

CNS : Assignment – 8

Name : Nikita Sopan Tipule

Mis : 111903051

Branch : Computer Engineering

Division : 1

Study and analysis of following networking tools:

1. Hydra
2. nmap
3. wp scan

1. Hydra:

- Hydra – a very fast network logon cracker which supports many different services.
- It is a parallelized login cracker which supports numerous protocols to attack.
- New modules are easy to add, besides that, it is flexible and very fast. This tool gives researchers and security consultants the possibility to show how easy it would be to gain unauthorized access from a remote to a system.
- It is used for brute forcing attack on network service or web service
- it also supports for ipv6 and proxy support
- It is available in GUI version too.
- It supports approx. 51 protocols
- Hydra types :
 - i. CLI based
 - ii. GUI based
- Hydra Style:
 - i. new style :
 1. - hydra [some command line options]
PROTOCOL://TARGET:PORT/MODULE-OPTIONS
 - ii. Old style:
 1. - hydra [some command line options] [-s PORT] TARGET
PROTOCOL [MODULE-OPTIONS]
- Options in Hydra:
 - i. -l single user name
 - ii. -L List of user names
 - iii. -p Single user passwords
 - iv. -P List of Passwords
 - v. -V Show output on the screen
 - vi. -t Tasks
 - vii. -o Output File
 - viii. -m Module Options

```
Activities Terminal Nov 14 6:39 PM user@nikita-laptop: ~/Desktop/CNS
user@nikita-laptop:~/Desktop/CNS$ hydra ssh://192.168.152.185:22 -L /home/user/Desktop/CNS/username.txt -P /home/user/Desktop/CNS/password.txt -V -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 18:39:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:6/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.152.185:22/
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "nikital23" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "1234" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "tipule12" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "12345" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "ntipule" - 5 of 30 [child 4] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "nikital23" - 6 of 30 [child 5] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "1234" - 7 of 30 [child 6] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "tipule12" - 8 of 30 [child 7] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "12345" - 9 of 30 [child 8] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "ntipule" - 10 of 30 [child 9] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "nikital23" - 11 of 30 [child 10] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "1234" - 12 of 30 [child 11] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "tipule12" - 13 of 30 [child 12] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "12345" - 14 of 30 [child 13] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "ntipule" - 15 of 30 [child 14] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita-laptop" - pass "nikital23" - 16 of 30 [child 15] (0/0)
[22][ssh] host: 192.168.152.185 login: user password: 12345
[STATUS] attack finished for 192.168.152.185 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 18:39:47
user@nikita-laptop:~/Desktop/CNS$
```

```
Activities Terminal Nov 14 7:07 PM user@nikita-laptop: ~/Desktop/CNS
user@nikita-laptop:~/Desktop/CNS$ hydra ssh://192.168.152.185:22 -L /home/user/Desktop/CNS/username.txt -P /home/user/Desktop/CNS/password.txt -V -f -t 2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 19:07:36
[DATA] max 2 tasks per 1 server, overall 2 tasks, 30 login tries (l:6/p:5), ~15 tries per task
[DATA] attacking ssh://192.168.152.185:22/
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "nikital23" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "1234" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "tipule12" - 3 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "nikita" - pass "12345" - 4 of 30 [child 0] (0/0)
```

```
Activities Terminal Nov 14 7:12 PM user@nikita-laptop: ~
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "12345" - 9 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "tipule" - pass "ntipule" - 10 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "nikital23" - 11 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "1234" - 12 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "tipule12" - 13 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.152.185 - login "user" - pass "12345" - 14 of 30 [child 0] (0/0)
[22][ssh] host: 192.168.152.185 login: user password: 12345
[STATUS] attack finished for 192.168.152.185 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 19:07:55
user@nikita-laptop:~/Desktop/CNS$ ssh user@192.168.152.185 -p 22
The authenticity of host '192.168.152.185 (192.168.152.185)' can't be established.
ECDSA key fingerprint is SHA256:m/h5e9kXRhX8PcXhXrmCjuvljwXa3qkx00gBOZBHM9Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.152.185' (ECDSA) to the list of known hosts.
user@192.168.152.185's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.11.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

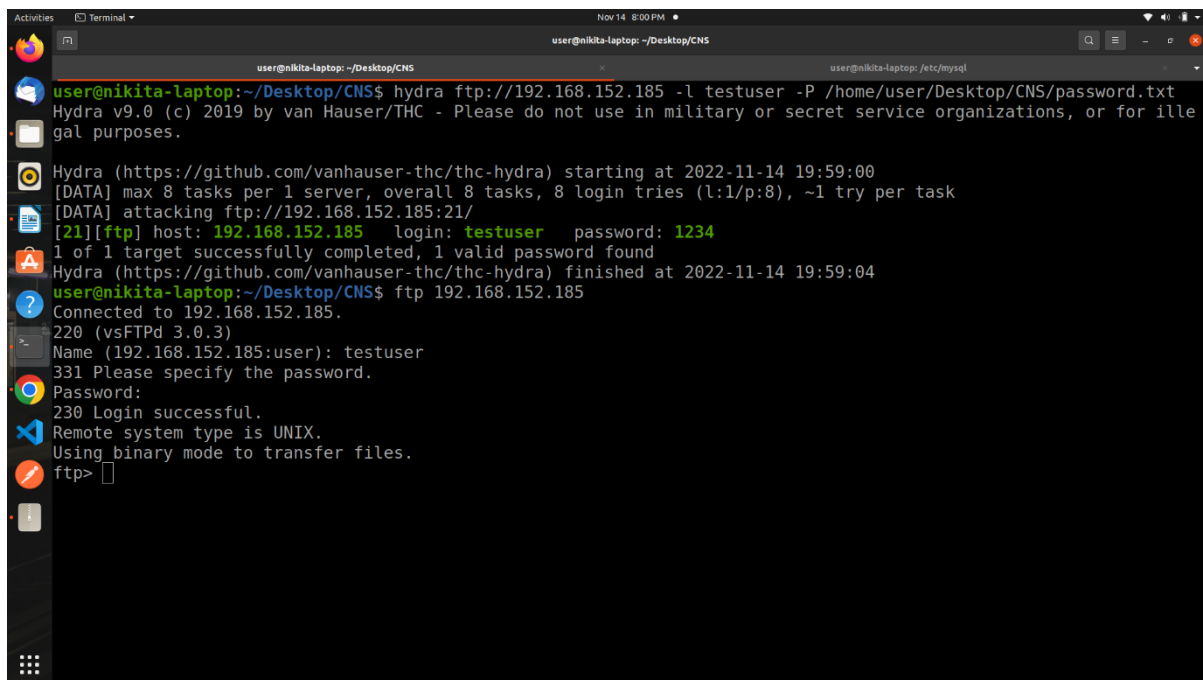
37 updates can be applied immediately.
10 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
user@nikita-laptop:~$
```

```
Activities Terminal Nov 14 7:59 PM user@nikita-laptop: ~/Desktop/CNS
user@nikita-laptop:~/Desktop/CNS$ hydra ftp://192.168.152.185 -l testuser -P /home/user/Desktop/CNS/password.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for ille
gal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 19:59:00
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ftp://192.168.152.185:21/
[21][ftp] host: 192.168.152.185 login: testuser password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 19:59:04
user@nikita-laptop:~/Desktop/CNS$
```



```
user@nikita-laptop: ~/Desktop/CNS
user@nikita-laptop: ~/Desktop/CNS
user@nikita-laptop: /etc/mysql

user@nikita-laptop:~/Desktop/CNS$ hydra ftp://192.168.152.185 -l testuser -P /home/user/Desktop/CNS/password.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 19:59:00
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ftp://192.168.152.185:21/
[21][ftp] host: 192.168.152.185 login: testuser password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 19:59:04
user@nikita-laptop:~/Desktop/CNS$ ftp 192.168.152.185
Connected to 192.168.152.185.
220 (vsFTPD 3.0.3)
Name (192.168.152.185:user): testuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

2. Nmap:

- Nmap is the most famous scanning tool used by penetration testers.
- Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.
- Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.
- There are a number of reasons why security pros prefer Nmap over other scanning tools.
-
- First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.
- Other features of Nmap include:
- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.

```
Activities Terminal Nov 14 9:18 PM user@nikita-laptop: ~ user@nikita-laptop: ~/etc/mysql user@nikita-laptop:~$ nmap moodle.coep.org.in Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:18 IST Nmap scan report for moodle.coep.org.in (210.212.183.6) Host is up (0.25s latency). Not shown: 997 filtered ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 443/tcp open https Nmap done: 1 IP address (1 host up) scanned in 35.67 seconds user@nikita-laptop:~$
```

```
Activities Terminal Nov 14 9:22 PM user@nikita-laptop: ~ user@nikita-laptop:~$ nmap -sV moodle.coep.org.in Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:21 IST Nmap scan report for moodle.coep.org.in (210.212.183.6) Host is up (0.081s latency). Not shown: 997 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 2.4.41 443/tcp open ssl/apache httpd (SSL-only mode) 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 22.60 seconds user@nikita-laptop:~$
```

```
Activities Terminal Nov 14 9:24 PM user@nikita-laptop: ~
user@nikita-laptop:~$ sudo nmap -p 80 moodle.coep.org.in
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:24 IST
Nmap scan report for moodle.coep.org.in (210.212.183.6)
Host is up (0.20s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
user@nikita-laptop:~$
```

```
Activities Terminal Nov 14 9:34 PM user@nikita-laptop: ~
user@nikita-laptop:~$ sudo nmap 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:34 IST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.11s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
user@nikita-laptop:~$
```

```
Nov 14 9:23 PM
user@nikita-laptop: ~
user@nikita-laptop:~$ sudo nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:23 IST
*****INTERFACES*****
DEV      (SHORT)      IP/MASK      TYPE      UP      MTU      MAC
lo        (lo)         127.0.0.1/8  loopback  up      65536
lo        (lo)         ::1/128     loopback  up      65536
eno1      (eno1)         (none)/0    ethernet  up      1500     80:E8:2C:26:69:A1
wlo1      (wlo1)         192.168.152.185/24  ethernet  up      1500     DC:FB:48:16:C0:C4
wlo1      (wlo1)         fe80::bala:f1e9:79fb:816d/64  ethernet  up      1500     DC:FB:48:16:C0:C4
wlo1      (wlo1)         2409:4081:111a:1f8e:6e1d:7b14:5857:7c4f/64  ethernet  up      1500     DC:FB:48:16:C0:C4
wlo1      (wlo1)         2409:4081:111a:1f8e:f6f6:6f4d:40e7:f1eb/64  ethernet  up      1500     DC:FB:48:16:C0:C4
virbr0    (virbr0)       192.168.122.1/24  ethernet  up      1500     52:54:00:0C:2F:BF
virbr0-nic (virbr0-nic)  (none)/0    ethernet  down    1500     52:54:00:0C:2F:BF

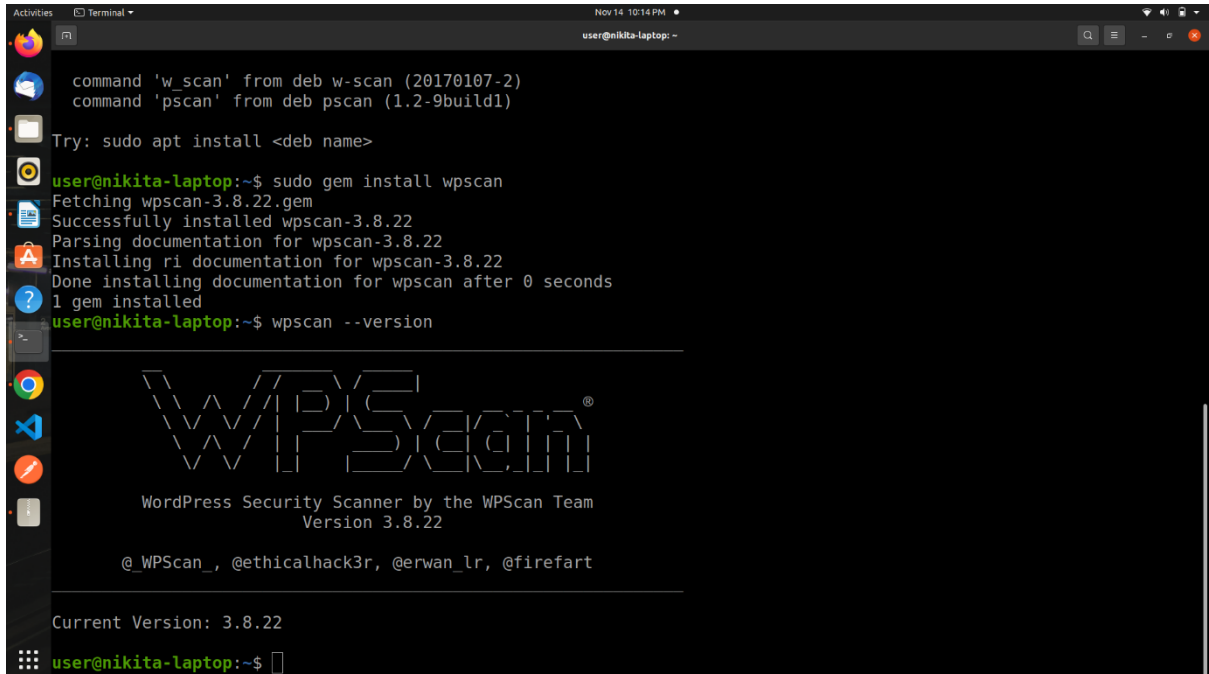
*****ROUTES*****
DST/MASK      DEV      METRIC GATEWAY
192.168.122.0/24  virbr0  0
192.168.152.0/24  wlo1    600
169.254.0.0/16    virbr0  1000
0.0.0.0/0         wlo1    600    192.168.152.181
::1/128          lo      0
2409:4081:111a:1f8e:6e1d:7b14:5857:7c4f/128  wlo1    0
2409:4081:111a:1f8e:f6f6:6f4d:40e7:f1eb/128  wlo1    0
fe80::bala:f1e9:79fb:816d/128  wlo1    0
::1/128          lo      256
2409:4081:111a:1f8e::/64      wlo1    600
fe80::/64         wlo1    600
ff00::/8          wlo1    256
::/0              wlo1    600    fe80::a05b:76ff:fe3d:a6ea

user@nikita-laptop:~$

Nov 14 9:23 PM
user@nikita-laptop: ~
user@nikita-laptop:~$ nmap 192.168.152.185
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-14 21:23 IST
Nmap scan report for nikita-laptop (192.168.152.185)
Host is up (0.000084s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
user@nikita-laptop:~$
```


3. Wp Scan:

- WPScan is a free tool that security professionals and website developers can use to perform “black box scanning” to test WordPress sites for vulnerabilities.
- Black box scans approach a website in the same way most hackers do. While they don’t have specific insider information, they’ll pore through your code and poke at sensitive points to find exploitable weaknesses.
- Because WordPress is one of the top CMS systems used to build websites, a lot of these vulnerabilities are well known across its popular themes, plugins, and even the core code itself.
- It’s a bit like having a house in a big subdivision, where all the houses have similar floor plans, construction, and even modifications. Once a thief knows of a weak point in one house, that weakness can likely be exploited across many.
- That’s both a pro and a con for site owners: A con because hackers don’t have to be particularly savvy to find and exploit vulnerabilities. But a pro because all those same tricks are known across the WordPress development and security communities. It can also be faster to identify weaknesses, implement fixes, and spread the word.
- WPScan bundles a huge chunk of that knowledge into a single tool. And because it takes that “black box” approach, you can see exactly how ripe-for-the-picking your site is in the eyes of hackers.



```
Activities Terminal Nov 14 10:14 PM user@nikita-laptop: ~
command 'w_scan' from deb w-scan (20170107-2)
command 'pscan' from deb pscan (1.2-9build1)
Try: sudo apt install <deb name>
user@nikita-laptop:~$ sudo gem install wpscan
Fetching wpscan-3.8.22.gem
Successfully installed wpscan-3.8.22
Parsing documentation for wpscan-3.8.22
Installing ri documentation for wpscan-3.8.22
Done installing documentation for wpscan after 0 seconds
1 gem installed
user@nikita-laptop:~$ wpscan --version

  WPSCAN®

WordPress Security Scanner by the WPScan Team
Version 3.8.22

 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Current Version: 3.8.22
user@nikita-laptop:~$
```



```
Activities Terminal Nov 14 10:29 PM user@nikita-laptop:~$ wpscan --url https://www.coepregatta.com/

  WPSCAN
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.coepregatta.com/ [2606:4700:8cad:52a3:aed7:2e:c676:8df]
[+] Started: Mon Nov 14 22:27:22 2022

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - platform: hostinger
| - content-security-policy: upgrade-insecure-requests
| - alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
| - x-turbo-charged-by: LiteSpeed
| - cf-cache-status: DYNAMIC
| - report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=0B8yA5NPG0jRLInT0luGqp8r41Lm4Aw%2BKo%2F2on%2FxPP%2Fp1FWNQJ0URRMSlmlQJCxub%2BIkzMKmoVXebh7rzp%2BnTzHNk0%2F%2BF2HAE7%2Bx%2BBV4wrguQDuZcQJzzEfBZPDNoLlrW4HfctxkMwqQ0I6Z3dLQsSk"}],"group":"cf-nel","max_age":604800}
| - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
```

```
Activities Terminal
user@nikita-laptop:~$ wpscan --url https://www.coepregatta.com/ --enumerate u

      WPSCAN
WordPress Security Scanner by the WPScan Team
      Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPScan_ @ethicalhack3r @erwan_lr @firefart

[+] URL: https://www.coepregatta.com/ [2606:4700:8d7d:52a3:aed7:3b:c676:8df]
[+] Started: Mon Nov 14 22:34:11 2022

Interesting Finding(s):

[+] Headers
    Interesting Entries:
    - platform: hostinger
    - content-security-policy: upgrade-insecure-requests
    - alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
    - x-turbo-charged-by: LiteSpeed
    - cf-cache-status: DYNAMIC
    - report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=0B8yA5NPG0jRLInT01uGqp8r41Lm4Aw%2BKo%2F2on%2FxPP%2Fp1FwNQJ0L"}]}
    - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
    - server: cloudflare
    - cf-ray: 76a1491d9e47f296-BOM
    Found By: Headers (Passive Detection)
    Confidence: 100%

[+] WordPress version 5.7 identified (Insecure, released on 2021-03-09).
    Found By: Emoji Settings (Passive Detection)
    - https://www.coepregatta.com/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.7'
    Confirmed By: Meta Generator (Passive Detection)
    - https://www.coepregatta.com/, Match: 'WordPress 5.7'

[+] WordPress theme in use: astra
    Location: https://www.coepregatta.com/wp-content/themes/astra/
    Latest Version: 3.9.4
    Last Updated: 2022-11-10T00:00:00.000Z
    Style URL: https://www.coepregatta.com/wp-content/themes/astra/style.css
    Found By: Urls In Homepage (Passive Detection)
    The version could not be determined.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:08 <====> (10 / 10) 100.00% Time: 00:00:08

[i] No Users 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 Nov 14 22:34:26 2022
[+] Requests Done: 31
[+] Cached Requests: 40
[+] Data Sent: 6.605 KB
[+] Data Received: 1.169 MB
[+] Memory used: 181.715 MB
[+] Elapsed time: 00:00:15
user@nikita-laptop:~$
```

```
Activities Terminal
user@nikita-laptop:~$ wpscan --url https://www.coepregatta.com/ --enumerate vp

      WPSCAN®
WordPress Security Scanner by the WPScan Team
      Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.coepregatta.com/ [2606:4700:8cad:52a3:aed7:2e:c676:8df]
[+] Started: Mon Nov 14 22:31:12 2022

Interesting Finding(s):

[+] Headers
Interesting Entries:
- platform: hostinger
- content-security-policy: upgrade-insecure-requests
- alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
- x-turbo-charged-by: LiteSpeed
- cf-cache-status: DYNAMIC
- report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=0B8yASNPG0jRLInT0LuGqp8r41Lm4Aw%2BKo%2F2on%2F2Fp1FwNQJ0UR"}], "success_fraction":0,"report_to":"cf-nel","max_age":604800}
- nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
- server: cloudflare
- cf-ray: 76a1491d9e47f296-BOM
Found By: Headers (Passive Detection)
Confidence: 100%

[+] WordPress version 5.7 identified (Insecure, released on 2021-03-09).
Found By: Emoji Settings (Passive Detection)
- https://www.coepregatta.com/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.7'
Confirmed By: Meta Generator (Passive Detection)
- https://www.coepregatta.com/, Match: 'WordPress 5.7'

[+] WordPress theme in use: astra
Location: https://www.coepregatta.com/wp-content/themes/astra/
Latest Version: 3.9.4
Last Updated: 2022-11-10T00:00:00.000Z
Style URL: https://www.coepregatta.com/wp-content/themes/astra/style.css
Found By: Urls In Homepage (Passive Detection)
The version could not be determined.

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] No plugins 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 Nov 14 22:31:15 2022
[+] Requests Done: 2
[+] Cached Requests: 77
[+] Data Sent: 498 B
[+] Data Received: 6.168 KB
[+] Memory used: 241.828 MB
[+] Elapsed time: 00:00:03
user@nikita-laptop:~$
```

```
Activities Terminal
user@nikita-laptop:~$ wpscan --url https://www.coepregatta.com/ --enumerate vt

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPScan, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.coepregatta.com/ [2606:4700:8d7d:52a3:aed7:3b:c676:8df]
[+] Started: Mon Nov 14 22:32:29 2022

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - platform: hostinger
| - content-security-policy: upgrade-insecure-requests
| - alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
| - x-turbo-charged-by: LiteSpeed
| - cf-cache-status: DYNAMIC
| - report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=0B8yASNPg0jRLInT0LuGqp8r41Lm4AwA2BKo%2F2on%2FxPP%2Fp1FwNQJ0URR"}], "group": "cf-nel", "max_age": 604800}
| - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
| - server: cloudflare
| - cf-ray: 76a1491d9e47f296-BOM
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] WordPress version 5.7 identified (Insecure, released on 2021-03-09).
| Found By: Emoji Settings (Passive Detection)
| - https://www.coepregatta.com/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.7'
| Confirmed By: Meta Generator (Passive Detection)
| - https://www.coepregatta.com/, Match: 'WordPress 5.7'

[+] WordPress theme in use: astra
| Location: https://www.coepregatta.com/wp-content/themes/astra/
| Latest Version: 3.9.4
| Last Updated: 2022-11-10T00:00:00.000Z
| Style URL: https://www.coepregatta.com/wp-content/themes/astra/style.css
| Found By: Urls In Homepage (Passive Detection)
| The version could not be determined.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:23 <=> (477 / 477) 100.00% Time: 00:00:23
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes 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 Nov 14 22:32:55 2022
[+] Requests Done: 479
[+] Cached Requests: 40
[+] Data Sent: 108.637 KB
[+] Data Received: 323.774 KB
[+] Memory used: 204.828 MB
[+] Elapsed time: 00:00:25
user@nikita-laptop:~$
user@nikita-laptop:~$
```