

Melakukan nmap 10.15.42.7

```
(baeblue@kali)~$ sudo nmap -sV -O 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 21:28 WIB
Nmap scan report for 10.15.42.7
Host is up (0.0083s 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)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.43 seconds
```

```
(baeblue@kali)~$ nmap -sV -sC -oN nmaplog.log 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 21:33 WIB
Nmap scan report for 10.15.42.7
Host is up (0.045s 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-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-title: Hello World
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-generator: WordPress 6.5.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

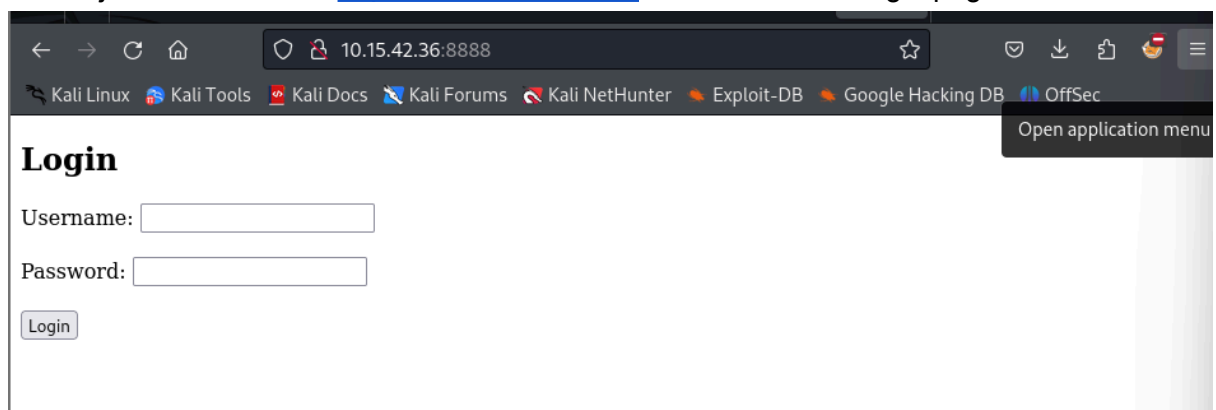
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.54 seconds
```

Melakukan nmap 10.15.42.36

```
(baeblue@kali)-[~]
$ sudo nmap -sV -O 10.15.42.36
[sudo] password for baeblue:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 22:18 WIB
Nmap scan report for 10.15.42.36
Host is up (0.0048s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp  open  http     Apache httpd 2.4.38 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 32.76 seconds
```

- ditemukan port yang terbuka yaitu port 8888
- jika masuk ke link <http://10.15.42.36:8888> akan ditemukan login page



← → ↻ 🏠 10.15.42.36:8888 ☆ 📁 📄 📄 📄 📄

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Open application menu

Login

Username:

Password:

Login

jalankan ftp 10.15.42.36 21 di terminal untuk masuk ke salah satu port yang terbuka

```
(baeblue@kali)-[~]
$ ftp 10.15.42.36 21
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:baeblue): 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 (|||65515|)
150 Here comes the directory listing.
-rwxrwxr-x  1 ftp      ftp      1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> get backup.sql
local: backup.sql remote: backup.sql
229 Entering Extended Passive Mode (|||65503|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |*****| 1997      1.08 MiB/s   00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (176.71 KiB/s)
ftp> quit
```

- masuk dengan nama user anonymous dan tanpa password
- lalu akan ditemukan file backup.sql

buka file backup.sql

```
(baeblue@kali)-[~]
$ ls
Desktop  Music  SecLists-master  backup.sql  nmaplog.log  rustscan_2.0.1_amd64.deb
Documents  Pictures  Templates  index.js  node_modules  rustscan_2.0.1_amd64.deb.1
Downloads  Public  Videos  nmap_7.txt  package-lock.json  wpscan_7.txt

(baeblue@kali)-[~]
$ cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
--
-- Server version      8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;
```


Melakukan scanning dengan nikto

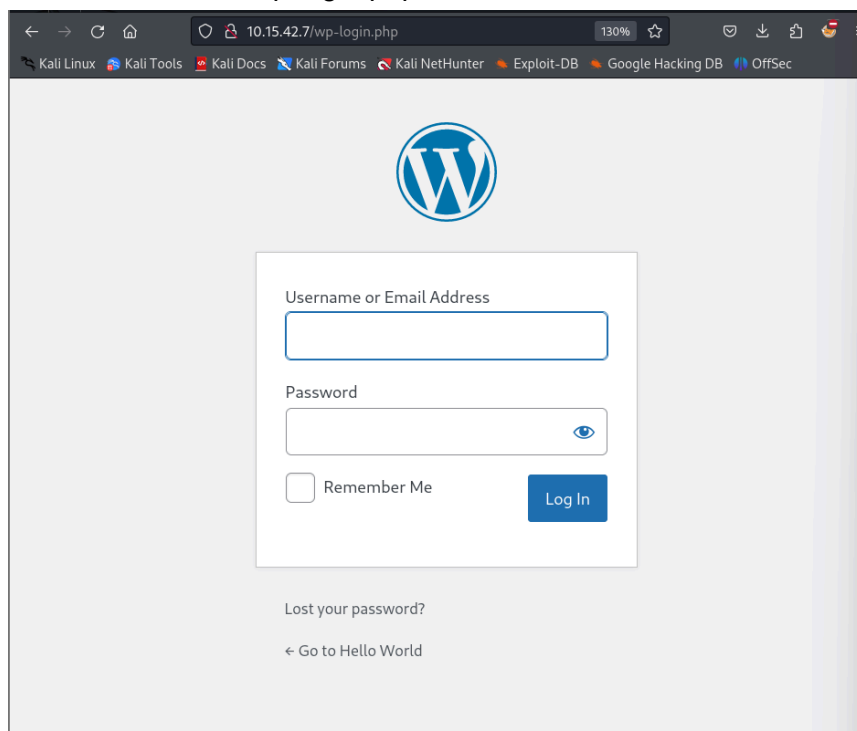
```
(baeblue@kali)-[~]
$ nikto -h 10.15.42.7
- Nikto v2.5.0

+ Target IP: 10.15.42.7
+ Target Hostname: 10.15.42.7
+ Target Port: 80
+ Start Time: 2024-05-08 00:20:29 (GMT7)

+ 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/
+ /: 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/
+ /smlaD6Xo.: 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.
+ /wp-links-opml.php: This Wordpress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /: A Wordpress installation was found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login.php: Wordpress login found.
+ 8118 requests: 3 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-05-08 00:51:38 (GMT7) (1869 seconds)

+ 1 host(s) tested
```

- ditemukan /wp-login.php



Melakukan Scanning dengan gobuster

```
(baeblue@kali)~[~/SecLists-master/Discovery/Web-Content/URLs]
$ gobuster dir -u 10.15.42.7 -w urls-wordpress-3.3.1.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: 10.15.42.7 http://10.15.42.7
[+] Method: 10.15.42.7 GET
[+] Threads: 10
[+] Wordlist: 10.15.42.7 urls-wordpress-3.3.1.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/license.txt (Status: 200) [Size: 19915]
/wp-admin/admin-footer.php (Status: 200) [Size: 2]
/readme.html (Status: 200) [Size: 7401]
/wp-admin/admin-header.php (Status: 500) [Size: 0]
/wp-admin/admin-functions.php (Status: 500) [Size: 0]
/wp-admin/about.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fabout.php&reauth=1]
/wp-activate.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?action=register]
/wp-admin/admin-ajax.php (Status: 400) [Size: 1]
/wp-admin/credits.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fcredits.php&reauth=1]
/index.php (Status: 301) [Size: 0] [→ http://10.15.42.7/]
/wp-admin/admin-post.php (Status: 200) [Size: 0]
/wp-admin/admin.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fadmin.php&reauth=1]
/wp-admin/comment.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fcomment.php&reauth=1]
/wp-includes/rss.php (Status: 500) [Size: 0]
/wp-includes/script-loader.php (Status: 500) [Size: 0]
/wp-includes/Text/Diff/Engine/string.php (Status: 200) [Size: 0]
/wp-includes/Text/Diff/Renderer/inline.php (Status: 200) [Size: 0]
/wp-includes/Text/Diff/Engine/xdiff.php (Status: 200) [Size: 0]
/wp-includes/Text/Diff/Renderer.php (Status: 200) [Size: 0]
/wp-includes/theme-compat/comments.php (Status: 500) [Size: 0]
/wp-includes/theme-compat/footer.php (Status: 500) [Size: 0]
/wp-includes/Text/Diff.php (Status: 200) [Size: 0]
/wp-includes/theme-compat/header.php (Status: 500) [Size: 0]
/wp-includes/theme.php (Status: 200) [Size: 0]
/wp-includes/theme-compat/sidebar.php (Status: 500) [Size: 0]
/wp-includes/user.php (Status: 200) [Size: 0]
/wp-includes/update.php (Status: 500) [Size: 0]
/wp-includes/widgets.php (Status: 200) [Size: 0]
/wp-includes/version.php (Status: 200) [Size: 0]
/wp-includes/vars.php (Status: 500) [Size: 0]
/wp-includes/wp-diff.php (Status: 500) [Size: 0]
/wp-includes/wp-db.php (Status: 200) [Size: 0]
/wp-load.php (Status: 200) [Size: 0]
/wp-signup.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?action=register]
/wp-settings.php (Status: 500) [Size: 0]
/wp-links-opml.php (Status: 200) [Size: 226]
/wp-register.php (Status: 301) [Size: 0] [→ http://10.15.42.7/wp-login.php?action=register]
/wp-mail.php (Status: 403) [Size: 2501]
/wp-login.php (Status: 200) [Size: 4049]
/xmlrpc.php (Status: 405) [Size: 42]
Progress: 927 / 928 (99.89%)

Finished
```