WEB DEVELOPER: 1

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A -sV -sT
192.168.103.154
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 12:53 EDT
Nmap scan report for 192.168.103.154
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_  256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.9.8
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Example site &#8211; Just another WordPress site
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 10.05 seconds
```

22

```
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_  256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
```

80

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.9.8
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Example site &#8211; Just another WordPress site
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

server

Searchsploit

website

```
<opml version="1.0">
<head>
<title>Links for Example site</title>
<dateCreated>Mon, 15 Mar 2021 17:19:12 GMT</dateCreated>
<!-- generator="WordPress/4.9.8" -->
</head>
<body> </body>
</opml>
```

Gobuster

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.103.154 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e -z -q -r -x php                                        2 ×
http://192.168.103.154/wp-content (Status: 200)
http://192.168.103.154/index.php (Status: 200)
http://192.168.103.154/wp-login.php (Status: 200)
http://192.168.103.154/wp-includes (Status: 200)
http://192.168.103.154/wp-trackback.php (Status: 200)
http://192.168.103.154/wp-admin (Status: 200)
http://192.168.103.154/wp-signup.php (Status: 200)
http://192.168.103.154/server-status (Status: 403)
```

WPScan

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.103.154
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.103.154/ [192.168.103.154]
[+] Started: Mon Mar 15 13:25:57 2021

Interesting Finding(s):
```

```
[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.103.154/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://192.168.103.154/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.103.154/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.103.154/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 4.9.8 identified (Insecure, released on 2018-08-02).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.103.154/index.php/feed/, <generator>https://wordpress.org/?v=4.9.8</generator>
 |  - http://192.168.103.154/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.9.8</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://192.168.103.154/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://192.168.103.154/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.6
 | Style URL: http://192.168.103.154/wp-content/themes/twentyseventeen/style.css?ver=4.9.8
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.7 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.103.154/wp-content/themes/twentyseventeen/style.css?ver=4.9.8, Match: 'Version: 1.7'
```

```
[+] 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
<=========================================================
(22 / 22) 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 Mar 15 13:26:00 2021
[+] Requests Done: 54
[+] Cached Requests: 5
[+] Data Sent: 13.483 KB
[+] Data Received: 290.307 KB
[+] Memory used: 240.816 MB
[+] Elapsed time: 00:00:02
```

Nikto

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://192.168.103.154:80'
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.154
+ Target Hostname:    192.168.103.154
+ Target Port:        80
+ Start Time:         2021-03-15 13:01:46 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with contents: </index.php/wp-json/>; rel="https://api.w.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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive
information
+ /wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:          2021-03-15 13:02:40 (GMT-4) (54 seconds)
```

Wordpress

```
┌──(kali㉿kali)-[~]
└─$ searchsploit WordPress
4.9.8
4 ×
----------------------------------------------------------------------------------------------------------------------------
--------------------------------
 Exploit
Title                                                                                                                      |
Path
----------------------------------------------------------------------------------------------------------------------------
--------------------------------
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private
Posts                                                                                  | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of
Service                                                                                                | php/dos/47800.py
WordPress Plugin Database Backup < 5.2 - Remote Code Execution
(Metasploit)                                                                                  | php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple
Vulnerabilities                                                                                   | php/webapps/-
39553.txt
WordPress Plugin EZ SQL Reports < 4.11.37 - Multiple
Vulnerabilities                                                                                  | php/webapps/-
38176.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL
Injection                                                                                          | php/webapps/-
44943.txt
WordPress Plugin Rest Google Maps < 7.11.18 - SQL
Injection                                                                                         | php/webapps/-
48918.sh
WordPress Plugin User Role Editor < 4.25 - Privilege
Escalation                                                                                     | php/webapps/44595.rb
WordPress Plugin Userpro < 4.9.17.1 - Authentication
Bypass                                                                                          | php/webapps/43117.txt
WordPress Plugin UserPro < 4.9.21 - User Registration Privilege
Escalation                                                                              | php/webapps/46083.txt
----------------------------------------------------------------------------------------------------------------------------
--------------------------------
Shellcodes: No Results
Papers: No Results
```

theme

twentyseventeen

metasploit

None