Bee-boop. Mr. Robot Write Up

Yo! Hi all. This is my Mr. Robot write-up and my very first attempt at capturing flags without any follow-along videos. I will use other write-ups for guidance if I truly get stuck or have exhausted all of my options via Google recon. This will take some time, as I just had my first child. So, with time off from work, I have one month to find all the flags. I just hope I can finish before then. Prayers up!

**Day One – May 18th**

After installing Mr. Robot, I entered my Linux credentials just to see if I could access it from the jump. Include an Image from screenshots.

I ran Ifconfig to find the IP address of the host system: **NAT Network 192.168.x.x** and **Bridged 10.0.0.x**

Conducted an Nmap scan on **192.168.x.0/24** using -sV (Services) and -A (OS and Version Detection). I checked each IP in the Firefox browser as a double check.

Mr.Robot IP discovered: **192.168.x.x**

I inserted Mr. Robot's IP in Firefox and did some recon. The author wrote a friendly message about learning from them and included a few commands. **Prepare** revealed a video about finances and the Mr.Robot movement. **F society** presented a question about moving forward. **Inform** displays international scandals. **Question** provided statements regarding false patriotism, capitalism, executives, and businessmen. **Wakeup** is another video with men talking aggressively and **Join** simply asks for your email address. I was a bit skeptical of “join”, but I took the chance and entered one of my old emails. It disappeared, leaving a message behind: **“I'll be in touch”** message. After doing some recon on that specifically, I found out it’s just a gimmick to pay homage to the show.

I right-clicked on **“View Source Page”** and checked the inspector for any suspicious data or anything out of place. Now, I honestly had no clue what I was looking for, but my Master's program taught me to be resilient and keep digging.

I found a message: **“You Are Not Alone”.** Not much value, but maybe this is a sign I’m getting closer.

I checked the rest of Nmap’s results and saw that **port 22** was closed and **ports 80** and **443** were open. Both ran **Apache** and did not have a title (txt/html). So, I decided to go over a pen test checklist I found on LinkedIn a few days ago to help keep me on track and also learn.

I checked the **robots.txt** file by adding **\robots.txt** to the end of the IP in the Firefox browser, and I discovered this:

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

I tried the same things for **sitemap.xml** and the **humans.txt files**. Neither yielded any valuable data.

**Day Two – May 20th**

Wooh. Day two.

I input the **key-1-of-3.txt** file at the end of the IP and received a string of numbers and letters.

Une image contenant texte, Police, capture d’écran, Graphique

Le contenu généré par l’IA peut être incorrect.

I looked at the string for a while. I thought it looked like a hash. I have minimal experience using hash functions aside from a homework assignment in my program, but I remember being just as puzzled. So, it clicked instantly. I tried the decoder for all hash types. No takers. So, maybe it isn't a hash???

Instead of giving up and trying something new, I tried the same string in the encoder, and it produced a value: **46e0b76caa96401382bf2ac1fa62798a**

After trying to force it to work in the browser and playing encoder–decoder via Base64, URL, MD5, SAML, I circled back to “maybe it isn’t a hash???”. So, maybe it’s a key or something that will lead me to another key. I’m moving on.

I went back to the robots.txt file and inserted the **\fsocity.dic** into the browser and was given a page with never-ending scrolling. Tons of data. It could be a list of critical usernames, passwords, or just random words. I am not sure if they will be of use, but I created and saved a file using vi. It could be useful later on.

**Day Three – May 23rd**

I wanted to use **gobuster** as I have in the past, but I forgot how it works. So, I watched some YouTube videos to explain it to me. I ended up using a write-up instead, as it was simpler to follow. Learning these commands will be fun for sure.

I just found out that **- - help** explains the letters in the commands to you. This is a lifesaver.

I did not have **dirb** or the **wordlists** set up on my Kali machine, so I downloaded the wordlists from GitHub and found dirb in another directory. I moved dirb into the share folder and then added the GitHub repository file into dirb, and bam, finished. So, I ran **gobuster dir -e -u 10.0.0.x -w /usr/share/dirb/wordlists/common.txt -x txt,php,py,cgi**

I think txt, php, py, and cgi are the types of files to search through? I could be wrong, but it makes the most sense to me.

The gobuster command said it had what looked like 800 thousand pieces of data to sift through, so I’m going to stop the scan and go to sleep.

**Day Four – May 24th**

Turns out I didn’t have time the next day. Baby called.

The gobuster command finished after 8 hours and nothing big turned up. I did, however, find a link to an HP login website.

Une image contenant texte, capture d’écran, Police, logo

Le contenu généré par l’IA peut être incorrect.

Will try to brute force it later on. In the meantime, I got stuck again and did a deep dive into other .txt files to see what else I need to learn to look for. I looked into **/readme and /license.txt**. /readme had a hidden message:

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

In the /license.txt file, I found another string **(ZWxsaW90OkVSMjgtMDY1Mgo=)**. Maybe this one is a hash? I decoded it and received **elliot:ER28-0652.** Odd looking for a username or password. So, I tried all the combinations.

Using the data found on the license.txt file, I was able to log in to the HP page under **Elliot Alderson**. It turns out he is an admin for WordPress.

I was able to recover an old post from the user, and it seems Elliot might be the one who created, or at least posted the video, about F Society. I recovered all of the deleted posts, but it did not yield any new data. I then checked the media page and found a screenshot that reveals a **username: alphanum** and **password: Dylan\_2791**. I inserted the credentials into the HP site and received a username error. At least I know the password must be correct. I did more recon on the media page and found two new usernames to try: **Dylan** and **mich05654**. Using mich05654 and Dylan\_2791 seemed to work. I logged in as **Krista Gordon**.

On Krista's profile, in her bio, it hints “another key”. So maybe I'm getting close.

**Day Five – May 27th**

I got stuck again and did not know what to look for. I’m sure I found something, but I can’t make heads or tails of it, so I used a guide. I saw another user run a **WPScan**. I found out that it is a vulnerability scan specifically for WordPress. The interesting findings turned up a good amount of data, so I followed up on each one.

Most data pointed to the **2015 theme editor**. I thought maybe something to do with the header. I clicked each tab available. Only a few were loaded. The others remained in an idle loading state. The exception was the editor tab, which gave me a full script to look at. Maybe I can edit this? or copy and paste it somewhere like the usernames from earlier?

I looked into **404 templates** and only saw numbers and letters all over the place. According to a YouTube video, there is something called a **reverse shell** that can be placed into the templates. So, I tried **pentestmonkey**’s reverse shell script that I found on GitHub.

I was unsuccessful in all of my attempts. I tried templates for 404 and **PHP**. I have internet access, I can ping my other devices and machines, but the pages are not loading properly. I think something is misconfigured in my network settings. I didn’t pay attention as closely as I thought when I ran Nmap earlier, but I found out all of my ports were closed. I know I looked at it, but I thought it was normal.

I will be taking a detour to figure this out. Though my master's program briefly covered networking, it did not stick as I’d hoped. Time to go learn more basic networking.

**Day Six – June 9th**

Yo! Hi, again. I found out that I need to implement port forwarding to resolve my issue. It is more complex than I thought, seeing as I know nothing about networking. I finally figured it out by watching countless videos, reading articles, asking Google and ChatGPT, and comparing all the notes to what makes sense in my mind. I tried everything I could think of, and it finally worked. I successfully configured my network to port forward from my host machine and receive the data on my guest machine. It was not a straightforward solution like the YouTube videos displayed. Creating rules and enabling them in the firewall did nothing. I aggressively attacked Google with question after question and took every little detail I found, wrote it out, pieced it together till I formed the final question for Google.

**“What is Sudo iptables and Netsh Interface? How do I use it to open ports and port forward?”**

Thanks to a video by **EmbraceTheRed** on YouTube, I learned what command to run and gained an understanding of what it does and how it works. Just a little. During this process, I learned more about Firewalls, reintroduced myself to the different functions of WAN and LAN, how to set and check firewall rules on the web interface and Windows and Kali command lines, how to force open and close ports, port forwarding and redirection, specific ports and their functions, how to find server data in the Inspector tab, and a bunch of commands that I saved in my notes. I am still green, but I’m feeling a new hue developing. Now, I think I can pick up where I left off.

**Day Seven – June 11th**

Two weeks left till I return to work. I really pray I can find all the flags by then. If not, well, that’s okay. As long as I complete the box, I will be pleased with my efforts and growth. As will my wife.