Additional Information Ethack Praktikum 2
Nicholas Marco Weinandra - 5027221042

1. nmap scan
- nmap -T4 -min-rate 10000 -sCV -p- -A -Pn -oN nmap_scan_ethack 10.15.42.7

```
nicholas@Nicholas:~$ cat nmap_scan_ethack
# Nmap 7.80 scan initiated Tue May  7 18:13:48 2024 as: nmap -T4 -min-rate 10000 -sCV -p- -A -Pn -oN nmap_scan_ethack 10
.15.42.7
Warning: 10.15.42.7 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.7
Host is up (0.22s latency).
Not shown: 65386 closed ports, 147 filtered ports
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))
|_http-generator: WordPress 6.5.2
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Hello World
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.
17) (90%), Adtran 424RG FTTH gateway (89%), Linux 2.6.39 - 3.2 (89%), Linux 3.1 - 3.2 (89%), Linux 3.11 (89%), Linux 3.2
 - 4.9 (89%), Linux 3.5 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   0.29 ms  Nicholas.mshome.net (172.30.0.1)
2   534.22 ms 10.33.0.1
```

- nmap -T4 -min-rate 10000 -sCV -p- -A -Pn -oN nmap_scan_ethack2 10.15.42.36

```
nicholas@Nicholas:~$ nmap -T4 -min-rate 10000 -sCV -p- -A -Pn -oN nmap_scan_ethack2 10.15.42.36
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-07 23:31 WIB
```

- sudo nmap -sN -PE 10.15.42.7

```
nicholas@Nicholas:~$ sudo nmap -sN -PE 10.15.42.7
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-07 18:21 WIB
Nmap scan report for 10.15.42.7
Host is up (0.033s latency).
Not shown: 998 closed ports
PORT   STATE        SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
```

- Sudo nmap -sN -PE 10.15.42.36

```
nicholas@Nicholas:~$ sudo nmap –sN –PE 10.15.42.36
[sudo] password for nicholas:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-07 22:37 WIB
Nmap scan report for 10.15.42.36
Host is up (0.094s latency).
Not shown: 996 closed ports
PORT      STATE          SERVICE
20/tcp    open|filtered ftp-data
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
8888/tcp open|filtered sun-answerbook
```

2. Nikto Scan

- Nikto -h 10.15.42.7 Tuning x

- Nikto –h 10.15.42.36 -Cgidirs all

- Nikto -h 10.15.42.7 -Cgidirs all

- Nikto -h 10.15.42.36:8888
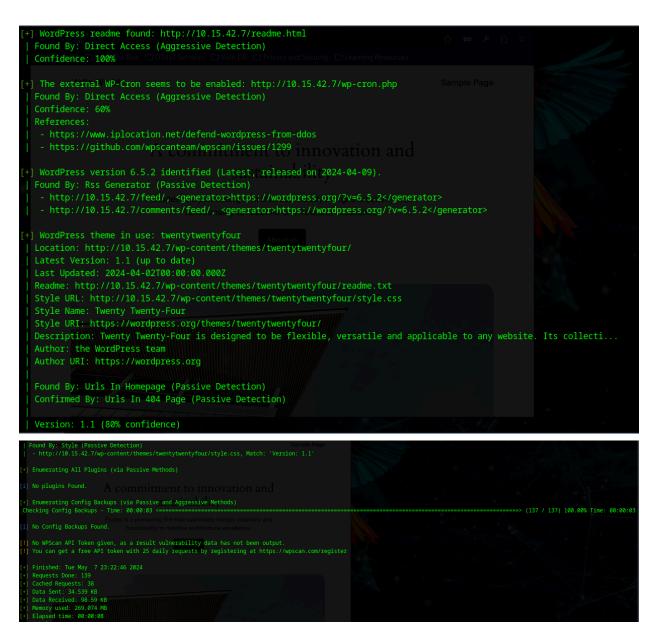
```
  [x]-[nicholas@parrot]-[~]
    $nikto -h 10.15.42.36:8888 -Cgidirs all
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.15.42.36
+ Target Hostname:    10.15.42.36
+ Target Port:        8888
+ Start Time:         2024-05-07 22:53:09 (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/
+ 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.
```

3. Gobuster

- Pake gobuster dir -u 10.15.42.7 -w
  /home/nicholas/subdirectories-discover/dsstorewordlist.txt -o gobuster-output.log

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content             (Status: 301) [Size: 313] [--> http://10.15.42.7/wp-content/]
/robots.txt             (Status: 200) [Size: 110]
/index.php              (Status: 301) [Size: 0] [--> http://10.15.42.7/]
/wp-includes            (Status: 301) [Size: 314] [--> http://10.15.42.7/wp-includes/]
/wp-admin               (Status: 301) [Size: 311] [--> http://10.15.42.7/wp-admin/]
/license.txt            (Status: 200) [Size: 19915]
/xmlrpc.php             (Status: 405) [Size: 42]
/wp-load.php            (Status: 200) [Size: 0]
/wp-comments-post.php   (Status: 405) [Size: 0]
/wp-links-opml.php      (Status: 200) [Size: 226]
/wp-cron.php            (Status: 200) [Size: 0]
/wp-settings.php        (Status: 500) [Size: 0]
/wp-config-sample.php   (Status: 500) [Size: 2412]
/.htaccess              (Status: 403) [Size: 275]
/wp-activate.php        (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-login.php?action=register]
/wp-config.php          (Status: 200) [Size: 0]
/wp-login.php           (Status: 200) [Size: 4049]
/admin                  (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-admin/]
/wp-signup.php          (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-login.php?action=register]
/sitemap.xml            (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-sitemap.xml]
/wp-mail.php            (Status: 403) [Size: 2501]
/login.php              (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-login.php]
/dashboard              (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-admin/]
/rss                    (Status: 301) [Size: 0] [--> http://10.15.42.7/feed/]
/wp-register.php        (Status: 301) [Size: 0] [--> http://10.15.42.7/wp-login.php?action=register]
/login                  (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-login.php]
```

4. WPScan

- wpscan --url 10.15.42.7

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
 | - 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/scanner/http/wordpress_xmlrpc_login/
 | - 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%

```
[+] 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: 00:00:03 <=====================================================================================================> (137 / 137) 100.00% Time: 00:00:03

[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: Tue May  7 23:22:46 2024
[+] Requests Done: 139
[+] Cached Requests: 38
[+] Data Sent: 34.539 KB
[+] Data Received: 98.59 KB
[+] Memory used: 269.074 MB
[+] Elapsed time: 00:00:08
```

- wpscan --url 10.15.42.36

```
┌─[nicholas@parrot]─[~]    □ OSINT Services  □ Vuln DB  □ Privacy and Security  □ Learning Resources
└─• $wpscan --url 10.15.42.36
           Hello World                                                    Sample Page

         __          _____   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___    __ _  _ _ ___ ®
           \ \/  \/ / |  ___/ \___ \  / _` | '_ \
            \  /\  /  | |     ____) | | (_| | | | |
             \/  \/   |_|    |_____/ \__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                    Version 3.8.25
         Sponsored by Automattic - https://automattic.com/
         @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart


Scan Aborted: The url supplied 'http://10.15.42.36/' seems to be down (Couldn't connect to server)
```

5. Nuclei

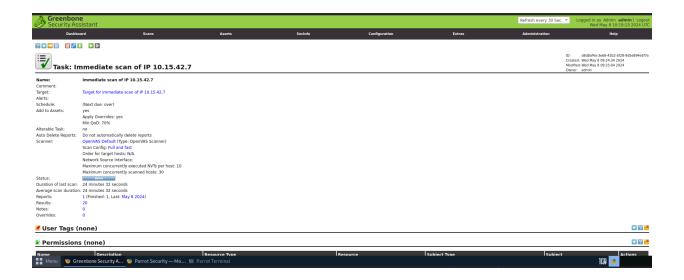- nuclei -u 10.15.42.7 -o nuclei_result.txt

```
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
```

```
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
```

- nuclei -u 10.15.42.36 -o nuclei_result2.txt

```
┌─[nicholas@parrot]─[~]
└──╼ $nuclei -u 10.15.42.36 -o nuclei_result2.txt



                      __          _____/ /_   (_)
   ___  __  _____/ /__   (_)
  / _ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                    projectdiscovery.io


[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: 7893
[INF] Executing 7838 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)
[INF] Using Interactsh Server: oast.site
[INF] No results found. Better luck next time!
```

6. OpenVAS

7. FTP


```
nicholas@Nicholas:~$ ftp 10.15.42.7
ftp: Can't connect to '10.15.42.7:21': Connection refused
ftp: Can't connect to '10.15.42.7:ftp'
ftp> ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:nicholas): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp        ftp           1997 May 04 15:40 backup.sql
```

```
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
```

8. Nessus Scan

NetworkScan_Policy / 10.15.42.36
‹ Back to Hosts

Configure | Audit Trail | Launch ▼ | Report | Export ▼

Vulnerabilities 22

Filter ▼ | Search Vulnerabilities 🔍 | 22 Vulnerabilities

	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾	⚙
☐	MIXED	...	...	📁 PHP (Multiple Issues)	CGI abuses	4	⊘ ✎
☐	MEDIUM	2.1 *	4.2	ICMP Timestamp Request Remote Date D...	General	1	⊘ ✎
☐	MIXED	...	...	📁 Openbsd Openssh (Multiple Issues)	Misc.	2	⊘ ✎
☐	INFO	...	...	📁 HTTP (Multiple Issues)	Web Servers	2	⊘ ✎
☐	INFO	...	...	📁 SSH (Multiple Issues)	General	2	⊘ ✎
☐	INFO	...	...	📁 SSH (Multiple Issues)	Misc.	2	⊘ ✎
☐	INFO	...	...	📁 SSH (Multiple Issues)	Service detection	2	⊘ ✎
☐	INFO	...	...	Nessus SYN scanner	Port scanners	3	⊘ ✎
☐	INFO	...	...	Service Detection	Service detection	3	⊘ ✎

Host Details 🗑

IP:	10.15.42.36
OS:	Linux Kernel 2.6
Start:	May 7 at 4:15 PM
End:	May 7 at 4:24 PM
Elapsed:	8 minutes
KB:	Download

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

NetworkScan_Policy / Plugin #10092
‹ Back to Vulnerabilities

Configure | Audit Trail | Launch ▼ | Report | Export ▼

Vulnerabilities 22

INFO **FTP Server Detection** ‹ ›

Description
It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Output

```
The remote FTP banner is :

220 FTP Server
```

To see debug logs, please visit individual host

Port ▴	Hosts
21 / tcp / ftp	10.15.42.36 ⧉

Plugin Details ✎

Severity:	Info
ID:	10092
Version:	1.57
Type:	remote
Family:	Service detection
Published:	October 12, 1999
Modified:	August 17, 2023

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Reference Information

IAVT: 0001-T-0030, 0001-T-0943