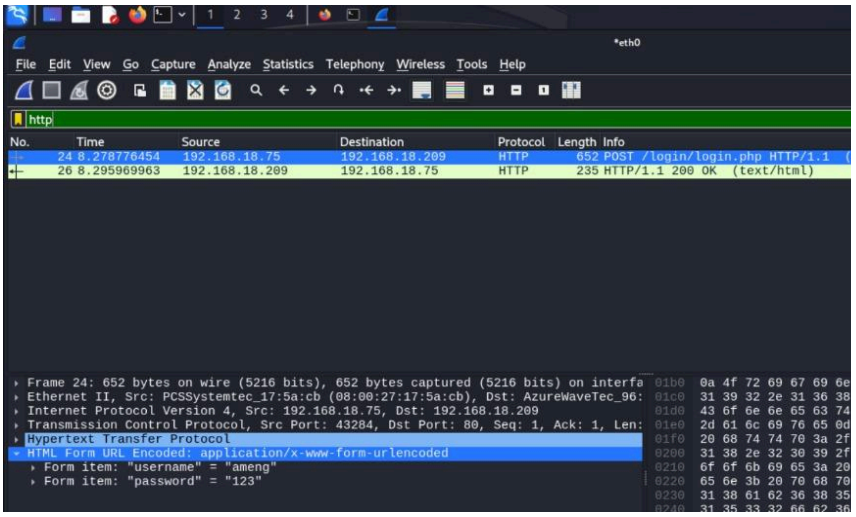
4. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **abi** dan password: **kera10**.



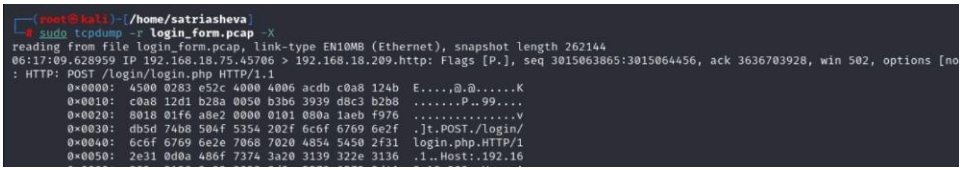
5. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** adalah username: **asep** dan password: **12345**.



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**.

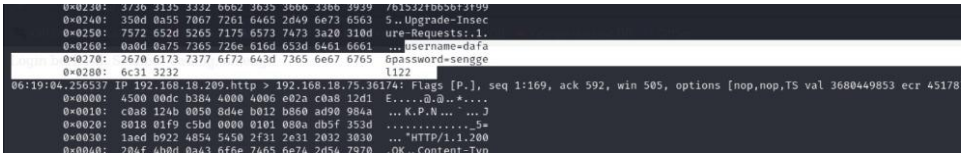


7. Sniffing melalui tcpdump yang dilakukan pada saat user login ke web server dengan perintah **sudo tcpdump -r login_form.pcap -X**.

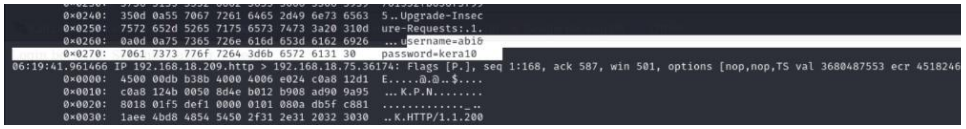


8. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **admin** dan password: **admin123**.

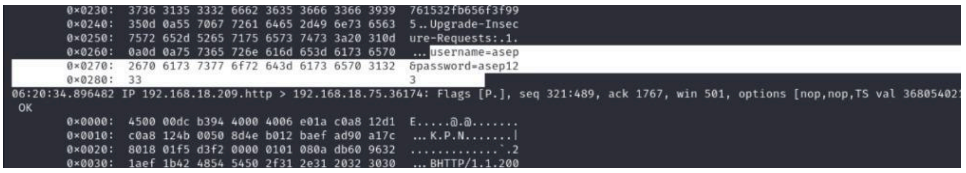
9. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **dafa** dan password: **senggel122**.



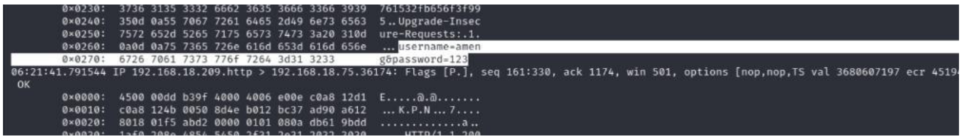
10. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **abi** dan password: **kera10**.



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

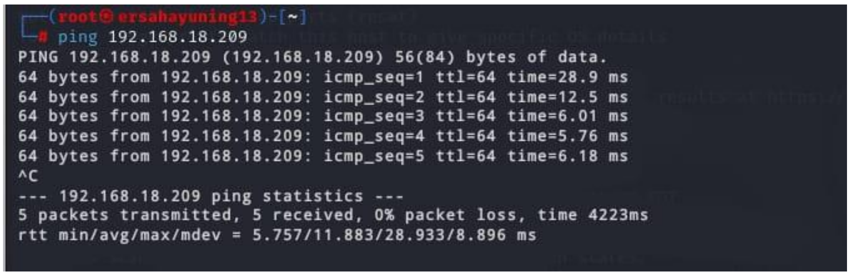


12. Hasilnya menunjukkan bahwa username dan password yang dikirimkan dan terlihat pada lognya tercatat username: **ameng** dan password: **123**.

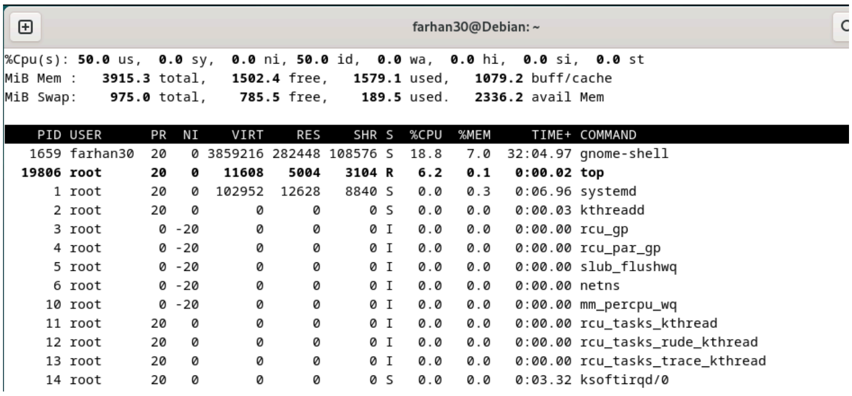


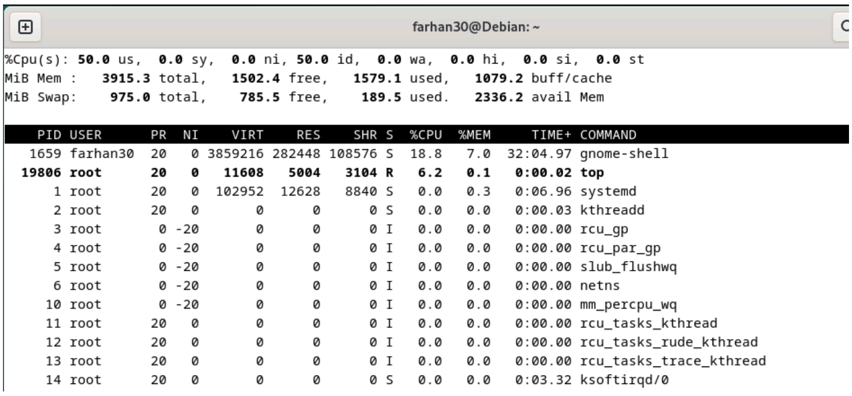
e. DDOS melalui Kali Linux

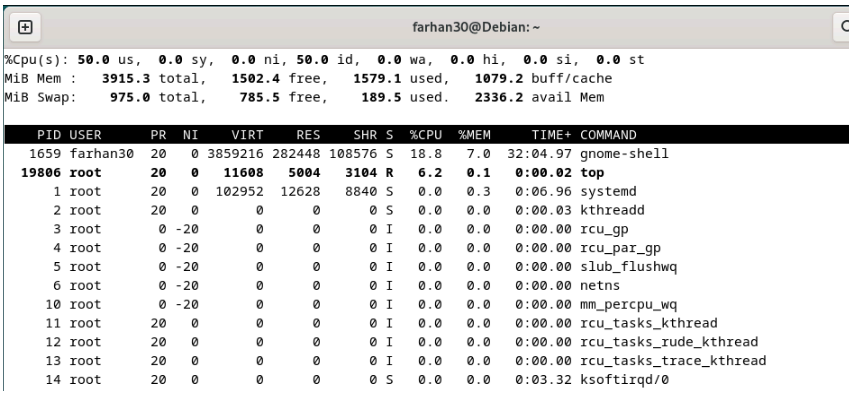
1. Melihat ping ke IP server terlebih dahulu sebelum dilakukan DDOS.



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 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
  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   0:03.32 ksoftirqd/0
```

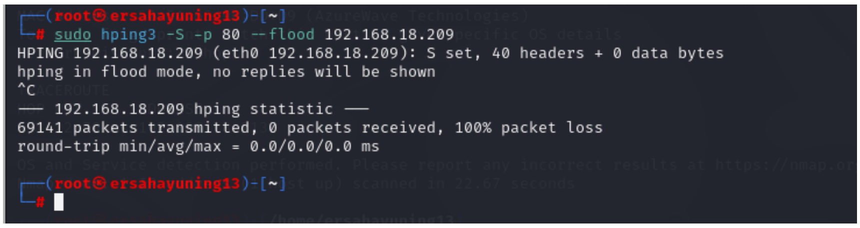

3. Melakukan DDOS dengan perintah **hping3 -S -p 80 --flood 192.168.18.209**.

```
┌──(root㉿ersahayuning13)-[~]
└─# sudo hping3 -S -p 80 --flood 192.168.18.209
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

┌──(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
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

┌──(root㉿ersahayuning13)-[~]
└─#
```

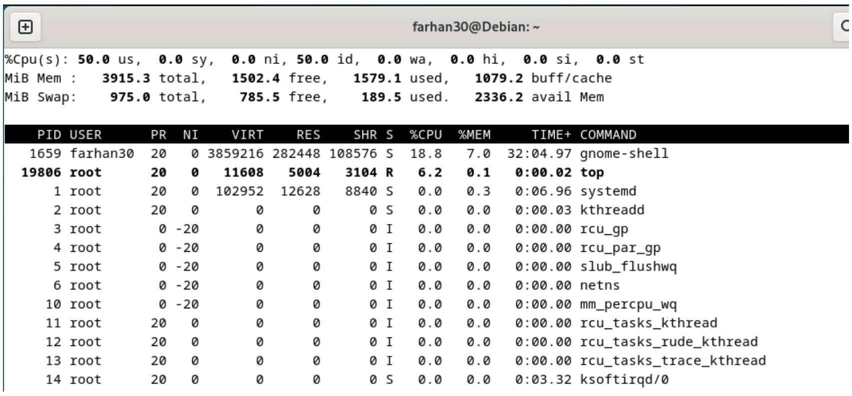
```
┌──(root㉿ersahayuning13)-[~]
└─# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.209 hping statistic ---
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(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
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

┌──(root㉿ersahayuning13)-[~]
└─#
```

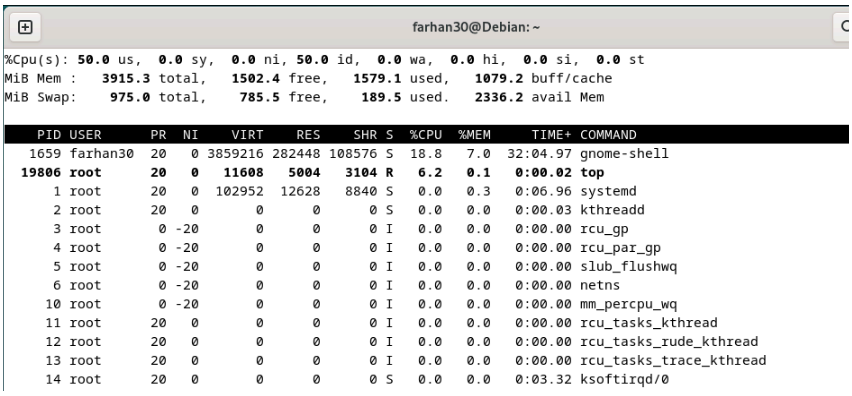


```
┌──(root㉿ersahayuning13)-[~]
└─# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.209 hping statistic ---
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿ersahayuning13)-[~]
└─# 
```

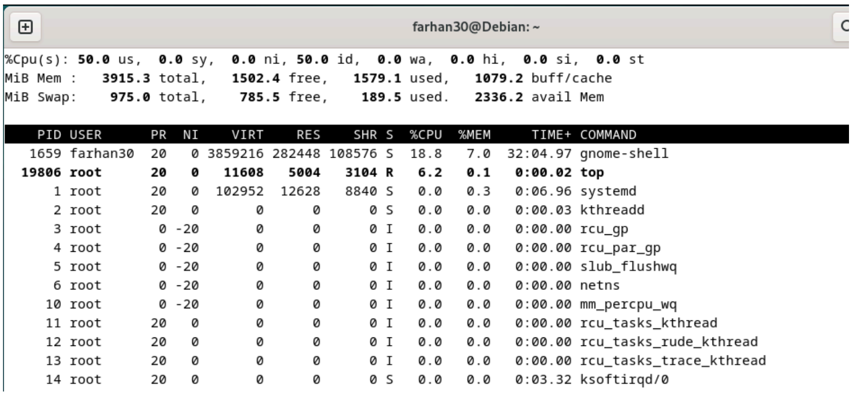
4. Cek kondisi CPU kembali dengan top setelah dilakukan DDOS. Kondisi CPU tidak ada perubahan signifikan.



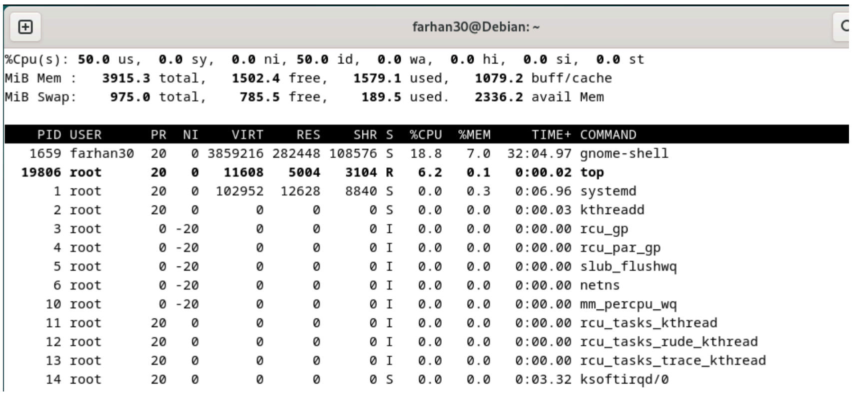
```
farhan30@Debian: ~
%Cpu(s): 50.0 us,  0.0 sy,  0.0 ni, 50.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3915.3 total,   1502.4 free,   1579.1 used,   1079.2 buff/cache
MiB Swap:    975.0 total,    785.5 free,    189.5 used.   2336.2 avail Mem

    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 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
```

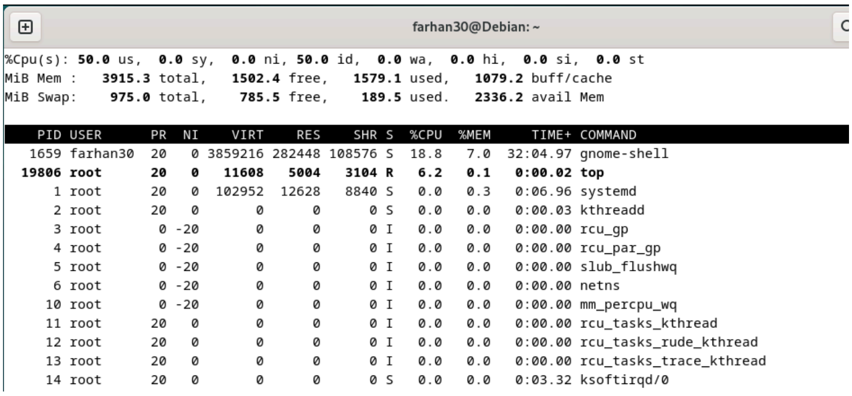



```
farhan30@Debian: ~
%Cpu(s): 50.0 us,  0.0 sy,  0.0 ni, 50.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3915.3 total,   1502.4 free,   1579.1 used,   1079.2 buff/cache
MiB Swap:    975.0 total,    785.5 free,    189.5 used.   2336.2 avail Mem

    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
  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   0:03.32 ksoftirqd/0
```

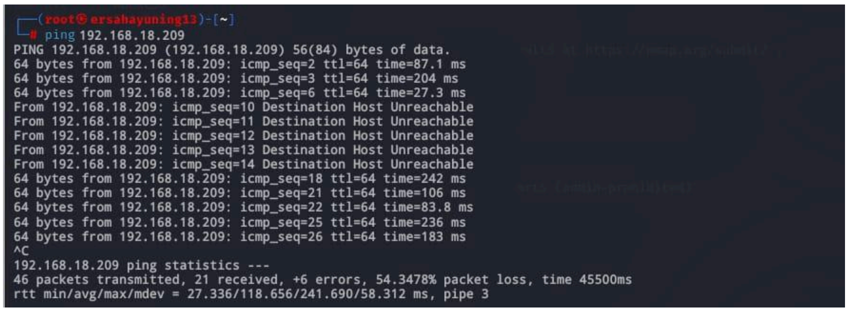



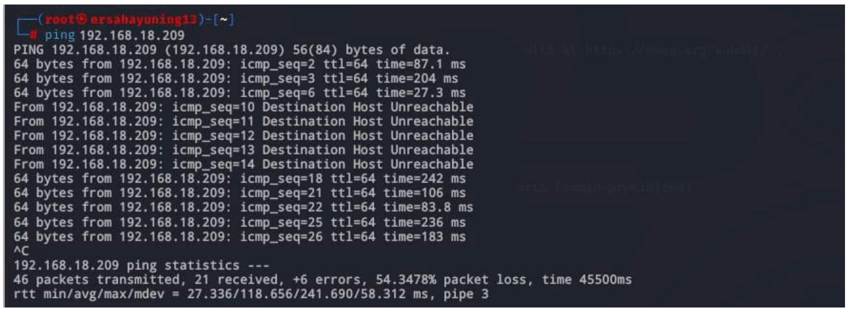

```
farhan30@Debian: ~
%Cpu(s): 50.0 us,  0.0 sy,  0.0 ni, 50.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3915.3 total,   1502.4 free,   1579.1 used,   1079.2 buff/cache
MiB Swap:    975.0 total,    785.5 free,    189.5 used.   2336.2 avail Mem

    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 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
```

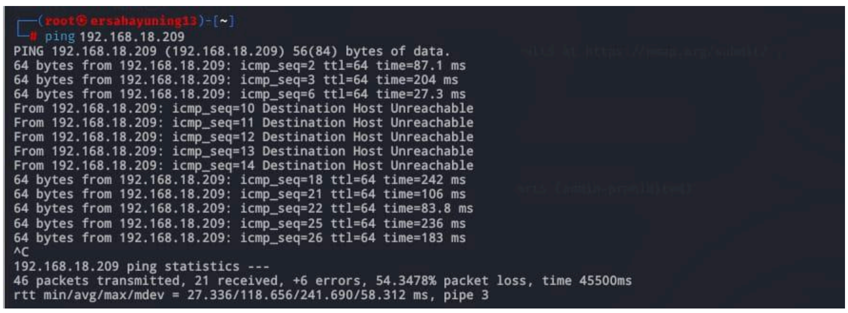




5. Lihat ping nya kembali setelah dilakukan DDOS apakah ada perubahan atau tidak. Tidak ada perubahan yang signifikan pada hasil respon time pada ping.





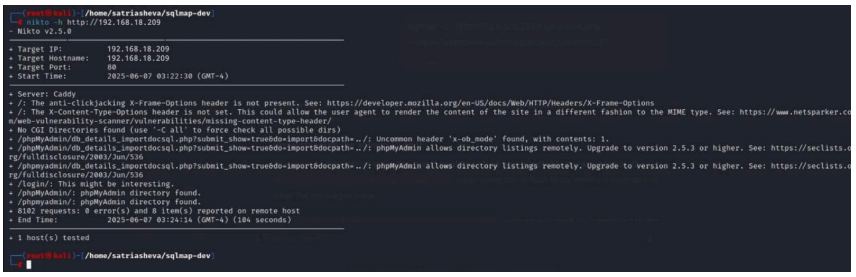


```
┌──(root㉿ersahayuning13)-[~]
└─# ping 192.168.18.209
PING 192.168.18.209 (192.168.18.209) 56(84) bytes of data.
64 bytes from 192.168.18.209: icmp_seq=2 ttl=64 time=87.1 ms
64 bytes from 192.168.18.209: icmp_seq=3 ttl=64 time=204 ms
64 bytes from 192.168.18.209: icmp_seq=6 ttl=64 time=27.3 ms
From 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㉿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=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 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/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importdocsql.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_importdocsql.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
+ /login/: This might be interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-06-07 03:24:14 (GMT-4) (104 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 v2.5.0
+ 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 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/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importdocsql.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_importdocsql.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
+ /login/: This might be interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-06-07 03:24:14 (GMT-4) (104 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 v2.5.0
---------------------------------------------------------------------------
+ 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 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/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importdocsql.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_importdocsql.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
+ /login/: This might be interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-06-07 03:24:14 (GMT-4) (104 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 v2.5.0
---------------------------------------------------------------------------
+ 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 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/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/db_details_importdocsql.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_importdocsql.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
+ /login/: This might be interesting.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-06-07 03:24:14 (GMT-4) (104 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[/home/satriasheva/sqlmap-dev]
└─#
```

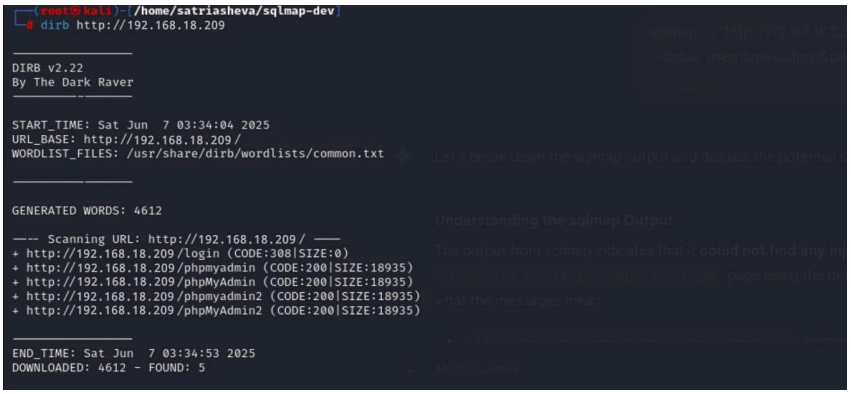

3. Web scanning yang kedua dilakukukan dengan tools Dirb.

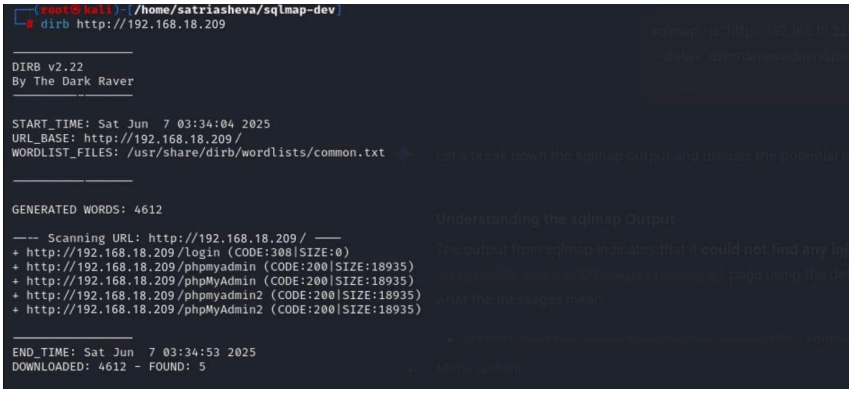
```
┌──(root㉿kali)-[/home/satriasheva/sqlmap-dev]
└─# dirb http://192.168.18.209

-----------------
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
```


```
┌──(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
```



```
┌──(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
```

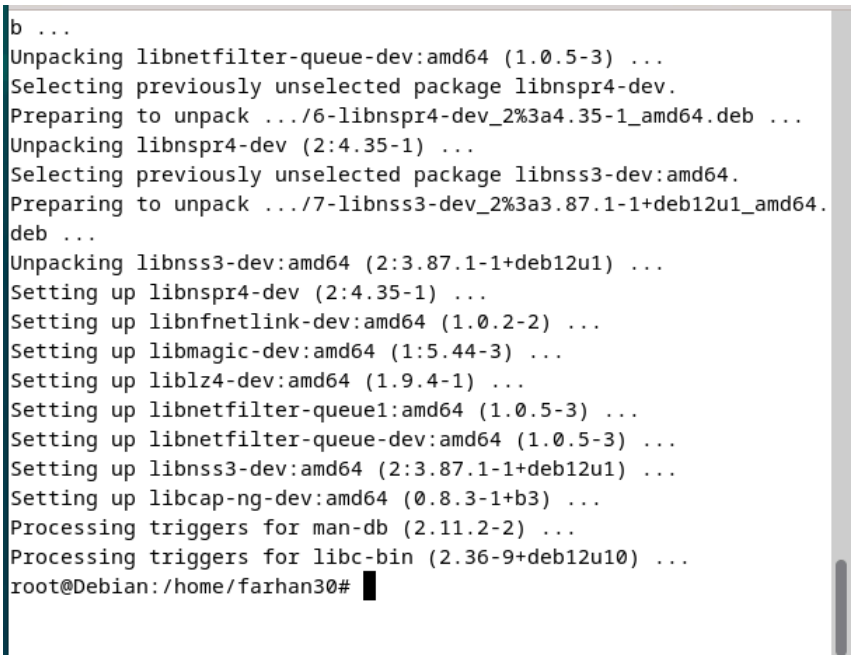




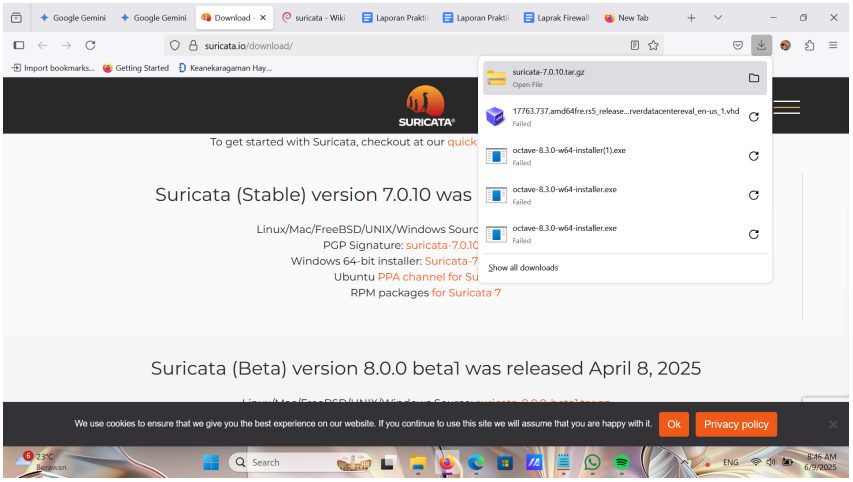
B. Pertahanan

a. Instalasi Suricata dan Membuat Tampilan GUI Suricata

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



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



3. 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#
```

4. 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 descr>
# 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:
^G Help      M-C Case Sens M-B Backwards ^P Older     ^T Go To Line
```

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

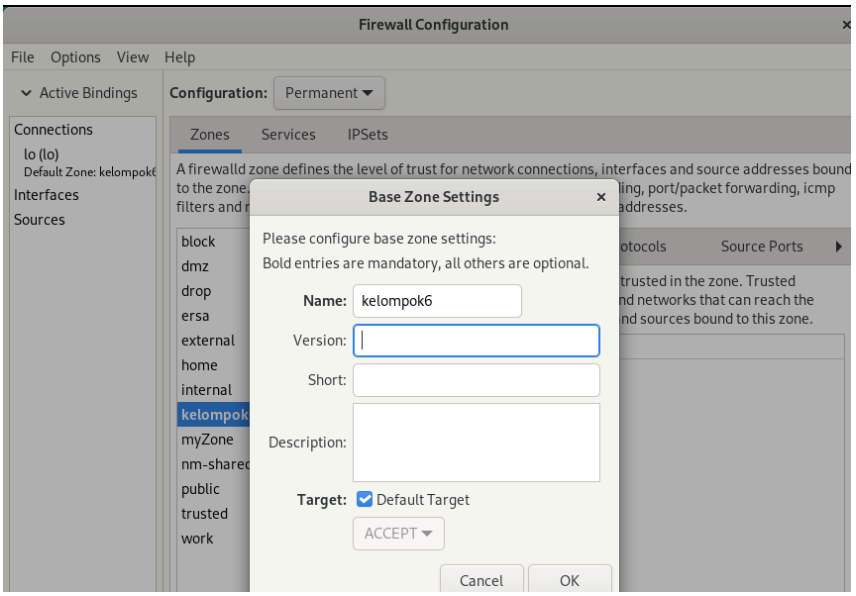
```
depcomp         Makefile.in
doc             missing
root@Debian:/home/farhan30/Downloads/suricata-7.0.10# nano surica
ta.yaml
root@Debian:/home/farhan30/Downloads/suricata-7.0.10# sudo system
ctl status suricata
● suricata.service - Suricata IDS/IPS daemon
     Loaded: loaded (/etc/systemd/system/suricata.service; enabl>
     Active: active (running) since Sun 2025-06-08 20:49:12 EDT;>
   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.y>

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 Suric>
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)
```

6. 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**.

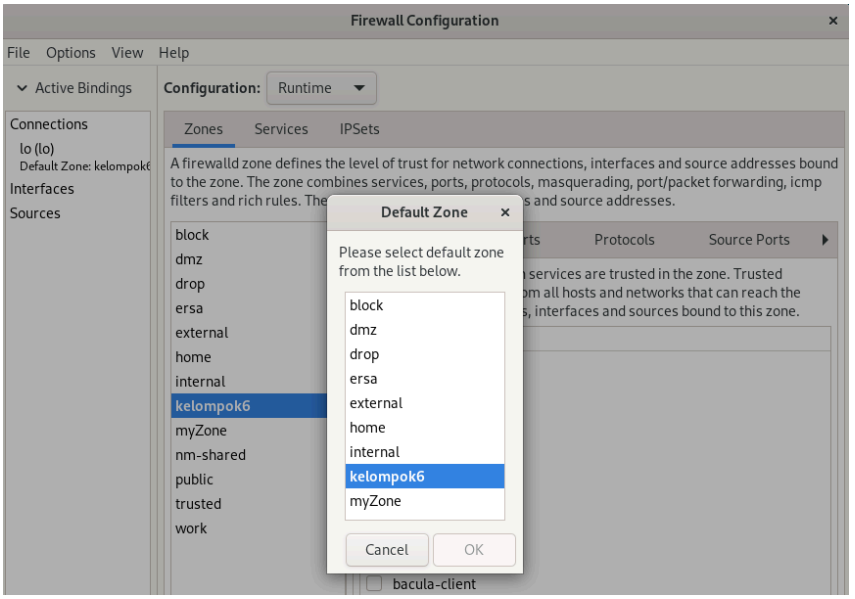
```
farhan30@Debian: ~
 GNU nano 7.2                  jaringan.php
<?php
// suricata_log_viewer_simple.php

// 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 Sur>
$linesToRead = 100; // Jumlah baris terakhir yang dibaca
$attackLogFile = "/var/log/suricata/attack_tracker.json"; // Fil>
$blockThreshold = 5; // Batas serangan sebelum IP diblokir

// --- FUNGSI PEMROSESAN LOG ---
function getLogData($logFile, $linesToRead) {
    $logs = [];
    if (file_exists($logFile)) {
        $command = "tail -n " . (int)$linesToRead . " " . escape>
                        [ Read 362 lines ]
^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

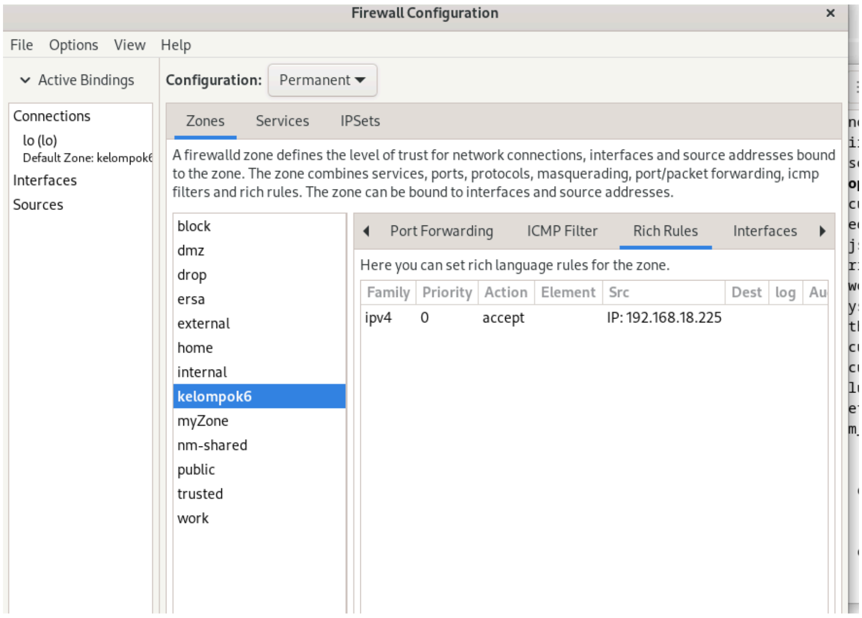
1. Menginstall GUI FirewallD pada server Debian dengan perintah **sudo apt install firewall-config**.
2. Menjalankan GUI FirewallD dengan perintah **sudo firewall-config**.
3. Mengatur Configuration menjadi **Permanent** dan membuat zone baru yaitu **kelompok6** dengan klik icon Plus (+). Firewalld direload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



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



5. 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.



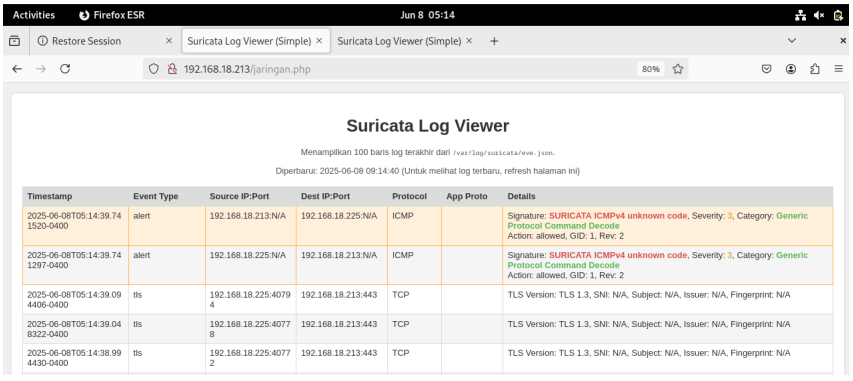
c. **Port Scanning**

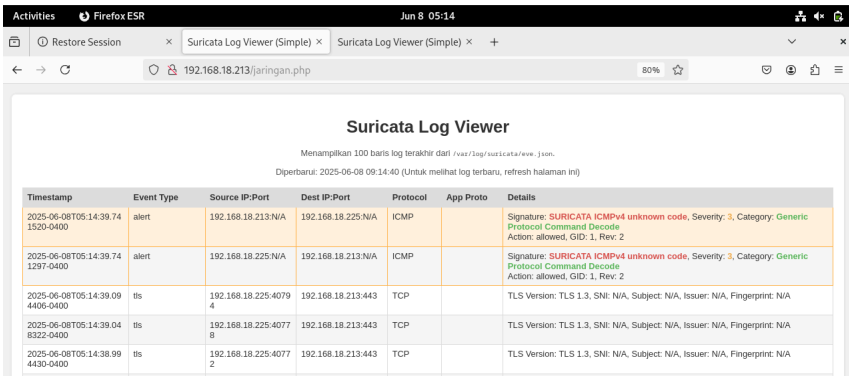
1. Penyerang melakukan scanning pada Kali Linux terhadap port dan IP dari server Debian,
2. Scanning yang pertama dilakukan menggunakan tools Nmap

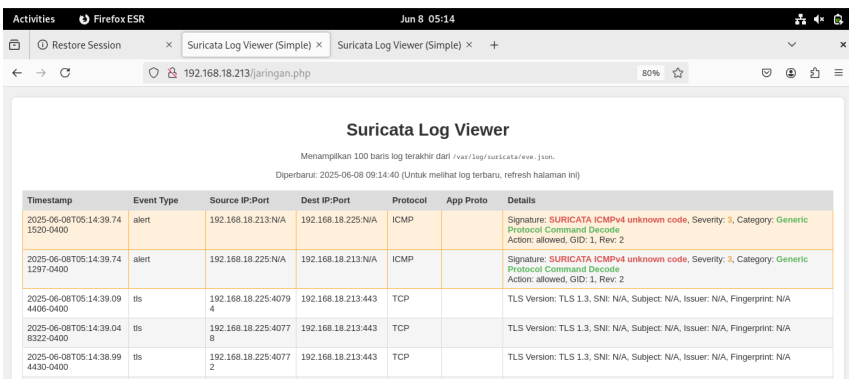
```
┌──(root㉿ersahayuning13)-[/home/ersahayuning13]
└─# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp 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]
└─#
```

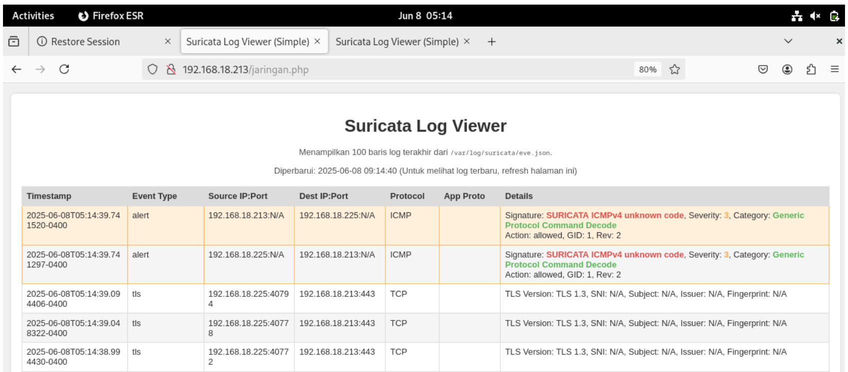

```
┌──(root㉿ersahayuning13)-[/home/ersahayuning13]
└─# nmap 192.168.18.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 05:07 EDT
Nmap scan report for 192.168.18.213
Host is up (0.0100s latency).
All 1000 scanned ports on 192.168.18.213 are in ignored states.
Not shown: 1000 filtered tcp 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]
└─#
```

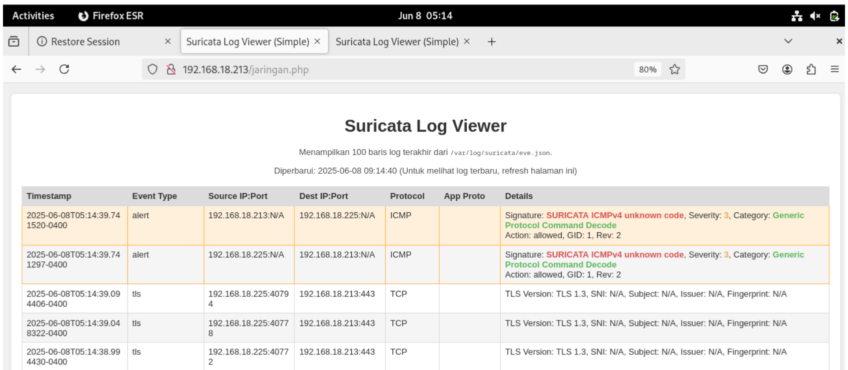

3. Tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 saat melakukan scanning Nmap



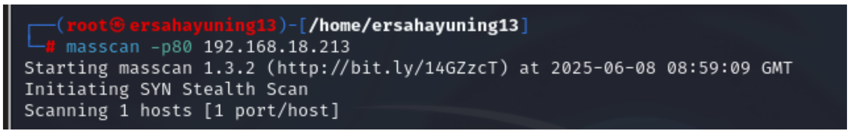


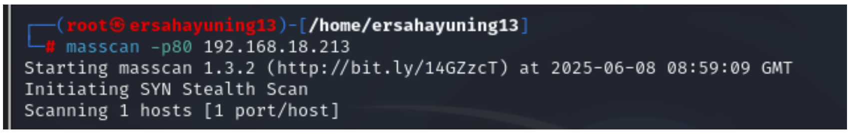


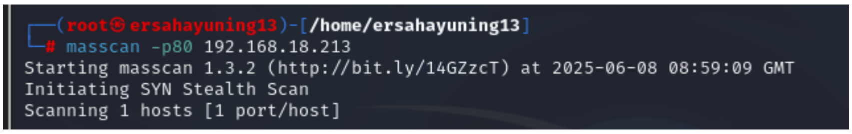


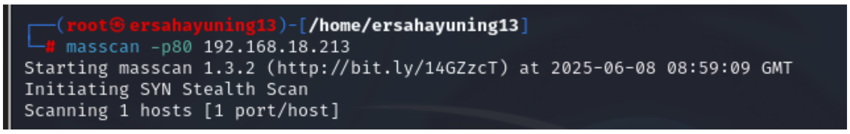


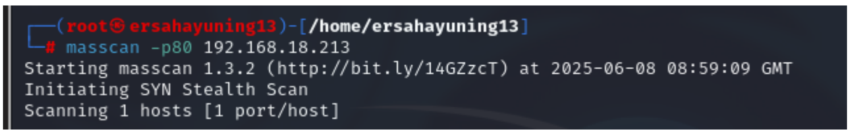
4. Scanning yang kedua dilakukan menggunakan tools masscan



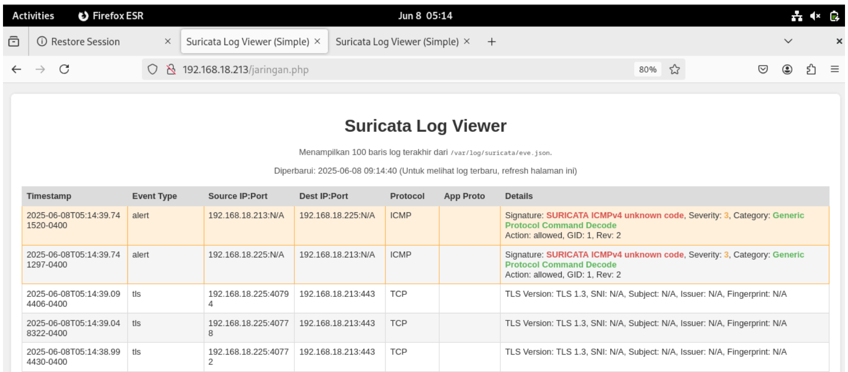


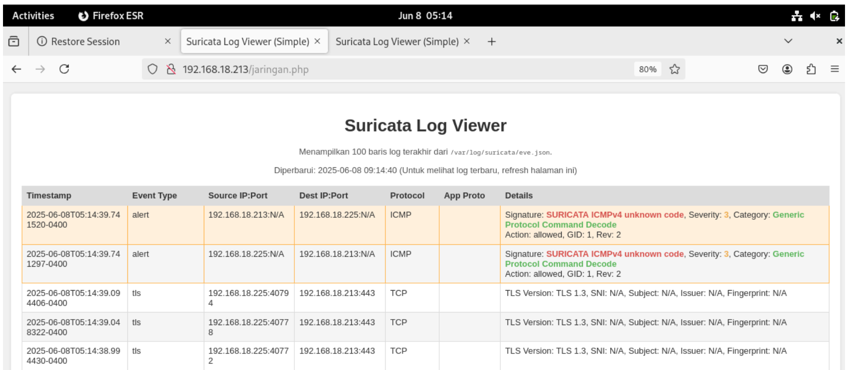


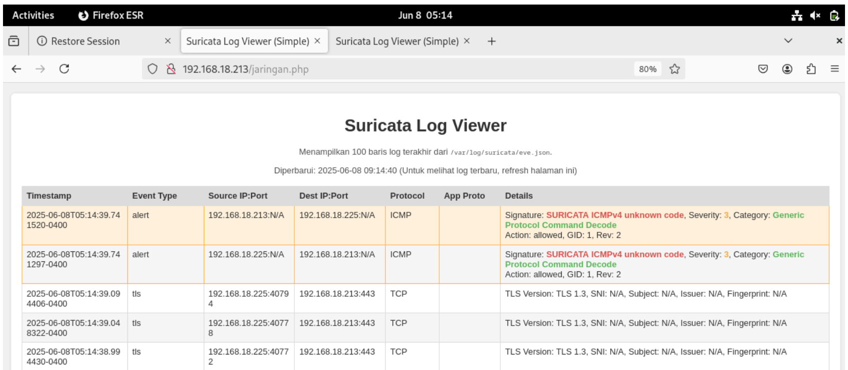


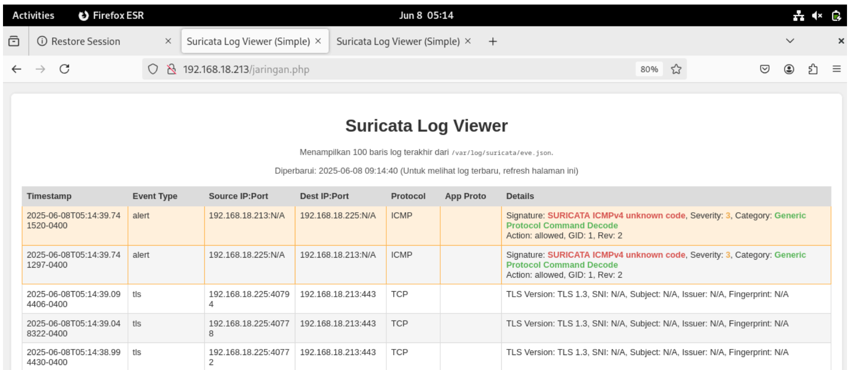


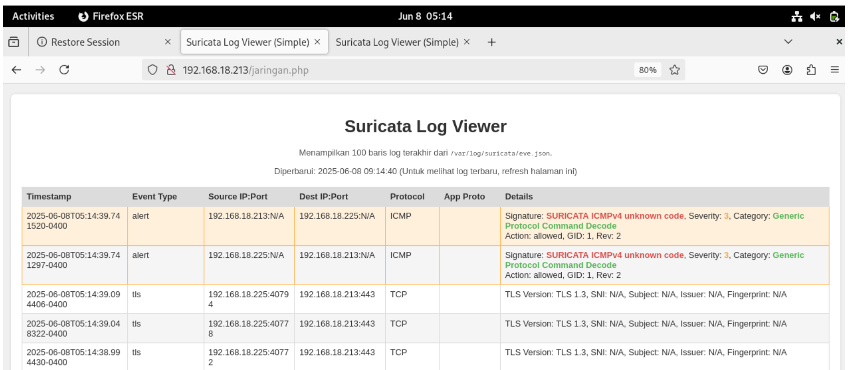
5. Tampilan log pada gui Suricata juga sama, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan scanning Masscan.


Activities
Firefox ESR
Jun 8 05:14
Restore Session
Suricata Log Viewer (Simple)
Suricata Log Viewer (Simple)
192.168.18.213/jaringan.php
80%
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
2025-06-08T05:14:39.741520-0400 | 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
2025-06-08T05:14:39.741297-0400 | 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
2025-06-08T05:14:39.094406-0400 | tls | 192.168.18.225:40794 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.048322-0400 | tls | 192.168.18.225:40778 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.994430-0400 | tls | 192.168.18.225:40772 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A


Activities
Firefox ESR
Jun 8 05:14
Restore Session
Suricata Log Viewer (Simple)
Suricata Log Viewer (Simple)
192.168.18.213/jaringan.php
80%
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
2025-06-08T05:14:39.741520-0400 | 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
2025-06-08T05:14:39.741297-0400 | 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
2025-06-08T05:14:39.094406-0400 | tls | 192.168.18.225:40794 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.048322-0400 | tls | 192.168.18.225:40778 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.994430-0400 | tls | 192.168.18.225:40772 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

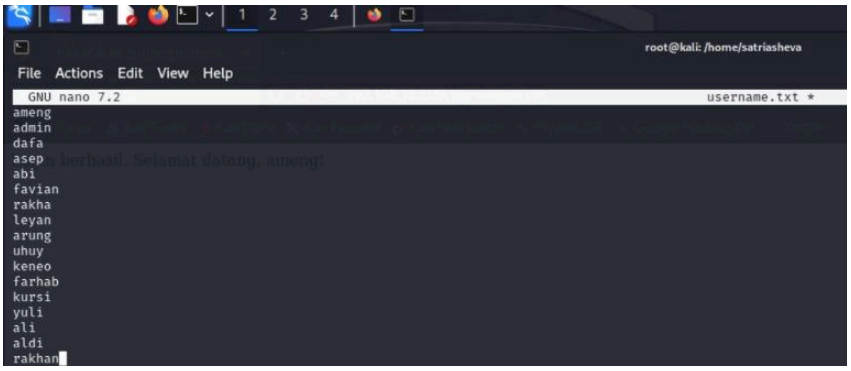

Activities
Firefox ESR
Jun 8 05:14
Restore Session
Suricata Log Viewer (Simple)
Suricata Log Viewer (Simple)
192.168.18.213/jaringan.php
80%
Suricata Log Viewer
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)
Timestamp | Event Type | Source IP:Port | Dest IP:Port | Protocol | App Proto | Details
2025-06-08T05:14:39.741520-0400 | 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
2025-06-08T05:14:39.741297-0400 | 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
2025-06-08T05:14:39.094406-0400 | tls | 192.168.18.225:40794 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.048322-0400 | tls | 192.168.18.225:40778 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.994430-0400 | tls | 192.168.18.225:40772 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A


Activities
Firefox ESR
Jun 8 05:14
Restore Session
Suricata Log Viewer (Simple)
Suricata Log Viewer (Simple)
192.168.18.213/jaringan.php
80%
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
2025-06-08T05:14:39.741520-0400 | 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
2025-06-08T05:14:39.741297-0400 | 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
2025-06-08T05:14:39.094406-0400 | tls | 192.168.18.225:40794 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.048322-0400 | tls | 192.168.18.225:40778 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.994430-0400 | tls | 192.168.18.225:40772 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

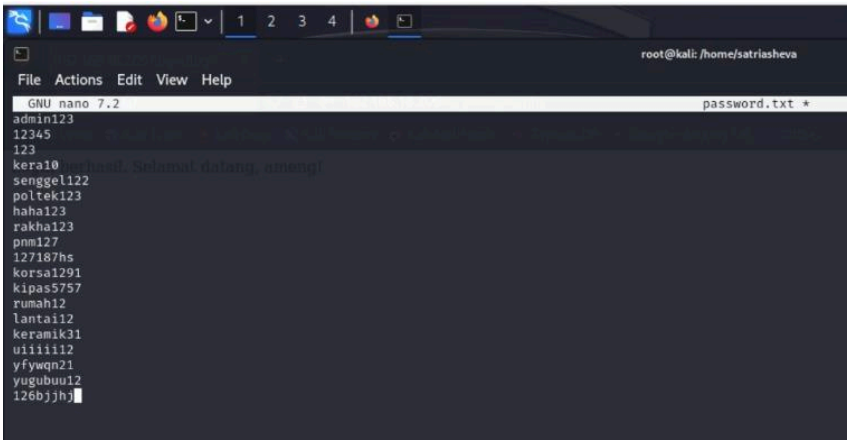

Activities
Firefox ESR
Jun 8 05:14
Restore Session
Suricata Log Viewer (Simple)
Suricata Log Viewer (Simple)
192.168.18.213/jaringan.php
80%
Suricata Log Viewer
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.
Diperbarui: 2025-06-08 09:14:40 (Untuk melihat log terbaru, refresh halaman ini)
Timestamp | Event Type | Source IP:Port | Dest IP:Port | Protocol | App Proto | Details
2025-06-08T05:14:39.741520-0400 | 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
2025-06-08T05:14:39.741297-0400 | 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
2025-06-08T05:14:39.094406-0400 | tls | 192.168.18.225:40794 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:39.048322-0400 | tls | 192.168.18.225:40778 | 192.168.18.213:443 | TCP | | TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:14:38.994430-0400 | tls | 192.168.18.225:40772 | 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

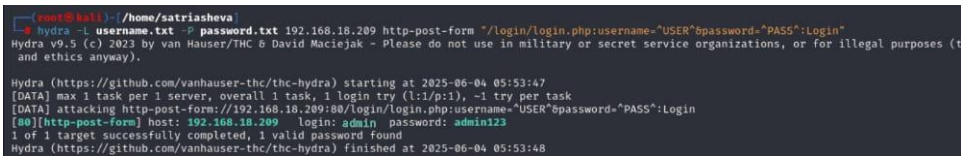
1. Brute force dilakukan untuk mencari username dan password user dilakukan dengan menggunakan dua tools yang berbeda, yaitu Hydra dan Medusa. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallD.
2. Membuat word list username bernama **username.txt** yang berisi list username yang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

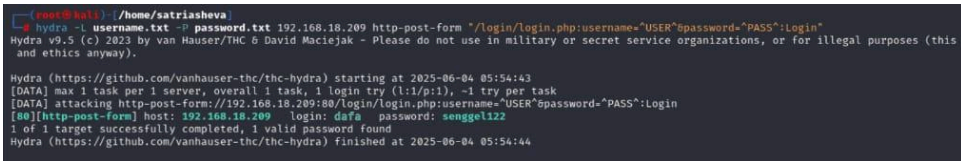


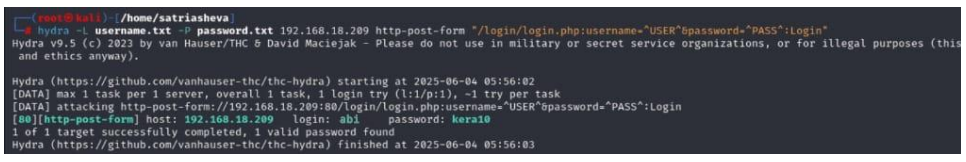
3. Membuat word list password bernama **password.txt** yang berisi list password yang akan dicoba.



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.



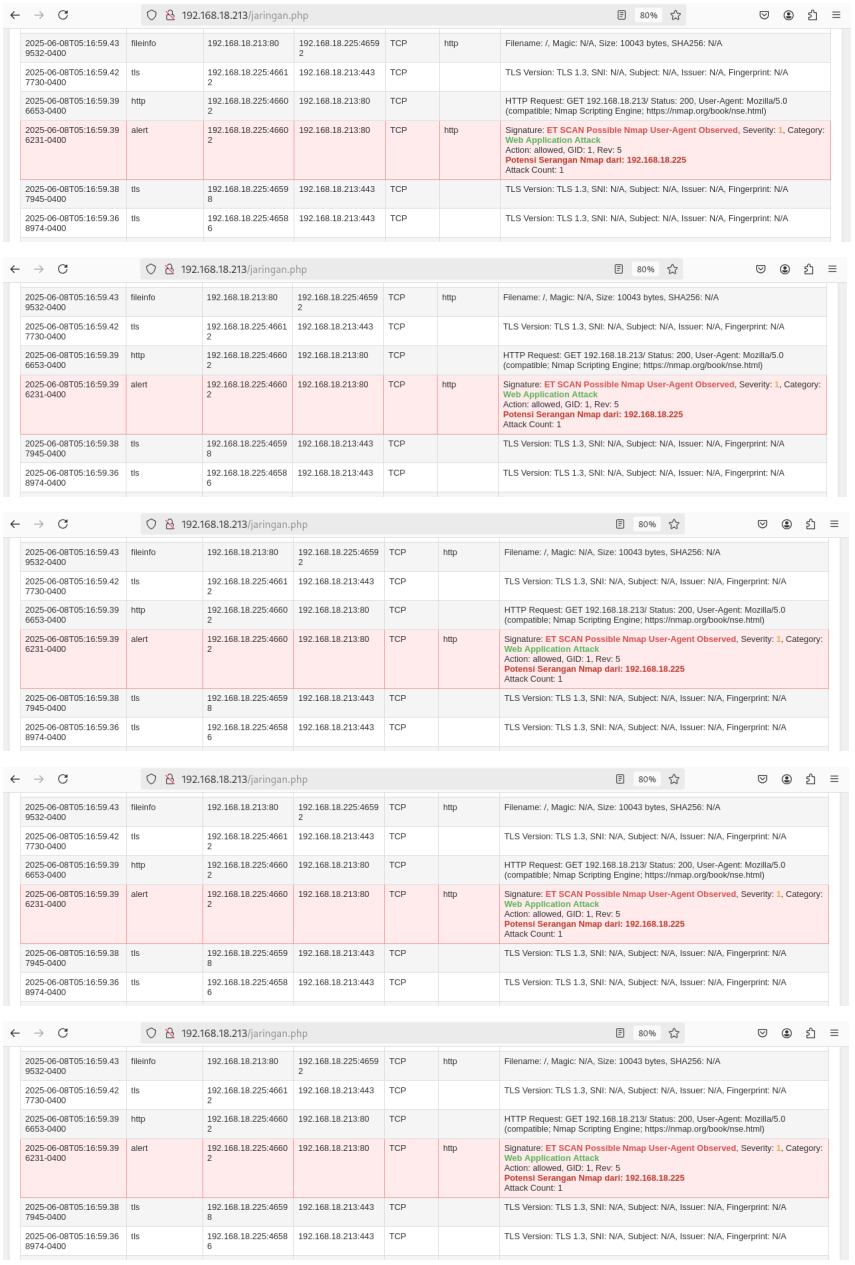




```
┌──(root㉿kali)-[/home/satriasheva]
└─# hydra -L username.txt -P password.txt 192.168.18.209 http-post-form "/login/login.php:username=^USER^&password=^PASS^:Login"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal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



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
```

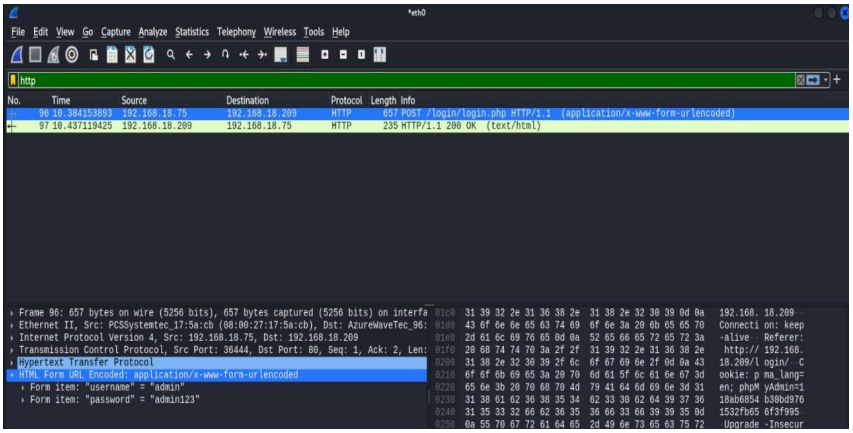
```
┌──(root㉿kali)-[/home/satriasheva]
└─# 2025-06-04 05:44:55 ACCOUNT CHECK: [http] Host: 192.168.18.209 (1 of 1, 0 complete) User: ameng (1 of 1
2025-06-04 05:44:55 ACCOUNT FOUND: [http] Host: 192.168.18.209 User: ameng Password: 123 [SUCCESS]

[1]  + done       medusa -h 192.168.18.209 -u admin -P password.txt -M http
```

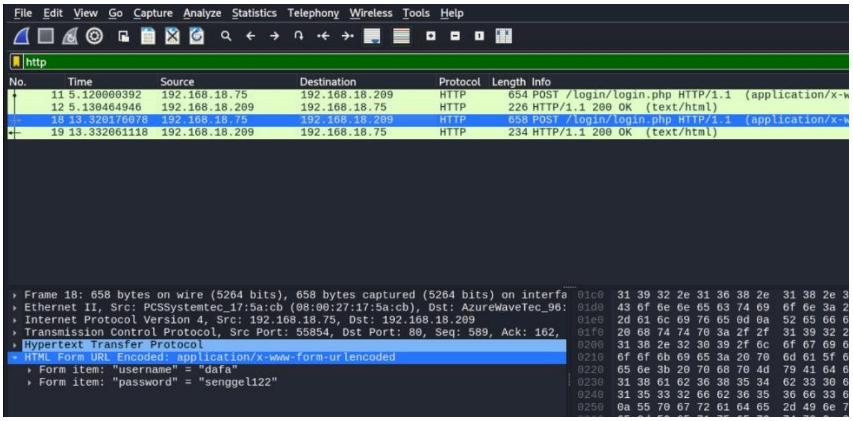
7. Selanjutnya, melihat tampilan log pada gui Suricata juga sama, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan brute force dengan medusa pada masing masing username.

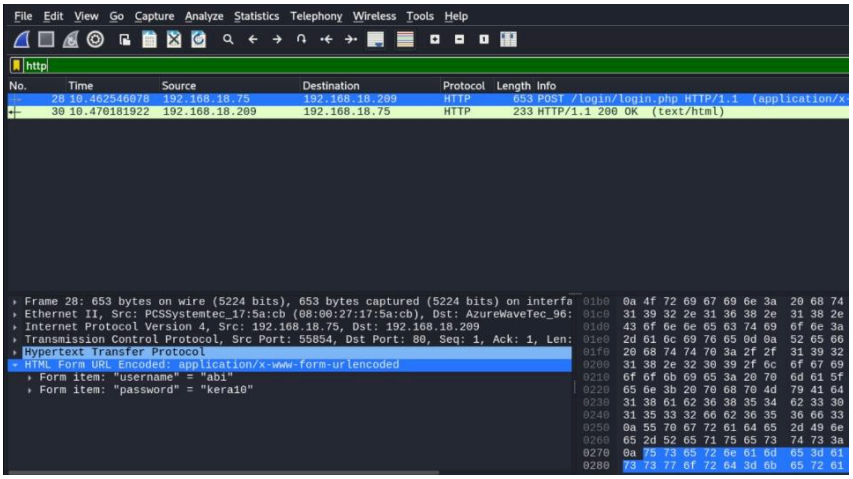
e. Sniffing

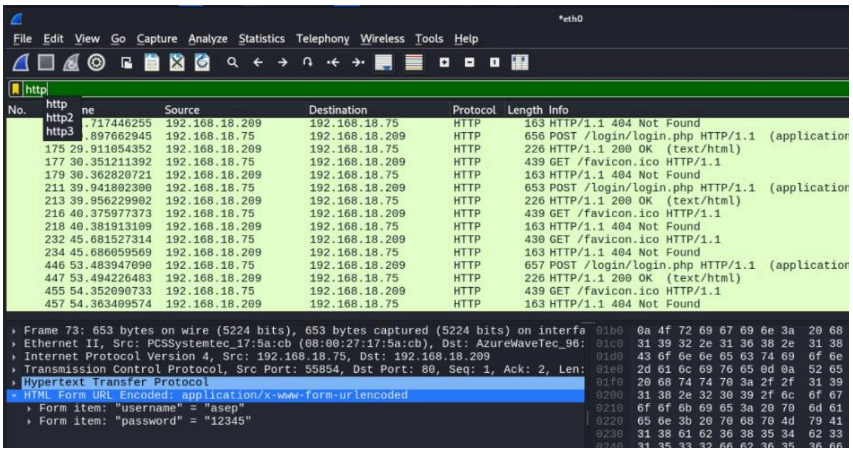
1. Sniffing dilakukan melalui dua tools yang berbeda, yaitu melalui wireshark dan tcpdump. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallD.

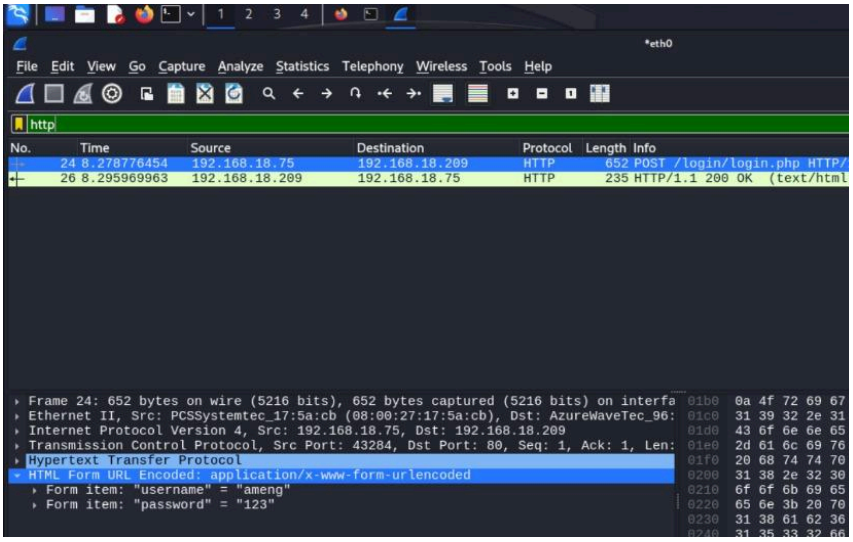
2. Sniffing melalui Wireshark yang dilakukan pada saat user login ke web server menunjukkan bahwa username dan password yang dikirimkan melalui metode **HTTP POST** untuk setiap username: admin, dafa, abi, asep, dan ameng**.**



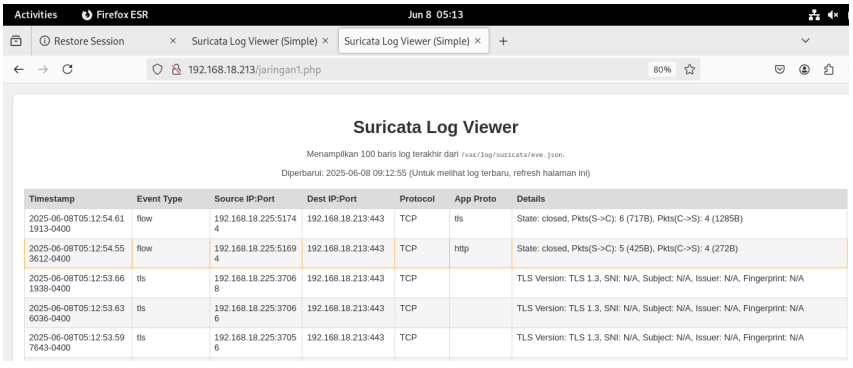


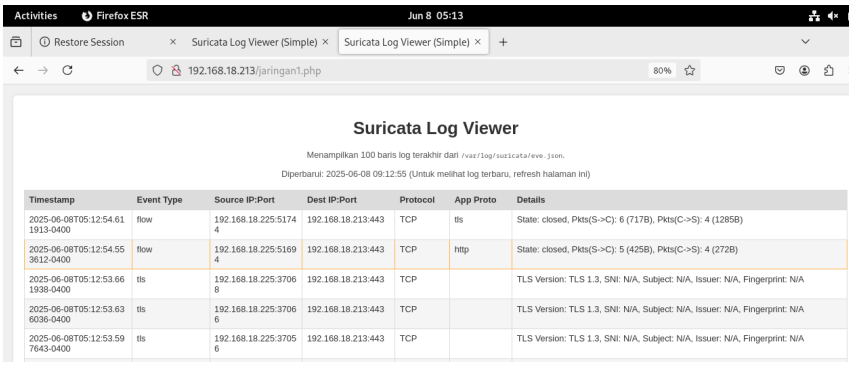


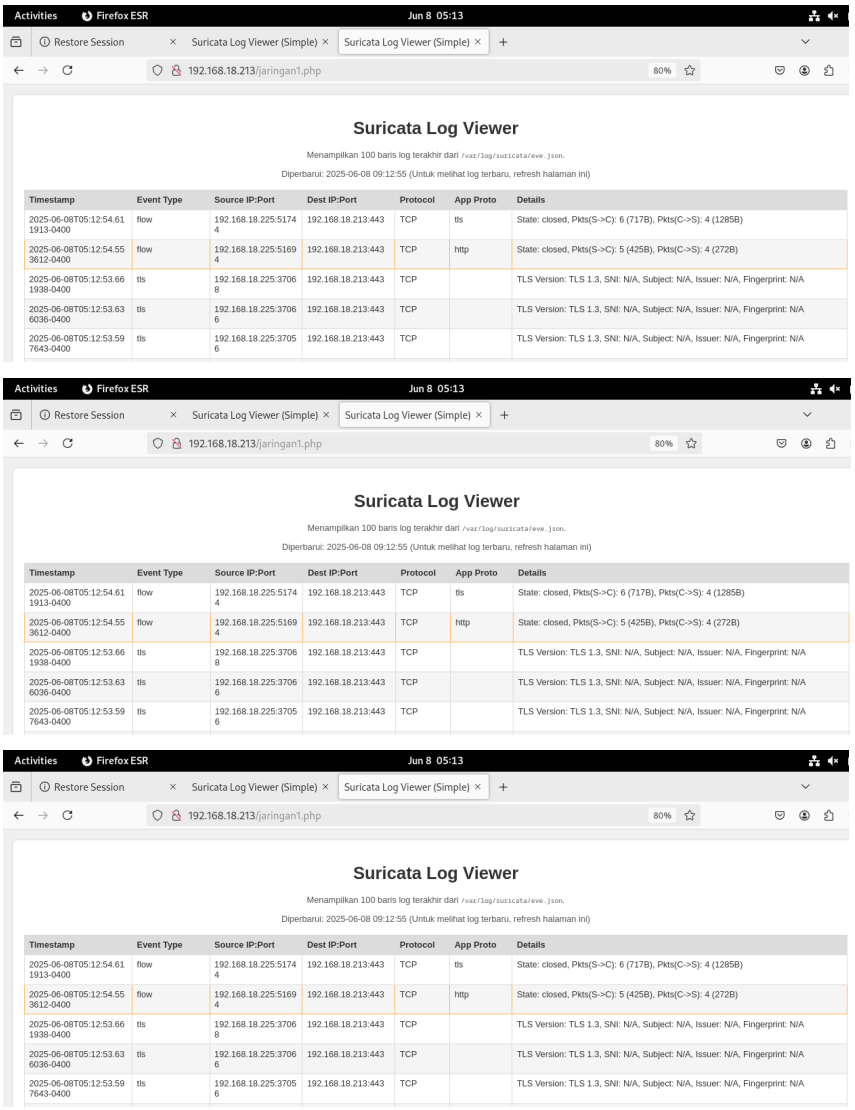




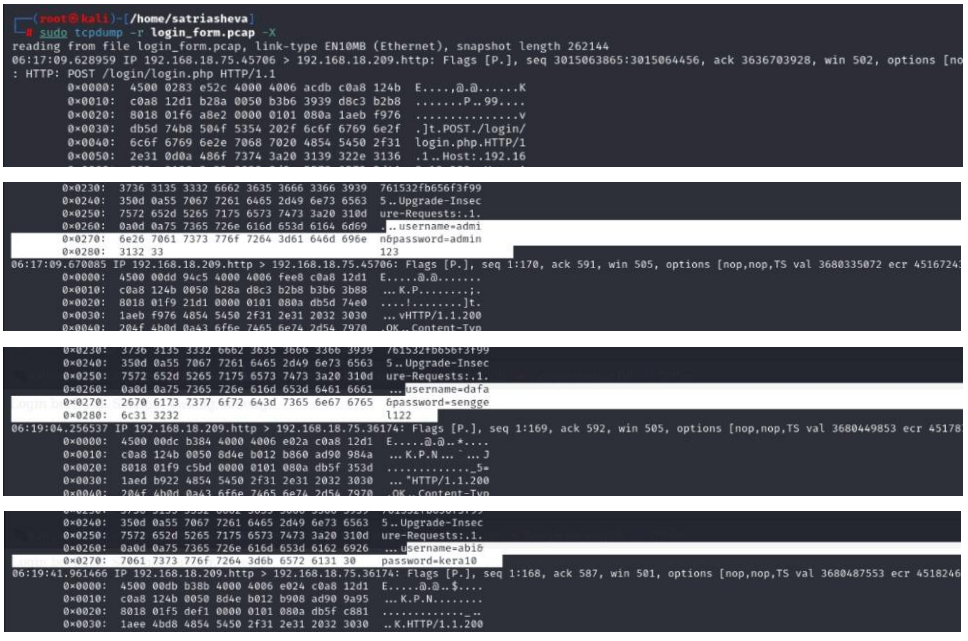
3. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan bahwa IP penyerang 192.168.18.225 tercatat tetapi tidak tercatat sebagai alert sehingga tidak berwarna orange pada saat dilakukan sniffing dengan Wireshark.

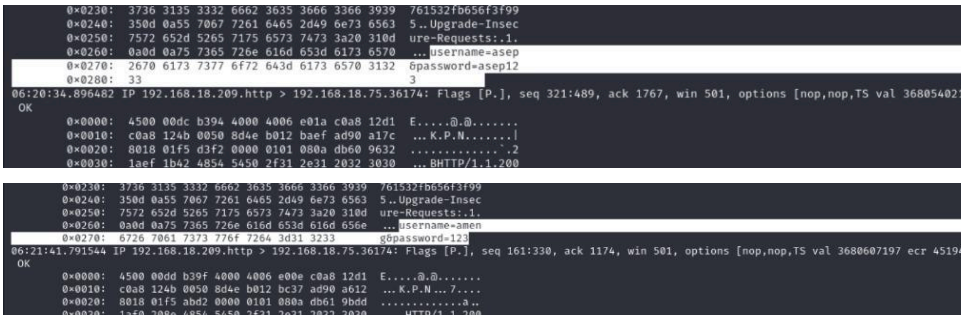



Activities Firefox ESR Jun 8 05:13
Restore Session Suricata Log Viewer (Simple) Suricata Log Viewer (Simple)
192.168.18.213/jaringan1.php
Suricata Log Viewer
Menampilkan 100 baris log terakhir dari /var/log/suricata/eve.json.
Diperbarui: 2025-06-08 09:12:55 (Untuk melihat log terbaru, refresh halaman ini)
Timestamp Event Type Source IP:Port Dest IP:Port Protocol App Proto Details
2025-06-08T05:12:54.611913-0400 flow 192.168.18.225:51744 192.168.18.213:443 TCP tls State: closed, Pkts(S->C): 6 (717B), Pkts(C->S): 4 (1285B)
2025-06-08T05:12:54.553612-0400 flow 192.168.18.225:51694 192.168.18.213:443 TCP http State: closed, Pkts(S->C): 5 (425B), Pkts(C->S): 4 (272B)
2025-06-08T05:12:53.661938-0400 tls 192.168.18.225:37068 192.168.18.213:443 TCP TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:12:53.636036-0400 tls 192.168.18.225:37066 192.168.18.213:443 TCP TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:12:53.597643-0400 tls 192.168.18.225:37056 192.168.18.213:443 TCP TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A

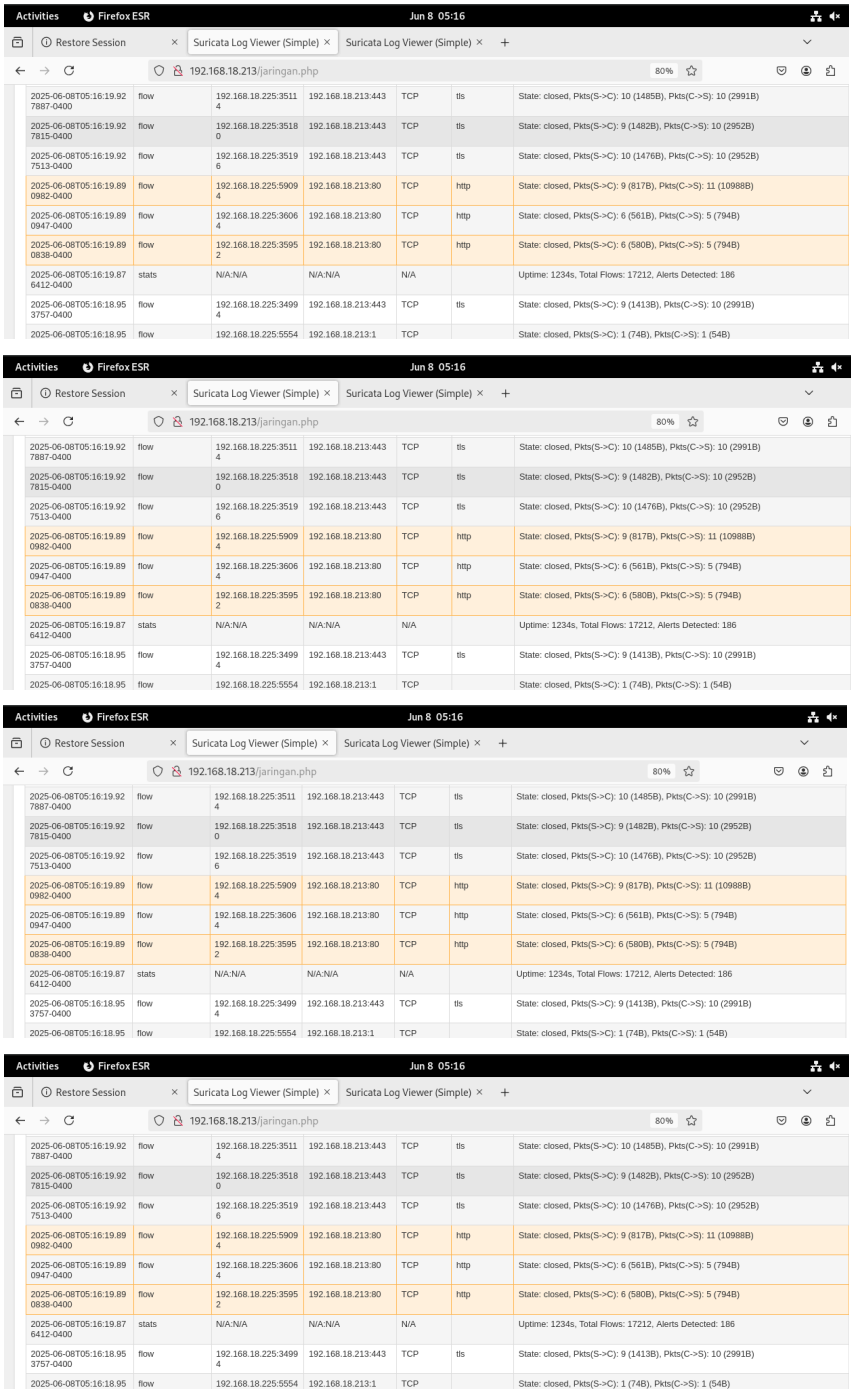


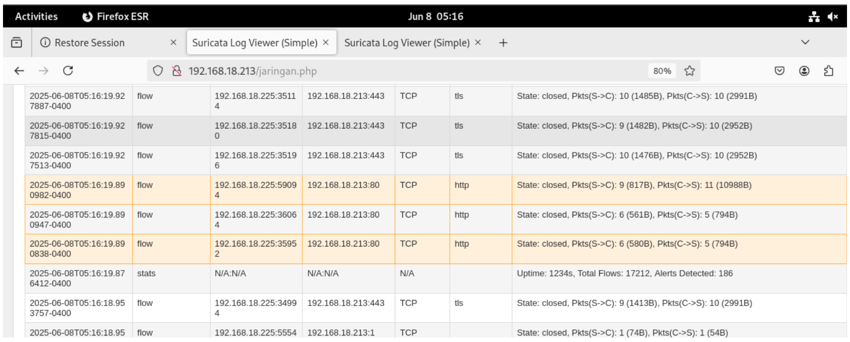
4. Selanjutnya sniffing melalui tcpdump yang dilakukan pada saat user login ke web server dengan perintah **sudo tcpdump -r login_form.pcap -X** untuk setiap username: admin, dafa, abi, asep, dan ameng.





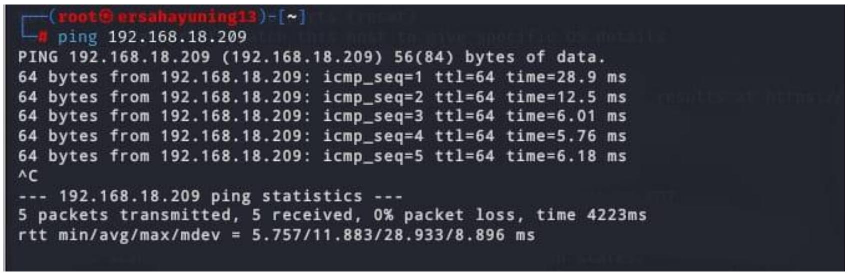
5. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan bahwa IP penyerang 192.168.18.225 tercatat tetapi tidak tercatat sebagai alert sehingga tidak berwarna orange pada saat dilakukan sniffing dengan tcpdump.

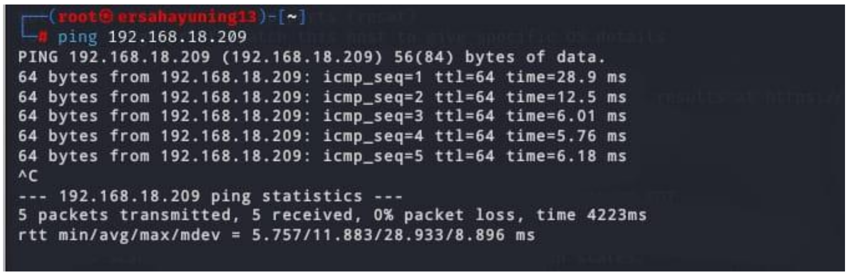


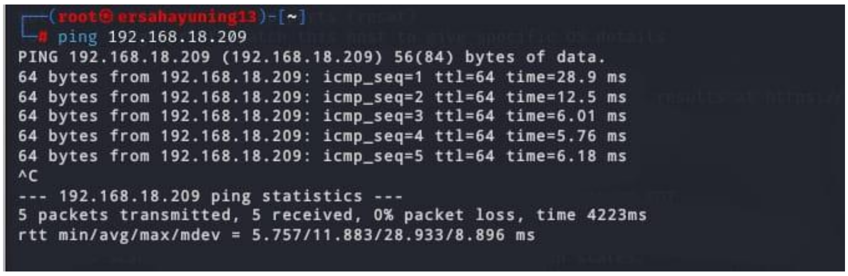


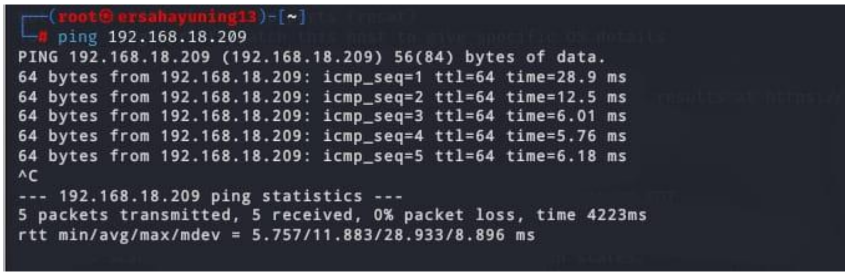
f. DDOS

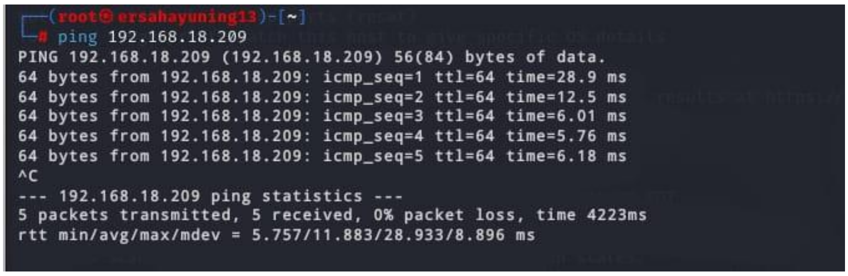
1. Melihat ping ke ip server terlebih dahulu sebelum dilakukan DDOS.

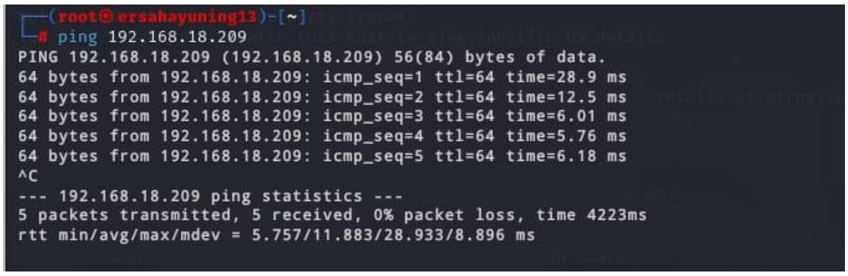




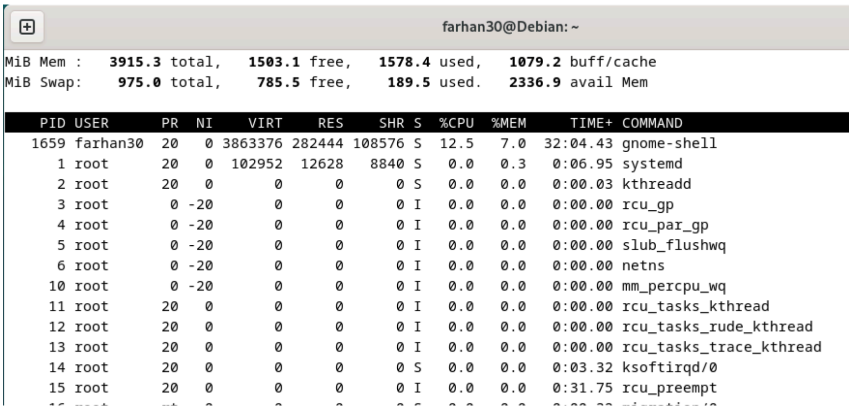


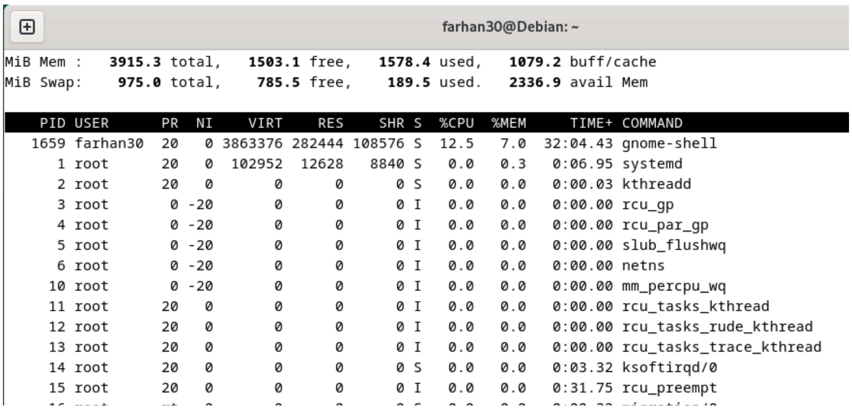


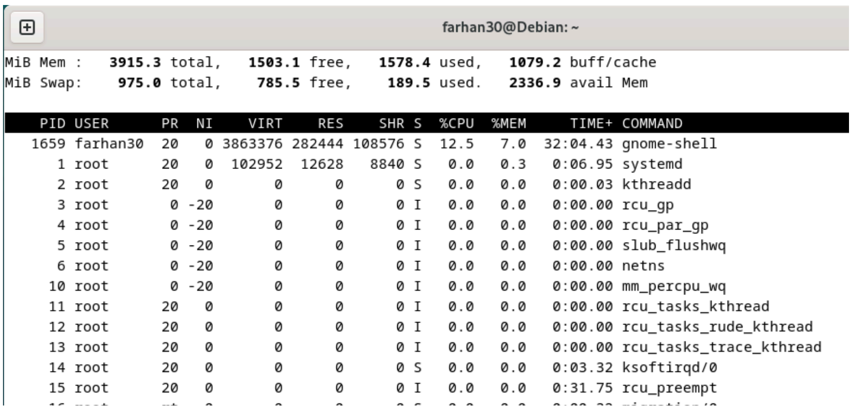


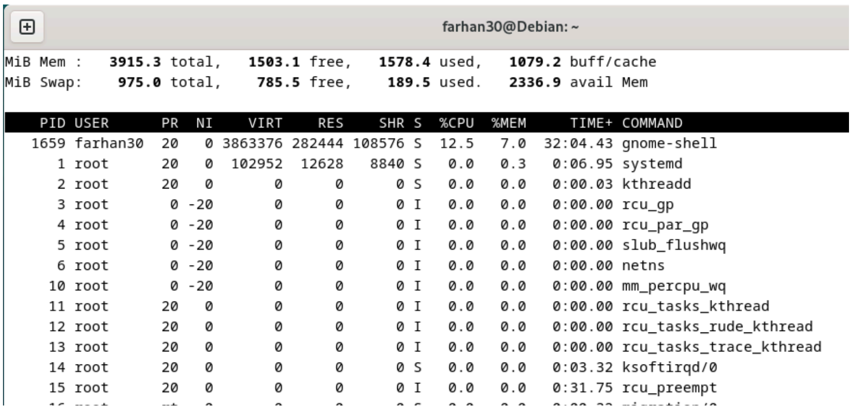


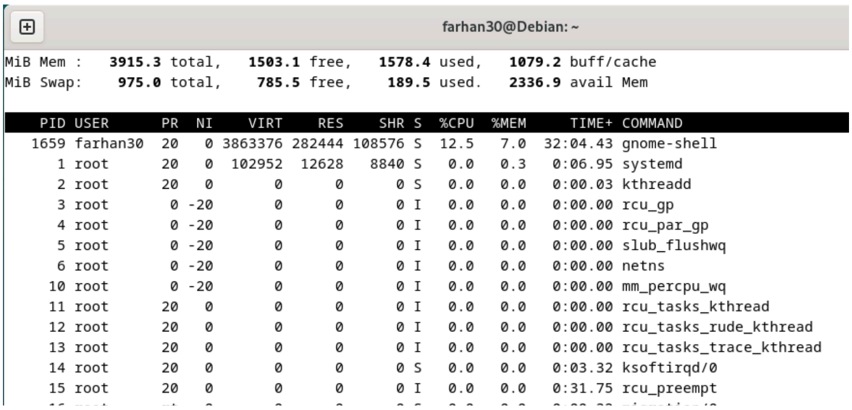
2. Cek kondisi CPU dengan perintah top untuk memantau.



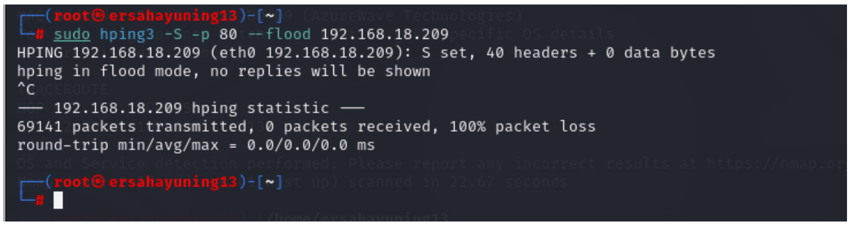


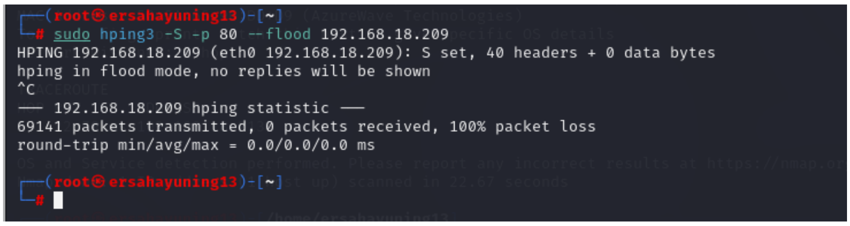


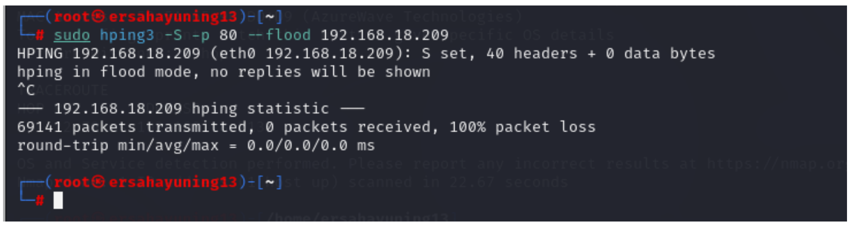


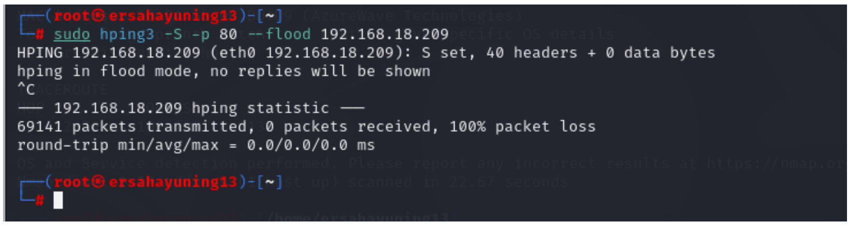


3. Melakukan DDOS dengan perintah **hping3 -S -p 80 --flood 192.168.18.209**

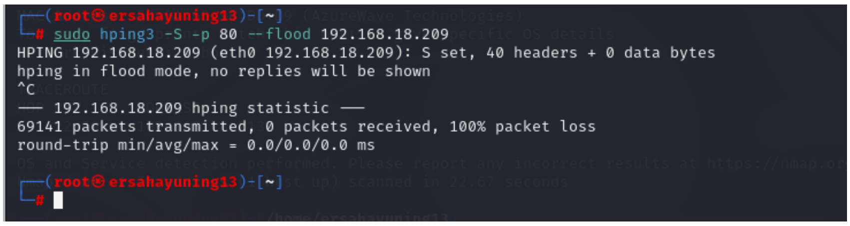






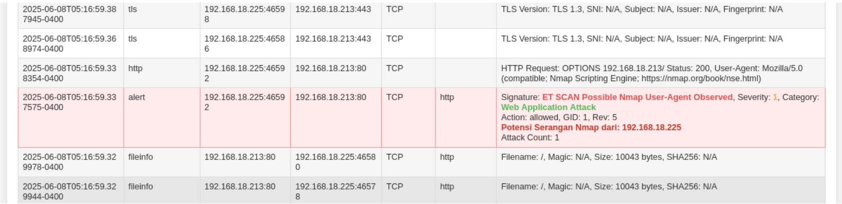


```
┌──(root㉿ersahayuning13)-[~]
└─# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.209 hping statistic ---
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿ersahayuning13)-[~]
└─# 
```

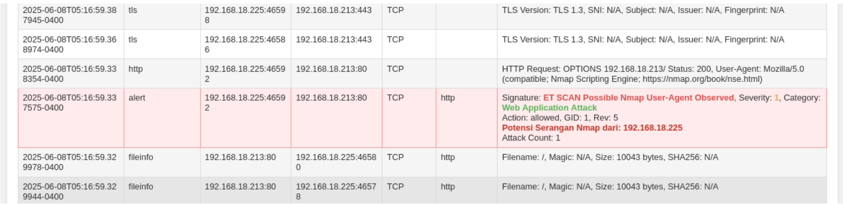


```
┌──(root㉿ersahayuning13)-[~]
└─# sudo hping3 -S -p 80 --flood 192.168.18.209
HPING 192.168.18.209 (eth0 192.168.18.209): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.209 hping statistic ---
69141 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿ersahayuning13)-[~]
└─# 
```

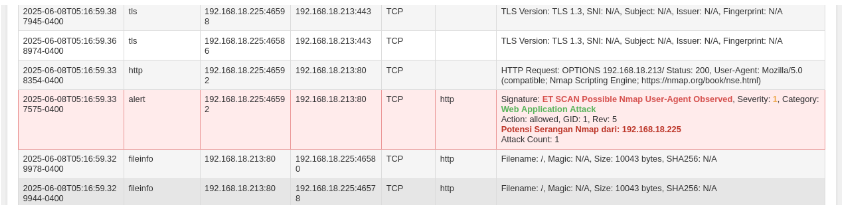
4. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan DDOS dengan hping3 karena request yang berlebihan.



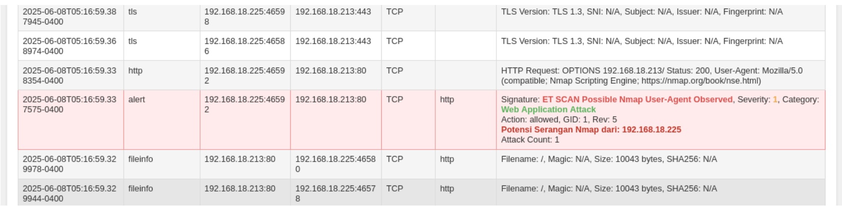
2025-06-08T05:16:59.387945-0400	tls	192.168.18.225:46598	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.368974-0400	tls	192.168.18.225:46586	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.338354-0400	http	192.168.18.225:46592	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)
2025-06-08T05:16:59.337575-0400	alert	192.168.18.225:46592	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
2025-06-08T05:16:59.329978-0400	fileinfo	192.168.18.213:80	192.168.18.225:46580	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.329944-0400	fileinfo	192.168.18.213:80	192.168.18.225:46578	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A



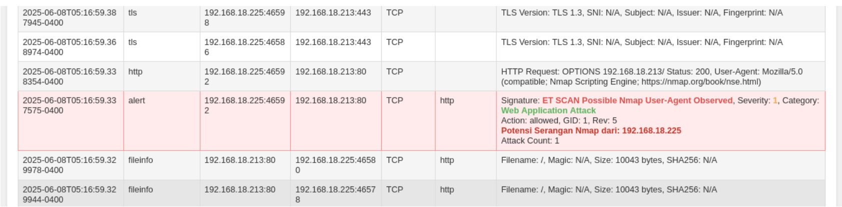
2025-06-08T05:16:59.387945-0400	tls	192.168.18.225:46598	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.368974-0400	tls	192.168.18.225:46586	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.338354-0400	http	192.168.18.225:46592	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)
2025-06-08T05:16:59.337575-0400	alert	192.168.18.225:46592	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
2025-06-08T05:16:59.329978-0400	fileinfo	192.168.18.213:80	192.168.18.225:46580	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.329944-0400	fileinfo	192.168.18.213:80	192.168.18.225:46578	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A



2025-06-08T05:16:59.387945-0400	tls	192.168.18.225:46598	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.368974-0400	tls	192.168.18.225:46586	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.338354-0400	http	192.168.18.225:46592	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)
2025-06-08T05:16:59.337575-0400	alert	192.168.18.225:46592	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
2025-06-08T05:16:59.329978-0400	fileinfo	192.168.18.213:80	192.168.18.225:46580	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.329944-0400	fileinfo	192.168.18.213:80	192.168.18.225:46578	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

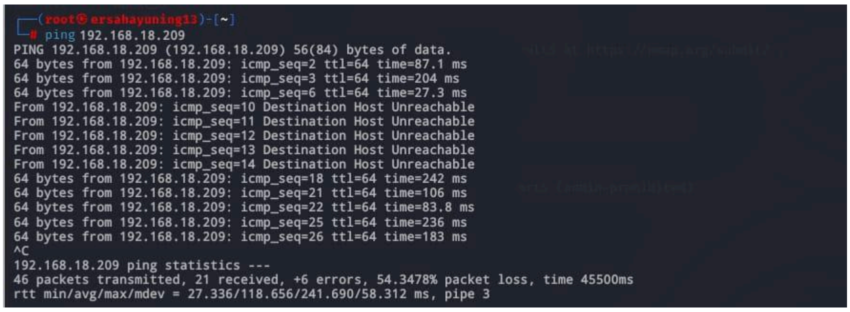


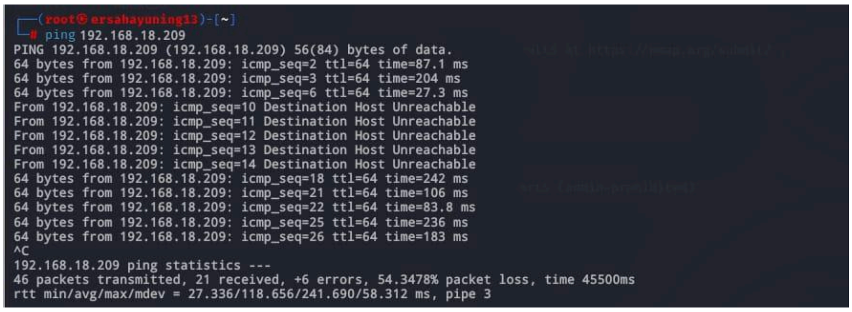
2025-06-08T05:16:59.387945-0400	tls	192.168.18.225:46598	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.368974-0400	tls	192.168.18.225:46586	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.338354-0400	http	192.168.18.225:46592	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)
2025-06-08T05:16:59.337575-0400	alert	192.168.18.225:46592	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
2025-06-08T05:16:59.329978-0400	fileinfo	192.168.18.213:80	192.168.18.225:46580	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.329944-0400	fileinfo	192.168.18.213:80	192.168.18.225:46578	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

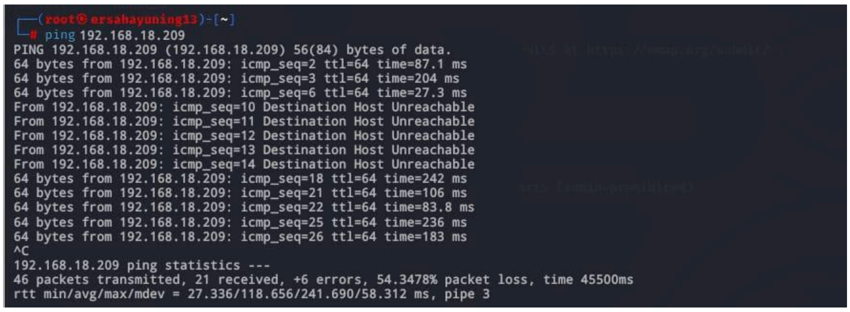


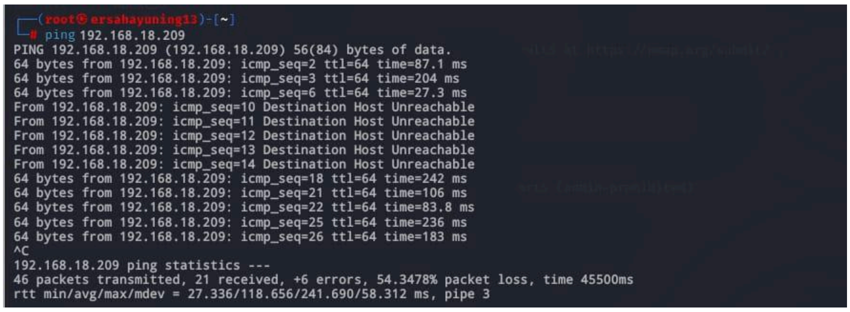
2025-06-08T05:16:59.387945-0400	tls	192.168.18.225:46598	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.368974-0400	tls	192.168.18.225:46586	192.168.18.213:443	TCP		TLS Version: TLS 1.3, SNI: N/A, Subject: N/A, Issuer: N/A, Fingerprint: N/A
2025-06-08T05:16:59.338354-0400	http	192.168.18.225:46592	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)
2025-06-08T05:16:59.337575-0400	alert	192.168.18.225:46592	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
2025-06-08T05:16:59.329978-0400	fileinfo	192.168.18.213:80	192.168.18.225:46580	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A
2025-06-08T05:16:59.329944-0400	fileinfo	192.168.18.213:80	192.168.18.225:46578	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

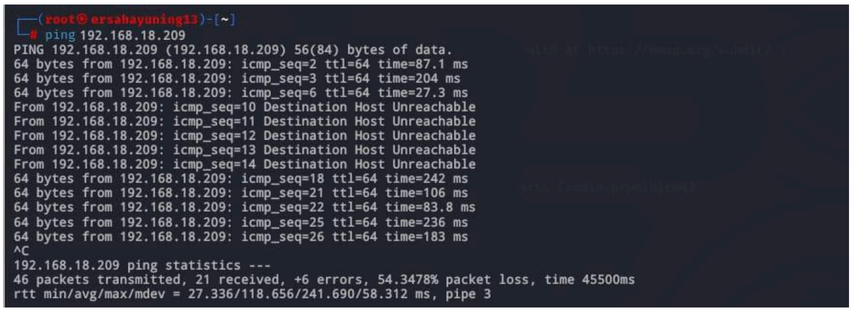
5. Hasil ping ketika dilakukan DDOS, respon time nya tidak ada perubahan signifikan.











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

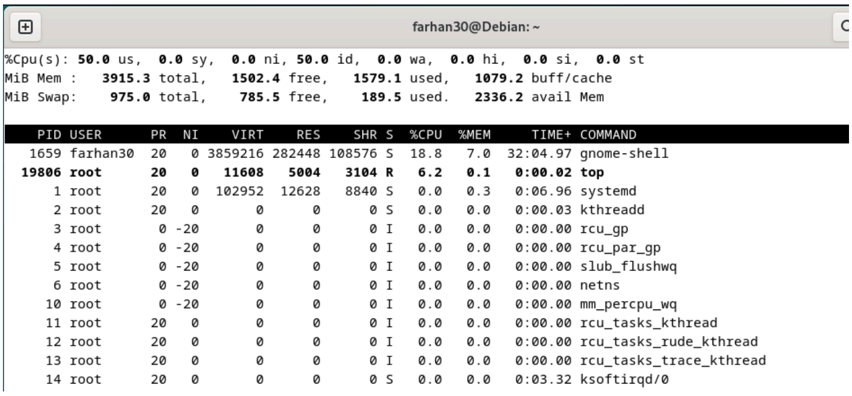
```
farhan30@Debian: ~
MiB Mem :   3915.3 total,   1503.1 free,   1578.4 used,   1079.2 buff/cache
MiB Swap:    975.0 total,    785.5 free,    189.5 used.   2336.9 avail Mem

    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
  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   0:03.32 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 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
```

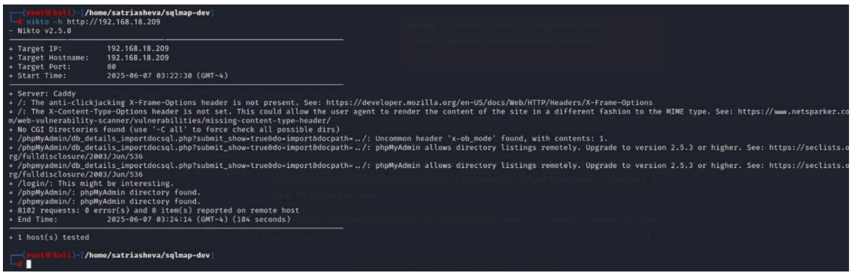


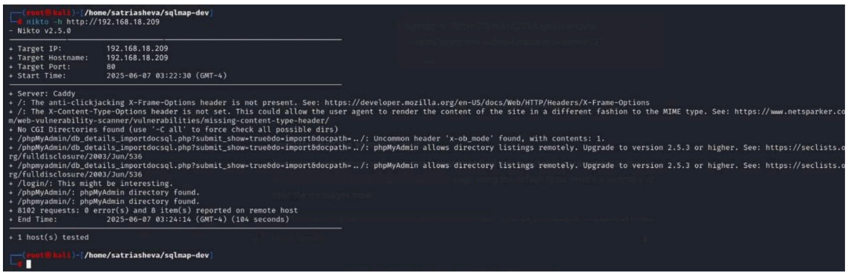
```
farhan30@Debian: ~
%Cpu(s): 50.0 us,  0.0 sy,  0.0 ni, 50.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3915.3 total,   1502.4 free,   1579.1 used,   1079.2 buff/cache
MiB Swap:    975.0 total,    785.5 free,    189.5 used.   2336.2 avail Mem

    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
  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   0:03.32 ksoftirqd/0
```

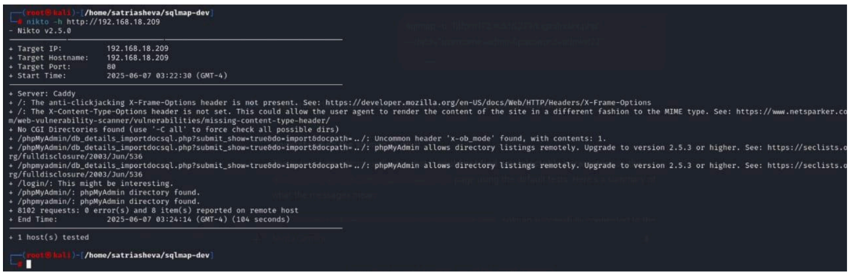


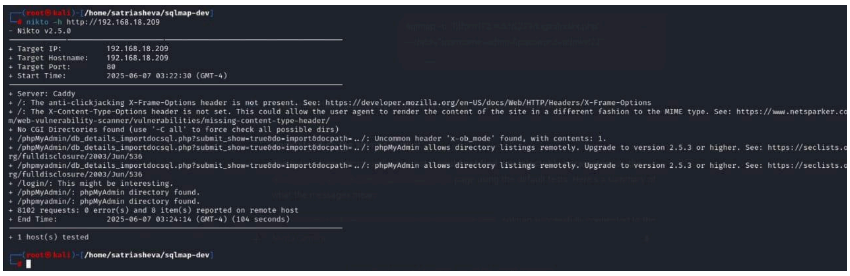
g. Web Scanning

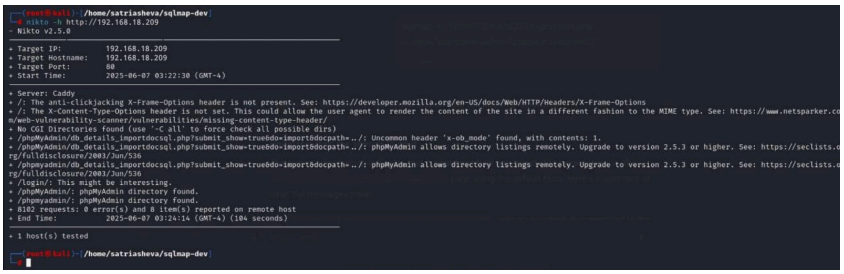
1. Penyerang melakukan web scanning pada Kali Linux terhadap aplikasi web dari server Debian, dengan menggunakan dua tools yang berbeda yaitu nikto dan dirb. Percobaan dilakukan setelah menambahkan rule untuk block pada FirewallD.
2. Web Scanning yang pertama dilakukan menggunakan tools nikto



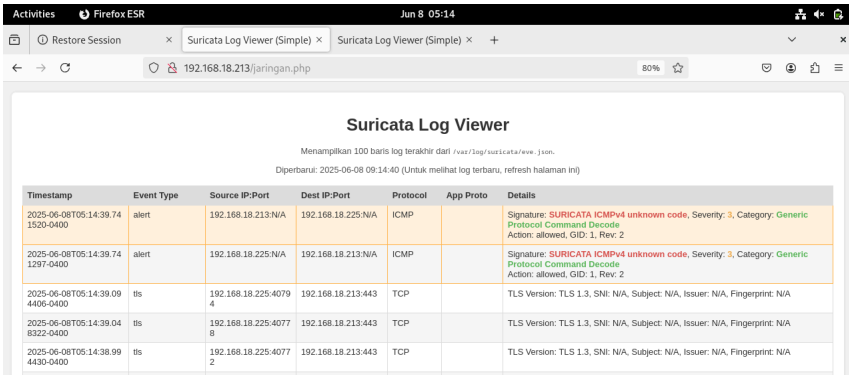


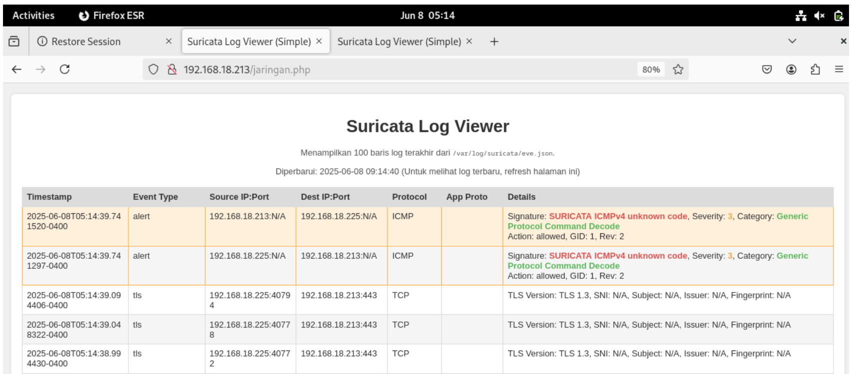




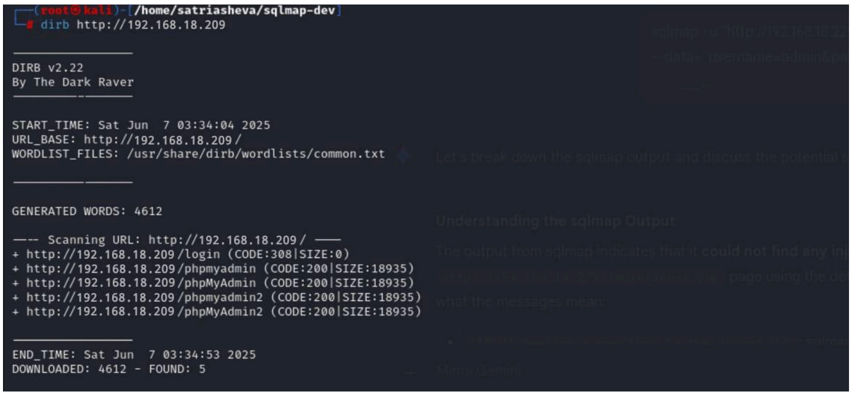


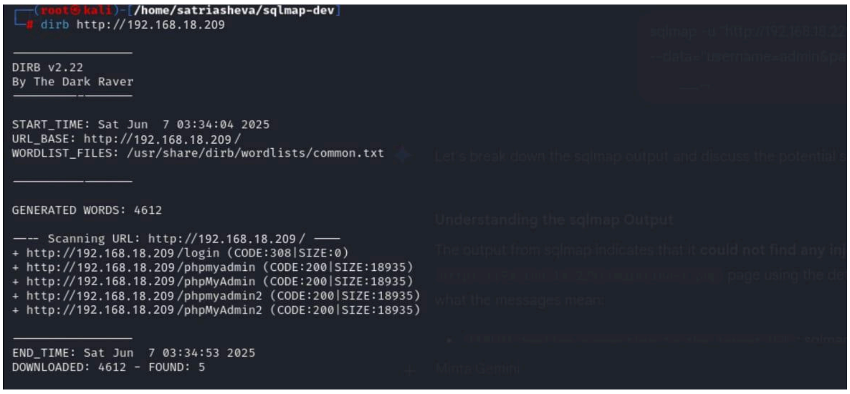
3. Selanjutnya, melihat tampilan log pada gui Suricata, menampilkan adanya alert berwarna orange pada IP penyerang 192.168.18.225 pada saat dilakukan web scanning yang berlebihan dengan tools Nikto.

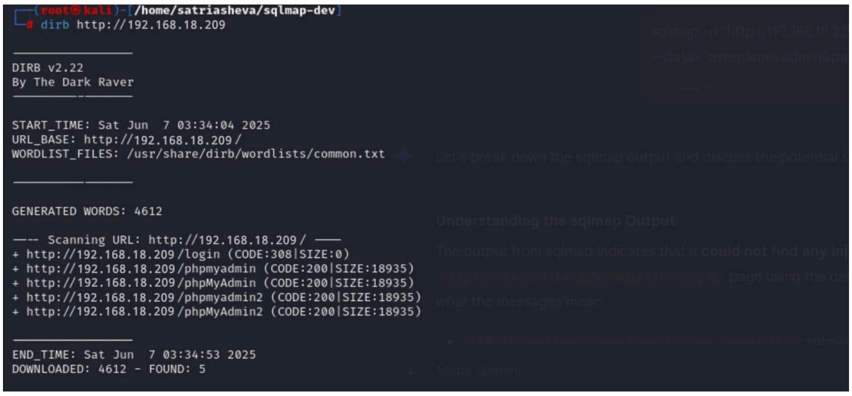




4. Web scanning yang kedua dilakukukan dengan tools Dirb.



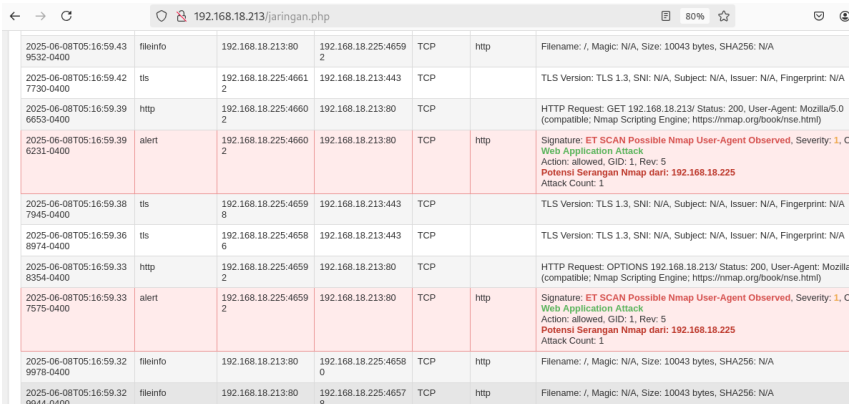




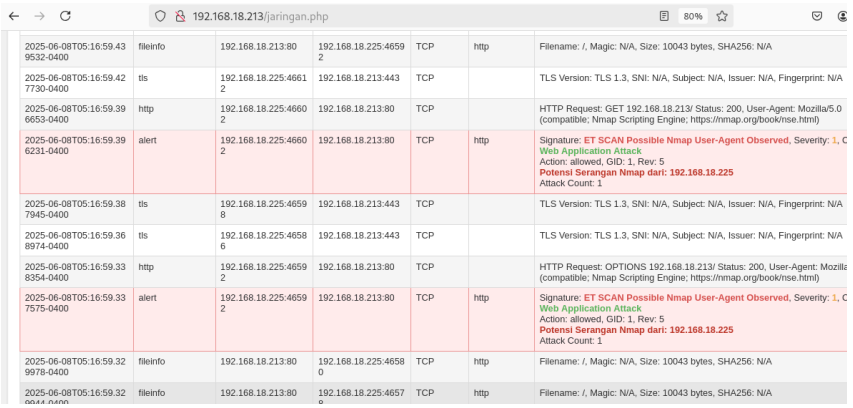
```
┌──(root㉿kali)-[/home/satriasheva/sqlmap-dev]
└─# dirb http://192.168.18.209

-----------------
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
```


```
┌──(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
```


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/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 (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	fileinfo	192.168.18.213:80	192.168.18.225:4657	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/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 (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	fileinfo	192.168.18.213:80	192.168.18.225:4657	TCP	http	Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

192.168.18.213/jaringan.php
80%
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
(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 fileinfo 192.168.18.213:80 192.168.18.225:4657 TCP http Filename: /, Magic: N/A, Size: 10043 bytes, SHA256: N/A

192.168.18.213/jaringan.php
80%
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
(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 fileinfo 192.168.18.213:80 192.168.18.225:4657 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 Honeypot 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