

# Laporan Praktikum Modul 2

## Ethical Hacking 2024

### Fortify Tech



Ahmad Fauzan Daniswara

5027221057

Date : 08 Mei 2024

Table of Content.....	1
Confidentially Statement.....	2
Contact Information.....	2
Assesment Overview.....	3
Assesment Components.....	3-4
Executive Summary.....	5
Langkah - langkah.....	5
-IP 10.15.42.36.....	5-9
-IP 10.15.42.7.....	10-16

## Confidentially Statement

Dokumen ini adalah milik eksklusif dari praktikan dan Fortify Tech. Dokumen ini berisi informasi hak milik dan rahasia. Duplikasi, redistribusi, atau penggunaan, seluruhnya atau sebagian, dalam bentuk apa pun, memerlukan izin dari praktikan dan Fortify Tech.

Praktikan dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan persyaratan uji penetrasi.

## Contact Information

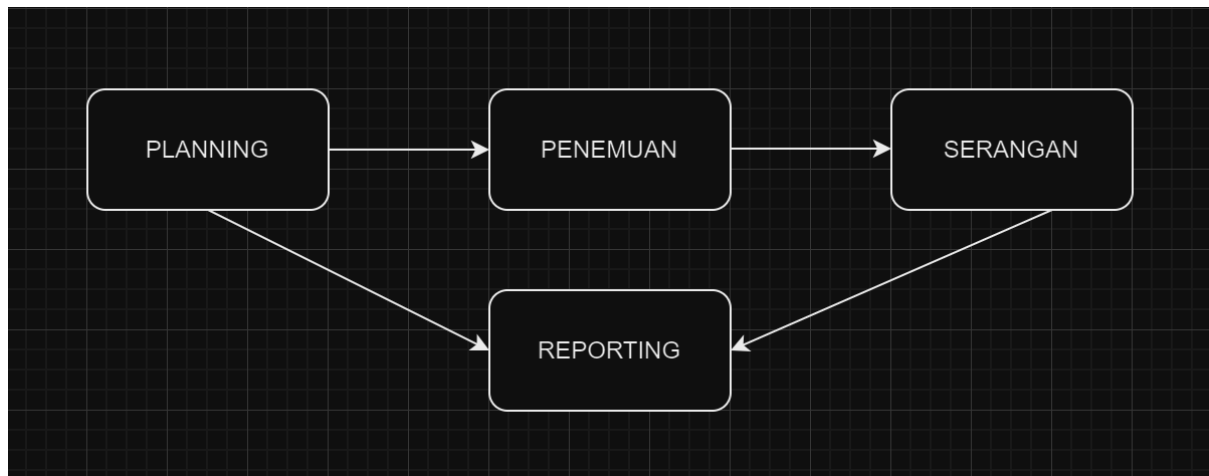
Nama	Judul	Information Contact
Praktikan		
Ahmad Fauzan Daniswara	Pentester	ahmaddaniswara2003@gmail.com
Fortify Tech		
Muhammad Azril Fathoni	General Manager Fortify Tech	

## Assesment Overview

Dari tanggal 4 Mei 2024 hingga 8 Mei 2024, praktikan diminta oleh FortifyTech untuk melakukan pentest pada infrastruktur perusahaan FortifyTech . Semua pengujian yang dilakukan didasarkan pada Panduan modul praktikum ethical hacking ke 4-6 untuk melakukan pentesting.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

- Perencanaan/Planning – Menyiapkan tools untuk melakukan pentesting pada IP address Fortify Tech.
- Penemuan – Lakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Serangan – Konfirmasikan potensi kerentanan melalui eksploitasi dan lakukan penemuan tambahan pada akses baru.
- Pelaporan/Reporting – Dokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



## Assesment Component

- Scope

Scope yang akan digunakan adalah :

10.15.42.36

10.15.42.7

-Pengecualian :

Hindari hal - hal yang melanggar etika atau Anda akan dimarahi (~~diberi nilai 0~~) oleh Project Manager 😊.

## Executive Summary

Berikut adalah dua IP Address yang digunakan untuk melakukan pentesting :

-10.15.42.36

-10.15.42.7

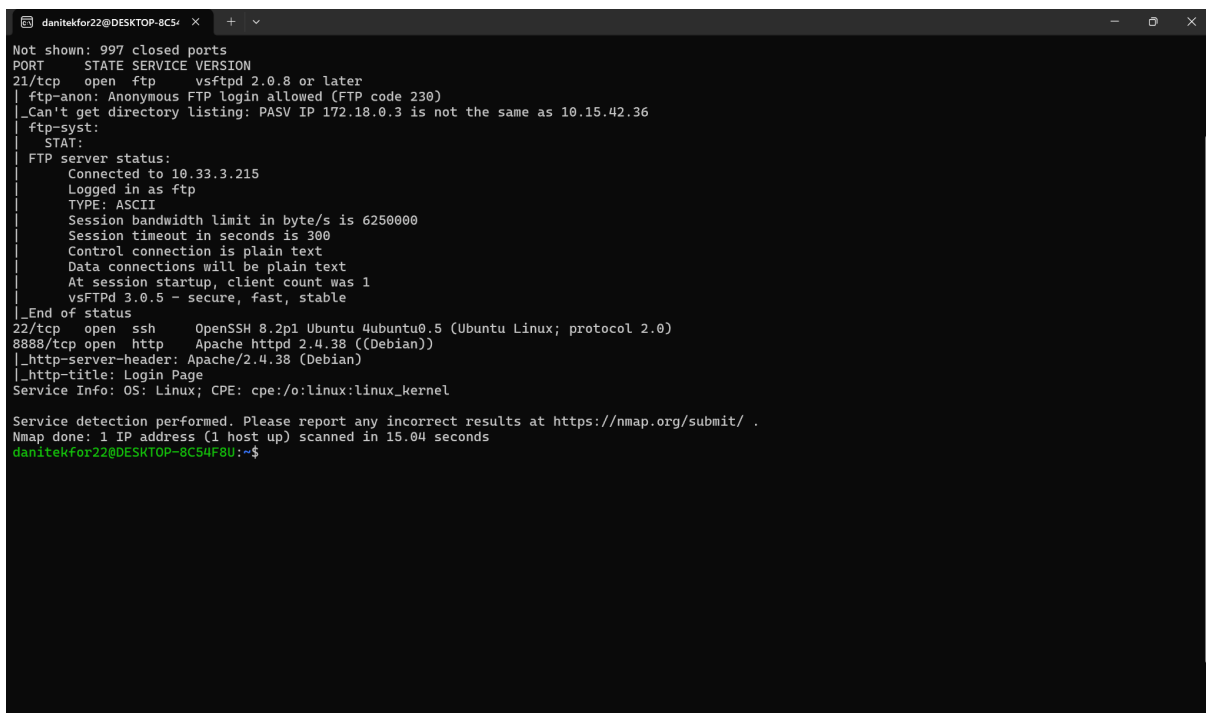
Percobaan untuk pentesting dimulai dari tanggal 5 Mei hingga 8 Mei 2024 pada dua IP Address diatas. Namun, hasil akhir pentesting masih belum ditemukan. Tetapi terdapat informasi yang bisa didapatkan dari dua IP Address diatas.

## Langkah - langkah

1.IP 10.15.42.36

Langkah-langkah :

-Melakukan reconnaissance pada IP 10.15.42.36 menggunakan nmap



```
danitekfor22@DESKTOP-8C54F8U: ~  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.0.8 or later  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36  
| ftp-syst:  
|   STAT:  
|   FTP server status:  
|     Connected to 10.33.3.215  
|     Logged in as ftp  
|     TYPE: ASCII  
|     Session bandwidth limit in byte/s is 6250000  
|     Session timeout in seconds is 300  
|     Control connection is plain text  
|     Data connections will be plain text  
|     At session startup, client count was 1  
|     vsFTPd 3.0.5 - secure, fast, stable  
|_ End of status  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)  
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))  
|_ http-server-header: Apache/2.4.38 (Debian)  
|_ http-title: Login Page  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.04 seconds  
danitekfor22@DESKTOP-8C54F8U:~$
```

Berikut adalah hasil analisis dari proses nmapping ip 10.15.42.36 =

1. Port 21 (FTP) =

- Status : Terbuka
- Service : FTP
- Informasi Tambahan: FTP anonim diizinkan (FTP code 230), tetapi gagal mendapatkan daftar direktori karena alamat PASV yang diberikan tidak sesuai dengan alamat yang dipindai.

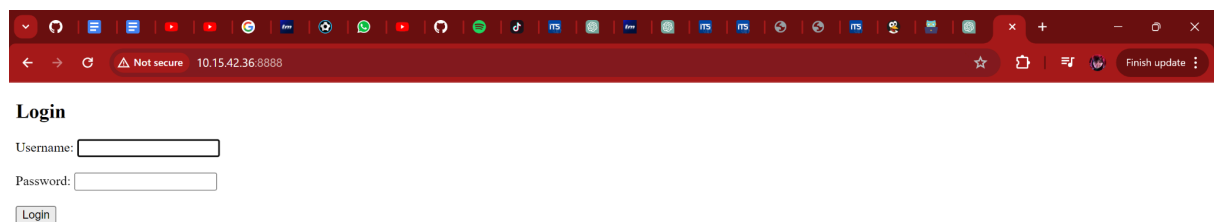
2. Port 22 (SSH) =

- Status: Terbuka
- Service: SSH (OpenSSH 8.2p1 Ubuntu 4ubuntu0.5).

3. Port 8888 (HTTP)

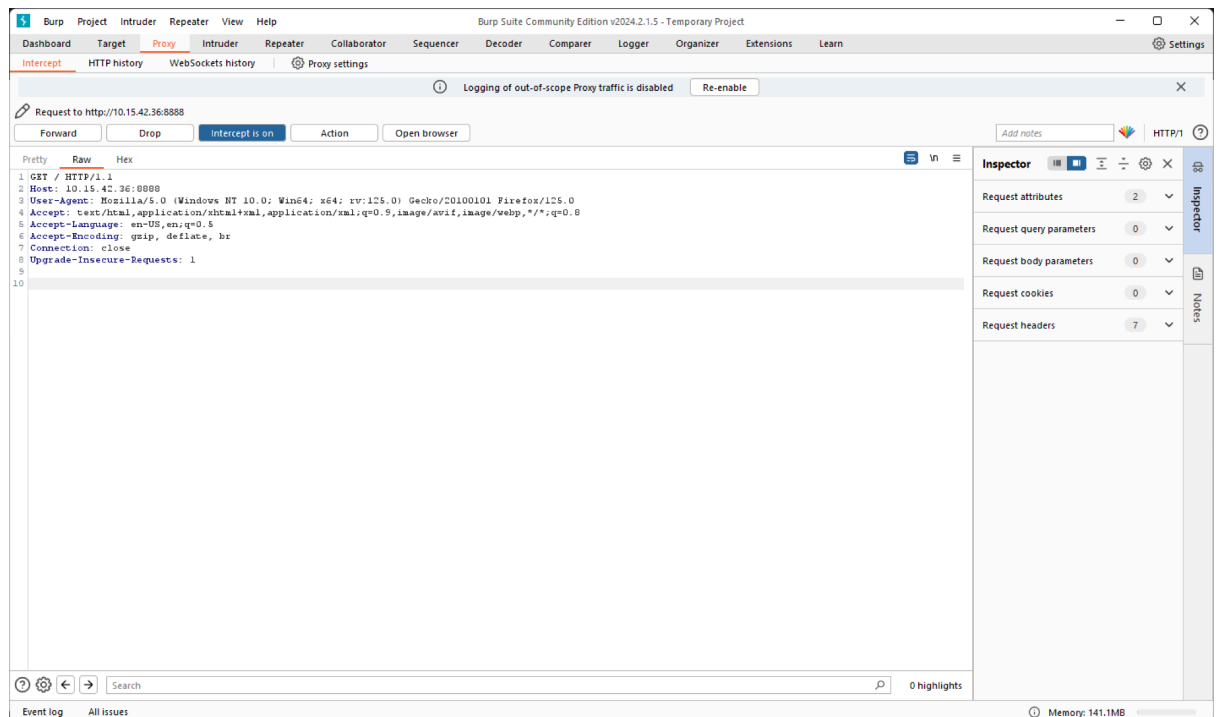
- Status : Terbuka
- Service: HTTP (Apache httpd 2.4.38).
- Informasi Tambahan: Server menjawab dengan header `Apache/2.4.38 (Debian)` dan halaman judul "Login Page".

- Lalu masuk ke login page dengan cara ketik <http://10.15.42.36:8888>

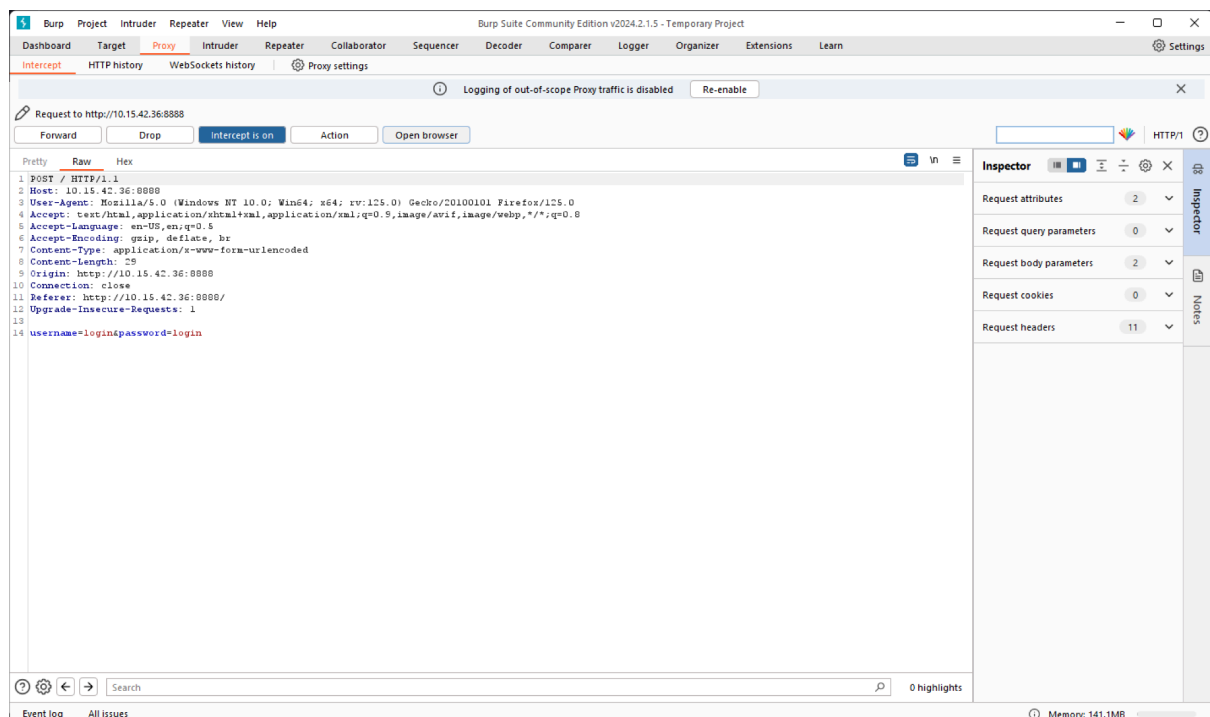


---

- Setelah itu masuk ke burpsuite community edition untuk coba intercept pada login page diatas

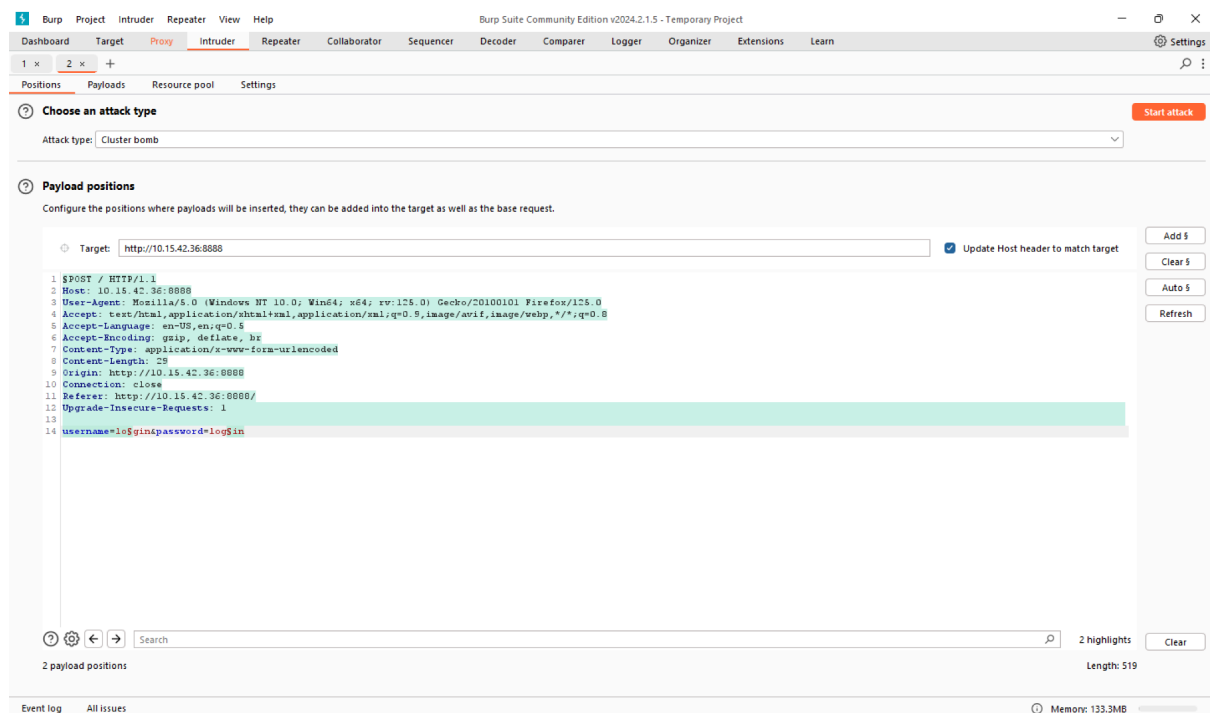


- Kemudian, mencoba login dengan username dan password berupa login dan hasilnya jadi sebagai berikut



- Setelah itu pindah ke intruder untuk mencoba lakukan serangan dengan tujuan mengetahui password dari login page 10.15.42.36:8888





- Kemudian, serangan dilakukan dengan mencoba metode cluster bomb namun terdapat kendala. Lalu, ketika mencoba metode sniper juga menemui kendala dan masih belum terselesaikan.

1 x 2 x 3 x +

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Cluster bomb

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.15.42.36:8080

Update Host header to match target

Intruder Attack Configuration

Errors

- Payload set 1: Preset payload list is empty.
- Payload set 2 has not been defined.

Ignore Go back

2 payload positions

Length: 519

Event log All issues

Memory: 143.1MB

1 x 2 x 3 x +

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.15.42.36:8080

Update Host header to match target

Intruder Attack Configuration

Errors

- Payload set 1: Preset payload list is empty.

Ignore Go back

2 payload positions

Length: 519

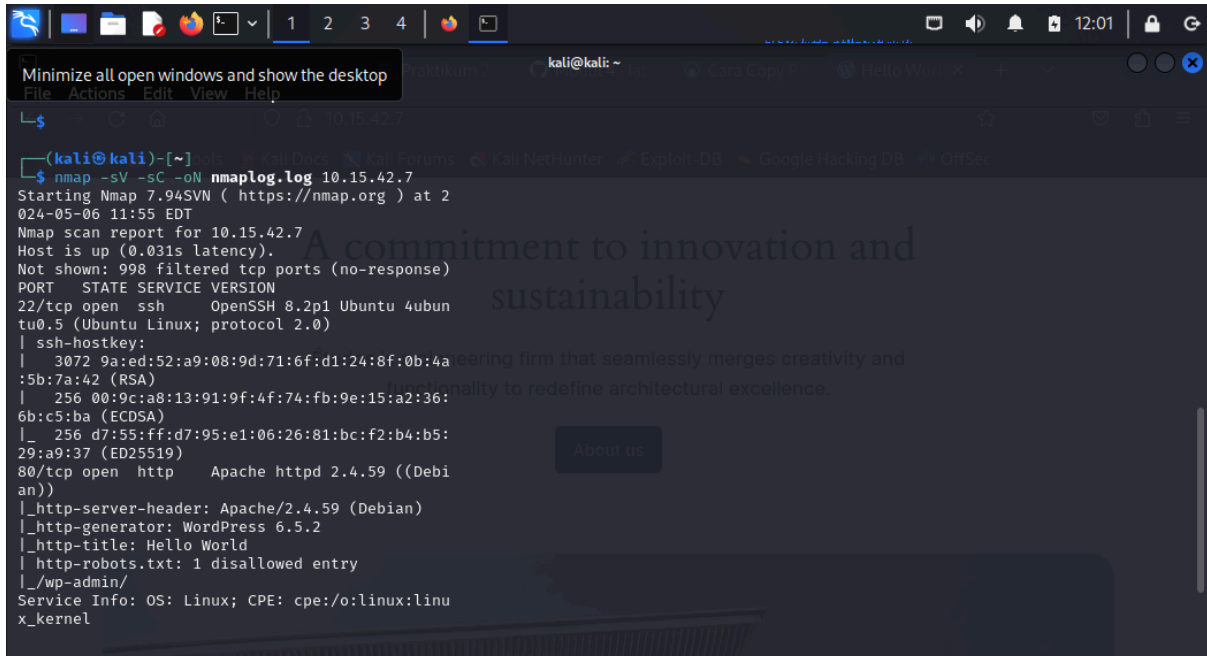
Event log All issues

Memory: 143.1MB

## 2. IP 10.15.42.7

Langkah-langkah =

1. Scan memakai nmap pada IP Addressnya =



```
(kali@kali)-[~]
└─$ nmap -sV -sC -oN nmaplog.log 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 11:55 EDT
Nmap scan report for 10.15.42.7
Host is up (0.031s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|_  256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_  256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp    open  http      Apache httpd 2.4.59 ((Debian))
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-generator: WordPress 6.5.2
|_ http-title: Hello World
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Berikut adalah sesuatu yang didapatkan dari informasi diatas =

1. Port SSH/22 :

Versi OpenSSH = 8.2p1 ubuntu 4ubuntu0.5

Sistem Operasi = Ubuntu Linux

Protokol = 2.0

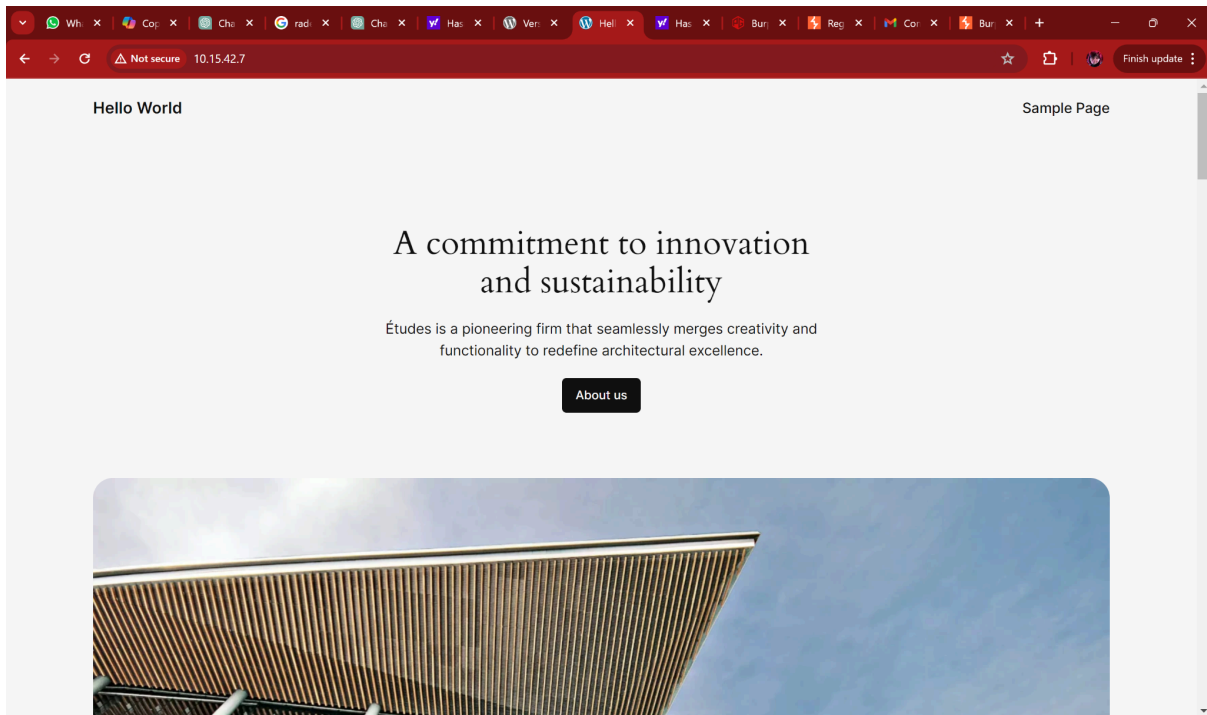
2. Port HTTP/80 :

Server = Apache httpd 2.4.59

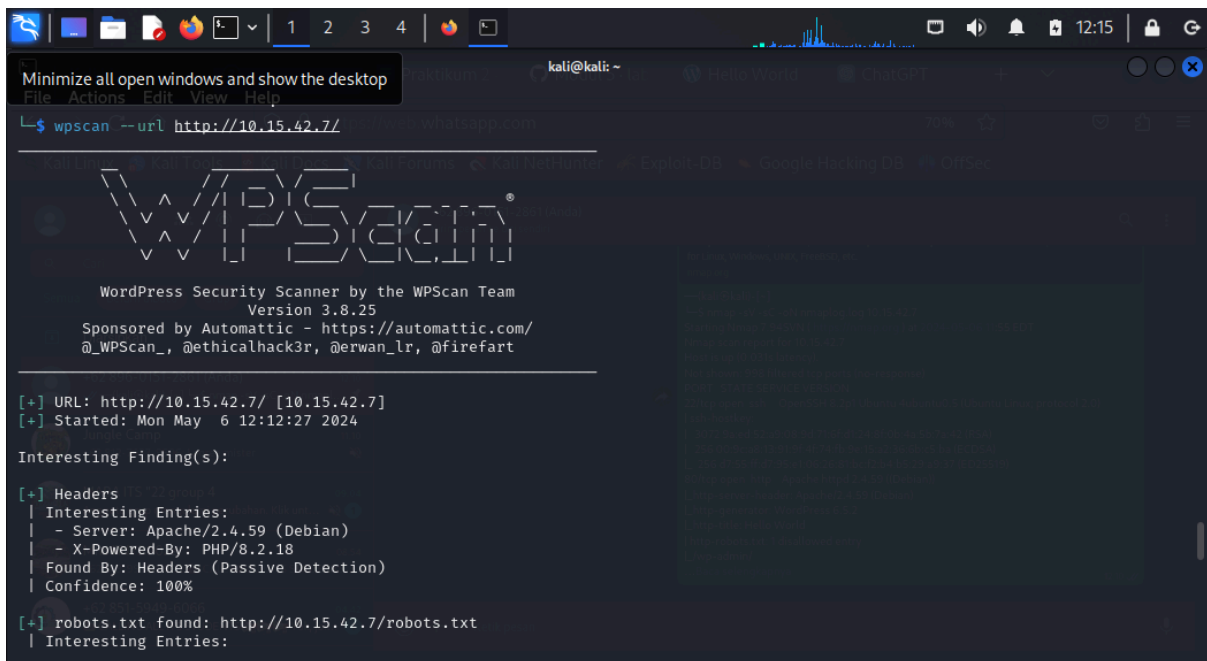
Wordpress Version = 6.5.2

Web content = Hello World and robots.txt file

2. Kemudian, saya masuk ke web tersebut =



3. Kemudian, coba pindai web tersebut pada wpscan =



Berikut adalah versi lengkapnya =

—(kaliⓈkali)-[~]

└─\$ wpscan --url http://10.15.42.7/

---

— — —

\\ // \_\ / \_|

\\ ^ / | | | ( \_ \_ \_ \_ \_ ®

\\ V / | \_ / \ \_ \ / \_ / \_ ' | '\

\ ^ / | | \_ | ( ( | | | |

V V || \_ / \ \_ \ , || ||

WordPress Security Scanner by the WPScan Team

Version 3.8.25

Sponsored by Automattic - <https://automattic.com/>

@WPScan, @ethicalhack3r, @erwan\_lr, @firefart

---

[+] URL: http://10.15.42.7/ [10.15.42.7]

[+] Started: Mon May 6 12:12:27 2024

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.59 (Debian)

| - X-Powered-By: PHP/8.2.18  
| Found By: Headers (Passive Detection)  
| Confidence: 100%

[+] robots.txt found: <http://10.15.42.7/robots.txt>

| Interesting Entries:  
| - /wp-admin/  
| - /wp-admin/admin-ajax.php  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%

[+] XML-RPC seems to be enabled: <http://10.15.42.7/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/)  
| - [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos/](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/)

[+] WordPress readme found: <http://10.15.42.7/readme.html>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: <http://10.15.42.7/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - <https://www.iplocation.net/defend-wordpress-from-ddos>

| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).

| Found By: Rss Generator (Passive Detection)

| - <http://10.15.42.7/feed/>, <generator><https://wordpress.org/?v=6.5.2></generator>

| - <http://10.15.42.7/comments/feed/>,  
<generator><https://wordpress.org/?v=6.5.2></generator>

[+] WordPress theme in use: twentytwentyfour

| Location: <http://10.15.42.7/wp-content/themes/twentytwentyfour/>

| Latest Version: 1.1 (up to date)

| Last Updated: 2024-04-02T00:00:00.000Z

| Readme: <http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt>

| Style URL: <http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css>

| Style Name: Twenty Twenty-Four

| Style URI: <https://wordpress.org/themes/twentytwentyfour/>

| Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...

| Author: the WordPress team

| Author URI: <https://wordpress.org>

|

| Found By: Urls In Homepage (Passive Detection)

| Confirmed By: Urls In 404 Page (Passive Detection)

|

| Version: 1.1 (80% confidence)

| Found By: Style (Passive Detection)

| - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:00

<=====> (137 / 137) 100.00%

Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at  
<https://wpscan.com/register>

[+] Finished: Mon May 6 12:12:34 2024

[+] Requests Done: 170

[+] Cached Requests: 7

[+] Data Sent: 41.821 KB



[+] Data Received: 439.594 KB

[+] Memory used: 252.492 MB

[+] Elapsed time: 00:00:07

Dari info diatas, berikut adalah hal yang bisa ditemukan =

1. XML-RPC Aktif: XML-RPC adalah protokol yang memungkinkan akses ke situs WordPress melalui API. Meskipun berguna, ini juga dapat menjadi titik masuk bagi serangan brute-force dan DDoS. Pertimbangkan untuk mematikan XML-RPC jika tidak diperlukan.
2. WP-Cron Aktif dengan Tingkat Keyakinan Rendah: WP-Cron digunakan untuk menjalankan tugas terjadwal di WordPress. Pastikan untuk memeriksa dan mengoptimalkan penggunaan WP-Cron agar tidak membebani server Anda.
3. File readme.html: File readme.html mengungkapkan informasi tentang instalasi WordPress. Ini dapat memberikan petunjuk kepada penyerang tentang versi dan komponen yang digunakan. Pertimbangkan untuk menghapus atau menyembunyikan file ini.
4. robots.txt: Aturan dalam file robots.txt mengarahkan ke direktori wp-admin. Pastikan aturan ini tidak memperlihatkan informasi sensitif atau mengizinkan akses yang tidak diinginkan.
5. Informasi Server: Informasi tentang server (Apache/2.4.59 dan PHP/8.2.18) dapat membantu penyerang dalam merencanakan serangan. Pertimbangkan untuk menyembunyikan informasi ini dari respons server.



