

# Laporan Pengerjaan Lab Praktikum

## Ethical hacking



Nama : Gilang Raya Kurniawan  
NRP : 5027221045

---

# Daftar pustaka

<b>Disclaimer .....</b>	<b>2</b>
<b>Contact Information .....</b>	<b>2</b>
<b>Mengidentifikasi Tingkat Kerentanan .....</b>	<b>2</b>
<b>Scope .....</b>	<b>2</b>
<b>Pengecualian Ruang Lingkup .....</b>	<b>2</b>
<b>Lingkup dan Batasan Waktu .....</b>	<b>2</b>
<b>Rangkuman Kerentanan &amp; Rapor .....</b>	<b>2</b>

## Disclaimer

Pengerjaan Praktikum 2 kali ini dilaksanakan dalam periode selama tiga hari, dimulai dari tanggal 5 Mei 2024 hingga 8 Mei 2024. Pengerjaan praktikum bertujuan untuk menemukan kerentanan IP web yang di berikan dengan menggunakan prinsip prinsip ethical hacking

## Contact Information

Name	Title	Contact Information
Peserta		
Gilang Raya Kurniawan	Mahasiswa Teknologi Informasi Angkatan 2022	Email: gilangraya869@gmail.com

# Mengidentifikasi Tingkat Kerentanan

## Penetration Test Findings

0	0	2	0	3
Critical	High	Moderate	Low	Informational

Penemuan	keparahan	Rekomendasi
<u>Internal Penetration Test</u>		
CVE-2023-48795 (Vulnerable to Terrapin)	Moderate	Perbarui Sistem dengan patch terbaru atau konfigurasi yang aman
FTP Anonymous Login	Moderate	Nonaktifkan login Anonymous jika tidak digunakan.
SSH Server Enumeration	Informational	Perbarui server SSH dengan patch terbaru untuk mengatasi kerentanan yang diketahui
SSH Authentication Methods	Informational	Konfigurasi SSH sudah sesuai dengan praktik keamanan terbaik. Disarankan untuk membatasi penggunaan password dan mengutamakan penggunaan kunci publik
SSH HMAC Algorithm dan SSH Password Authentication	Informational	Pastikan bahwa pengaturannya aman dan sesuai dengan praktik keamanan terbaik

## Scope

### Pengecualian Ruang Lingkup

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

### Lingkup dan Batasan Waktu

Digunakan IP web Seperti di bawah

- 10.15.42.36
- 10.15.42.7

Server dibuka mulai tanggal 5 Mei 2024 hingga 8 Mei 2024

## Rangkuman Kerentanan & Rapor

`nmap --unprivileged -sV -sC -oN nmap1.log -Pn 10.15.42.36` di IP 10.15.42.36

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 20:48 SE Asia Standard Time
Nmap scan report for 10.15.42.36
Host is up (0.059s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to 10.33.3.205
|_    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 2
|_    vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.19.0.2 is not the same as 10.15.42.36
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|_   256  df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_   256  b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/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 71.50 seconds
```

Maka akan mendapatkan hasil sebagai berikut

1. Port 21/tcp: Terbuka, berjalan layanan FTP menggunakan vsftpd versi 3.0.5. Layanan ini memungkinkan login FTP anonim (kode FTP 230) dan

memberikan informasi tentang status FTP server, termasuk koneksi saat ini dan informasi lainnya.

2. Port 22/tcp: Terbuka, berjalan layanan SSH menggunakan OpenSSH versi 8.2p1 pada sistem operasi Ubuntu Linux. Informasi kunci host SSH (RSA, ECDSA, ED25519) juga diberikan.
3. Port 8888/tcp: Terbuka, berjalan layanan HTTP menggunakan Apache HTTP Server versi 2.4.38 di sistem operasi Debian.

Terlihat bahwa ditemukan port 8888 pada IP tersebut yang dapat diakses yang dimana berupa login Page, lalu IP tersebut mempunyai FTP(File transfer protocol) yang dapat kita akses

Membuka riwayat ftp dengan ftp 10.15.42.36

```
(root@GRK66-TUF)~[/home/grk]
# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65511|)
150 Here comes the directory listing.
-rwxrwxr-x  1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
```

Setelah saya telusuri ternyata riwayat ftp web tersebut cukup mudah dibobol dikarenakan riwayat username sudah terlihat ketika saya menggunakan nmap ke web tersebut dan digunakan non password

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Setelah digunakan command LS di ftp terlihat bahwa terdapat data bernama backup.sql

nikto -h http://10.15.42.36:8888/

```
- Nikto v2.5.0
-----
+ Target IP:      10.15.42.36
+ Target Hostname: 10.15.42.36
+ Target Port:    8888
+ Start Time:     2024-05-08 21:17:18 (GMT7)
-----
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: 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)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vinteb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:     2024-05-08 21:26:53 (GMT7) (575 seconds)
-----
+ 1 host(s) tested
```

Setelah dilakukan scanning dengan menggunakan Nikto ditemukan kerentanan pada web tersebut pada port 8888, antara lain

1. Versi Server: Apache/2.4.38 (Debian). memberikan informasi tentang versi server web yang sedang berjalan.
2. X-Powered-By Header: PHP/7.2.34. Mengungkapkan bahwa server menggunakan PHP sebagai bahasa pemrograman backend.
3. X-Frame-Options Header
4. X-Content-Type-Options Header
5. Versi Apache: Apache/2.4.38 outdated
6. File README Apache: Terdapat file README Apache yang ditemukan di /icons/README. Hal ini bisa memberikan petunjuk kepada hacker tentang struktur server atau konfigurasi default yang mungkin bisa dieksploitasi.
7. Junk HTTP Methods: Server merespons dengan metode HTTP yang tidak valid.

nuclei -u 10.15.42.36 -o grk.txt

```
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7894
[INF] Executing 7839 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 0 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["publickey", "password"]
[INF] Using Interactsh Server: oast.online
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.36:22
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21
[openssh-detect] [tcp] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
```

```
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["publickey","password"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-shal-hmac-algo] [javascript] [info] 10.15.42.36:22
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21
[openssh-detect] [tcp] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
```

Ditemukan satu Common Vulnerabilities and Exposures pada IP 10.15.42.36 ketika di scan dengan menggunakan nuclei dengan tingkat CVE (CVE-2023-48795) medium/moderate

`nmap --unprivileged -sV -sC -oN nmap1.log -Pn 10.15.42.7`

```
(root@GRK66-TUF)~/home/grk
# nmap --unprivileged -sV -sC -oN nmap1.log -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 22:09 WIB
Nmap scan report for 10.15.42.7
Host is up (0.061s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
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-title: Hello World
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-generator: WordPress 6.5.2
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 14.31 seconds
```

1. Port 22/tcp (SSH): Terbuka. Menjalankan OpenSSH 8.2p1 di atas sistem Ubuntu Linux. Tiga kunci host SSH telah diungkapkan.
2. Port 80/tcp (HTTP): Terbuka. Menjalankan server web Apache httpd 2.4.59 di atas sistem Debian. Judul halaman web adalah "Hello World", dan server header menunjukkan versi Apache yang sedang berjalan. robots.txt menyatakan bahwa akses ke `/wp-admin/` dilarang. Situs web dibangun menggunakan WordPress 6.5.2.

Ditemukan bahwa port 80 pada port tersebut terbuka, dengan robots.txt menyatakan bahwa akses ke `/wp-admin/` dilarang tapi mungkin masih ada cara lain

`nikto -h 10.15.42.7`



```

+ Target IP: 10.15.42.7
+ Target Hostname: 10.15.42.7
+ Target Port: 80
+ Start Time: 2024-05-08 22:17:09 (GMT)

+ Server: Apache/2.4.59 (Debian)
+ /: Retrieved x-powered-by header: PHP/8.2.18.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: <http://10.15.42.7/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/canner/vulnerabilities/raising-content-type-header/
+ /: 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/raising-content-type-header/
+ /ncghuJ7.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

```

Setelah dilakukan scanning dengan menggunakan Nikto ditemukan kerentanan pada web tersebut antara lain

1. Versi Server: Apache/2.4.59 (Debian).
2. X-Powered-By Header: PHP/8.2.18.
3. X-Frame-Options Header
4. Drupal Link Header: Link header yang mengacu pada situs Drupal
5. X-Content-Type-Options Header: Header ini juga tidak diatur. Dapat meningkatkan risiko serangan XSS.
6. Header X-Redirect-By: Header yang tidak umum ditemukan mungkin menunjukkan penggunaan fitur atau plugin khusus WordPress.
7. robots.txt: File robots.txt mengandung 2 entri yang sebaiknya dilihat secara manual. Ini adalah aturan untuk robot mesin telusur web.
8. Junk HTTP Methods: Server merespons dengan metode HTTP yang tidak valid. Ini bisa menjadi tanda serangan atau konfigurasi yang salah.

curl http://10.15.42.7/robots.txt

```

C:\Users\Gilang>curl http://10.15.42.7:robots.txt
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535

C:\Users\Gilang>curl http://10.15.42.7/robots.txt
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://10.15.42.7/wp-sitemap.xml

```

Ditemukan bahwa kita bisa mengakses /wp-admin/admin-ajax.ph tetapi kita tidak bisa mengakses /wp-admin/ saja hanya saja didalamnya terisi nilai 0

```
C:\Users\Gilang>curl http://10.15.42.7/wp-admin/admin-ajax.php
0
```