SIMPLE CTF Writeup

Written by Firestorm

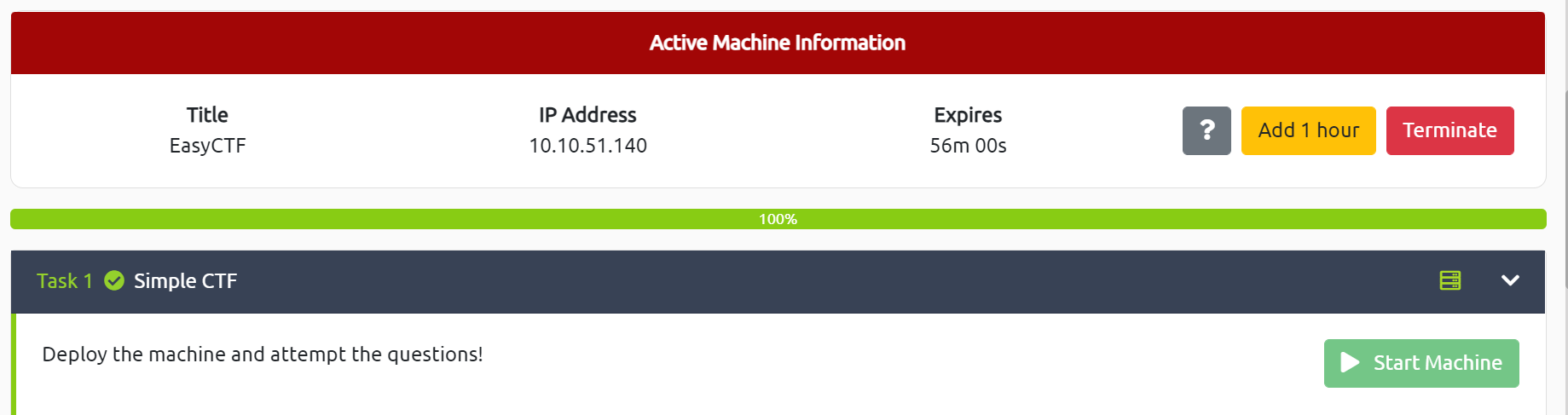
<https://tryhackme.com/room/easyctf>

**INTRODUCTION**

Structured Query Language Injection (SQLi) is an attack on a web application database server that allows malicious SQL queries to be executed on the server. SQL is a language used for querying databases i.e., retrieving, inserting, removing and updating data from the database. If the input is not properly validated user-provided SQL queries can be executed on the server. To learn more about database and its types check out the SQL injection room on tryhackme; <https://tryhackme.com/room/sqlinjectionlm>

**SET-UP**

Deploy the target machine and connect to your THM Openvpn profile from your linux machine using the command sudo openvpn [filename].ovpn. In a few seconds you will get the Ip address for the target machine.



**ENUMERATION**

Now that we have the IP address for the target machine, we will scan it using Nmap to search for any open ports/services running on it.

**nmap -sVC [TARGET IP] -vvv**

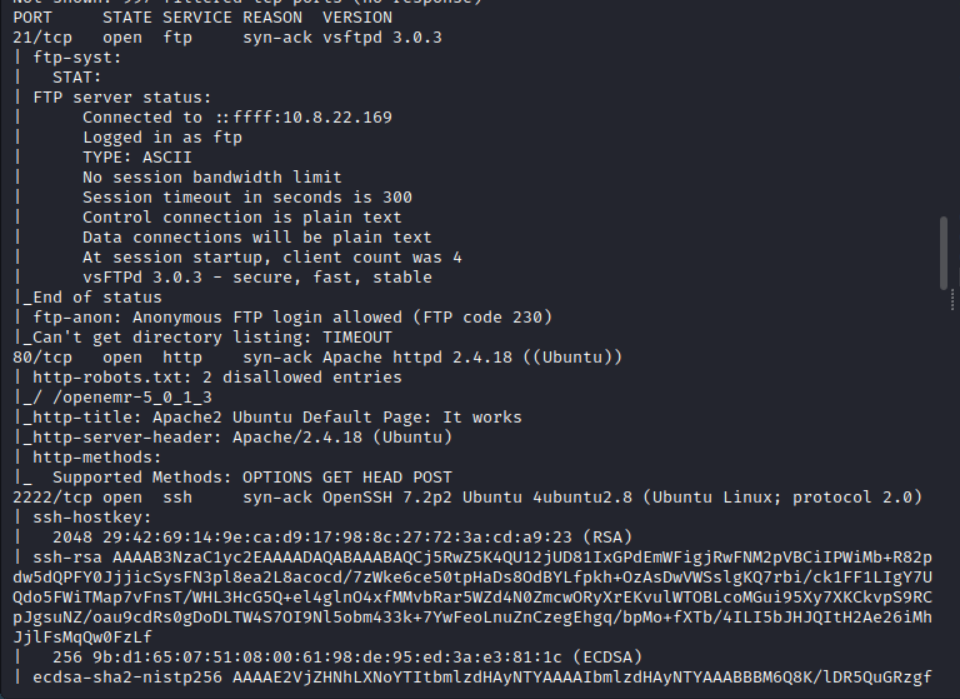
**-sVC:**

**-sV:** Enables service and version detection allowing us to see the services running on the ports and their version.

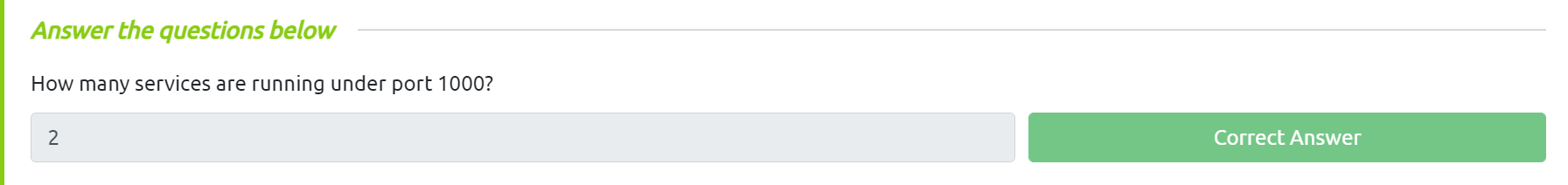
-**sC:** Performs a simple script scan using the default set of scripts.

**-vvv:** Increase verbosity.

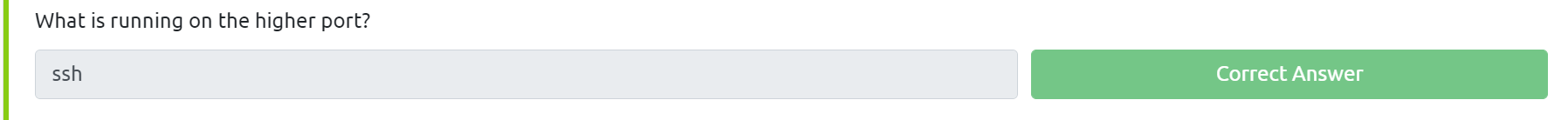
We can see from the Nmap scan results that there are 2 services running below port 1000 which are ftp on port 21 and http on port 80.



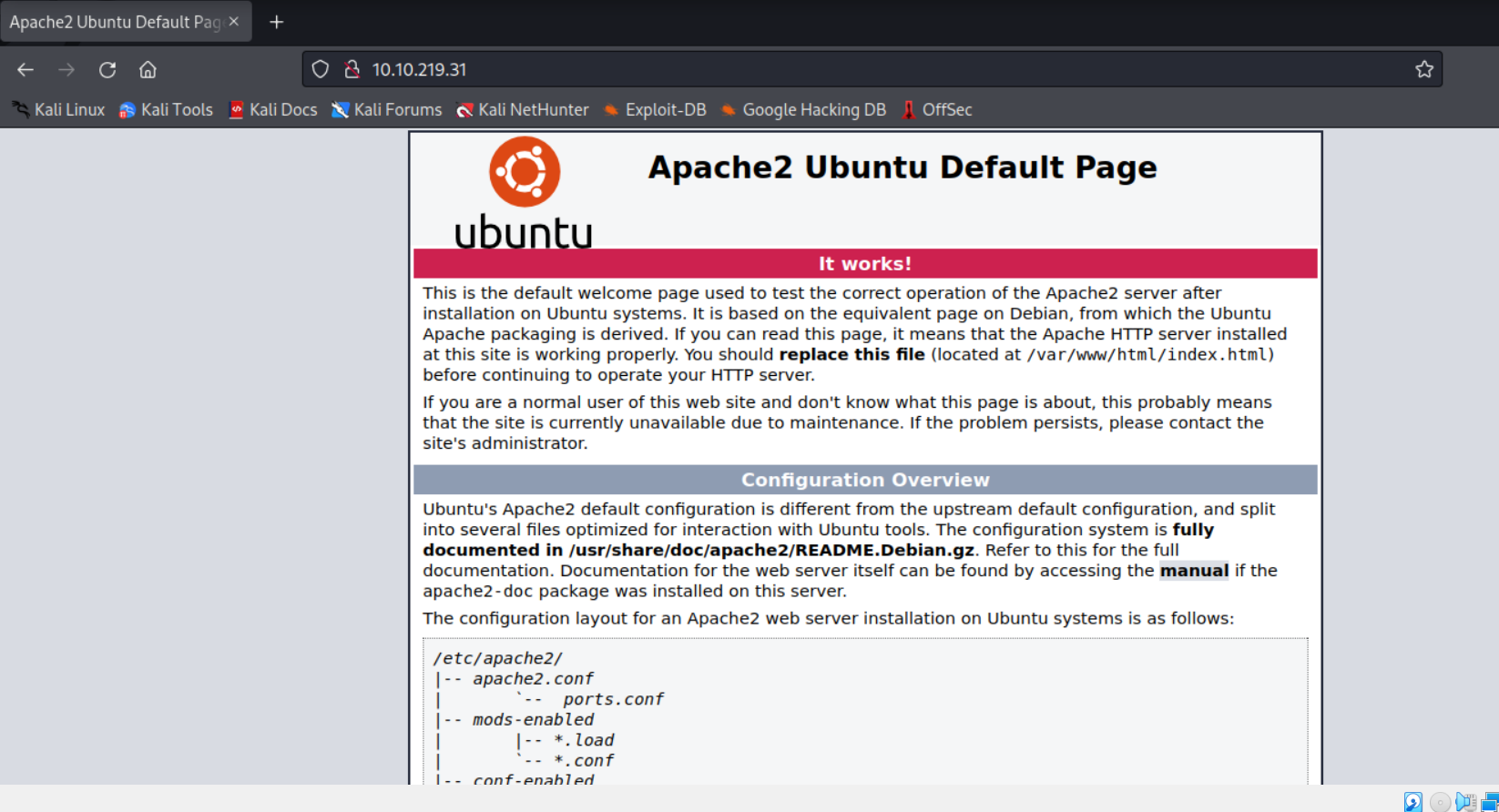
Hence, we have our first answer



From the same nmap scan we can see the service running on the higher port namely port 2222 is ssh which is the answer to the second question.

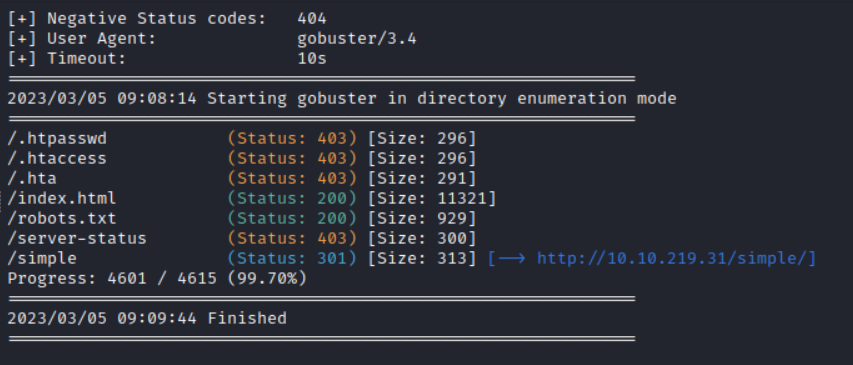


Since there is an http server on port 80, we can use the IP address to access the website on it. Simply enter the IP address in the search bar of your web browser.

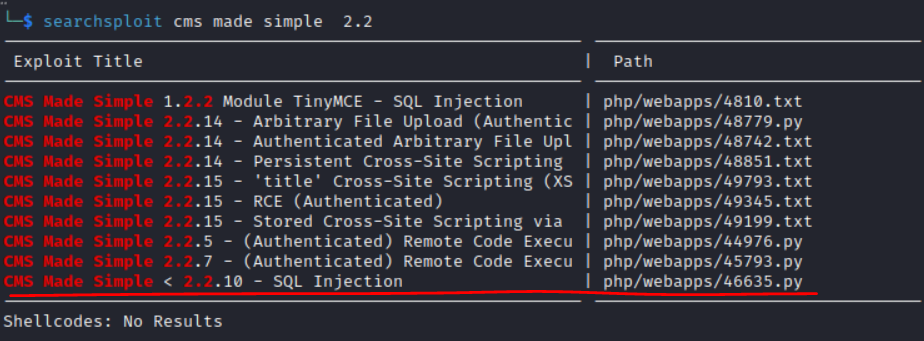
  
Unfortunately, nothing of interest can be found on this page. We can try accessing the robots.txt page which has 1 disallowed entry however it leads to a dead end.

When running Gobuster (A tool for brute forcing directories on web servers) a potentially interesting hidden folder shows up: /simple/

**gobuster dir --url http://10.10.219.31 --wordlist /usr/share/wordlists/dirb/common.txt**



This folder is running a content manager called CMS Made Simple (CMSMS) version 2.2. Upon searching for CVE’s for this content manager we will find a SQL injection vulnerability for our desired version.



At this point we can answer questions 3 and 4(you can check the CVE by googling the name of this exploit):

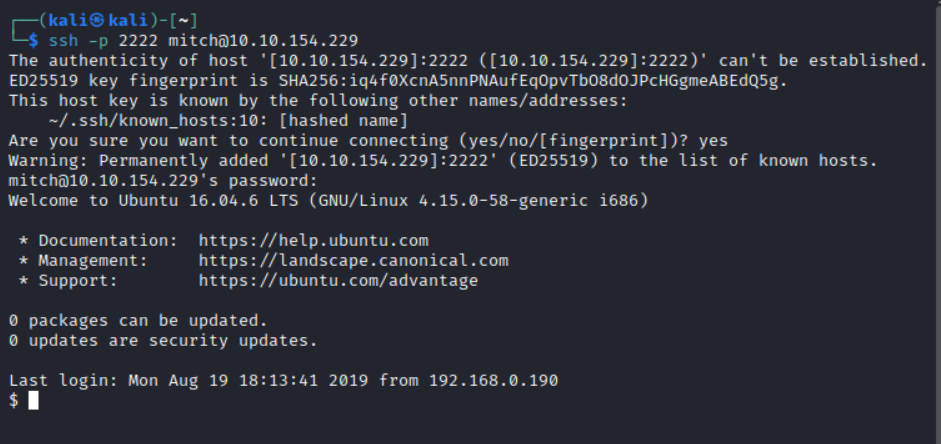


Google the exploit usi and run it with the following flags and arguments.

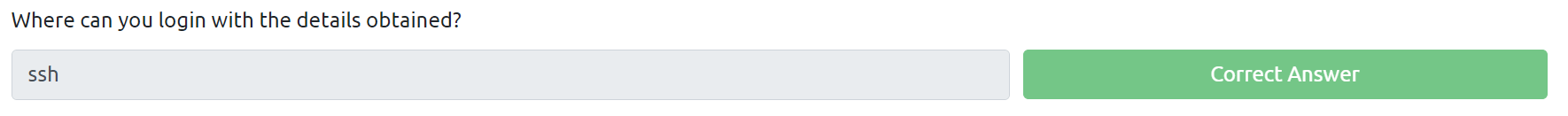
**python2 cmsms\_exploit.py -u http://[Target\_IP\_Address]/simple/ --crack -w [Wordlists]**

But where exactly do we login with the details obtained? One of the other services running is Openssh, on port 2222(refer to the nmap scan we used to answer the 2nd question). Lets try to login to that.

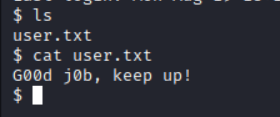
**ssh -p 2222 username@IPAddress**

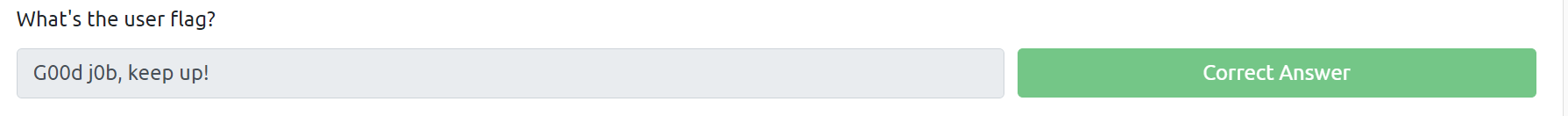


We have successfully logged in and can answer the 5th question.

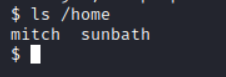


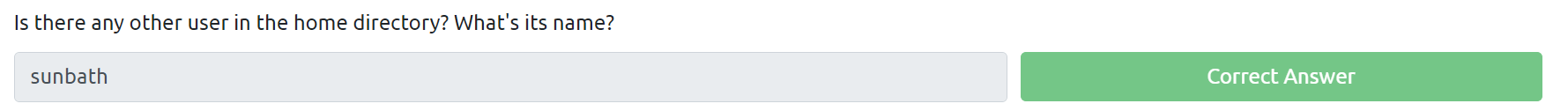
Moving on we have to search for the user flag; using ls we can see there is only one file present named user.txt. Opening this file provides us with our flag.



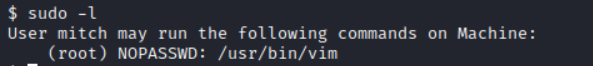


To check for other users in the home directory we can ls the home directory.

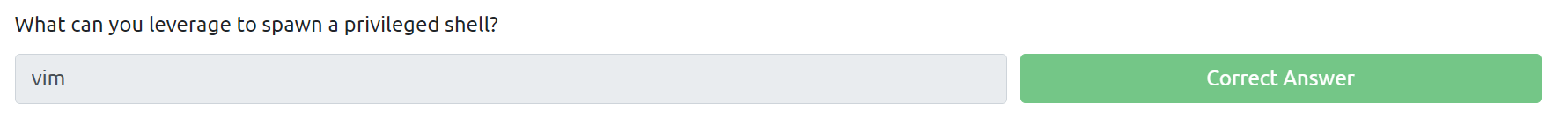




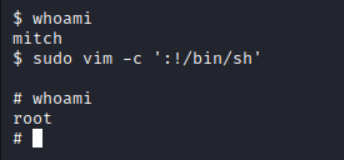
Since we need to spawn a root shell we can check what higher privileged rights the current user has using the **sudo -l** command



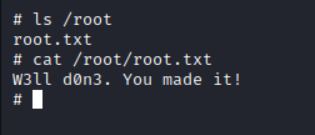
We can see the current user(mitch) can run the binary file called vim as root without needing a password.

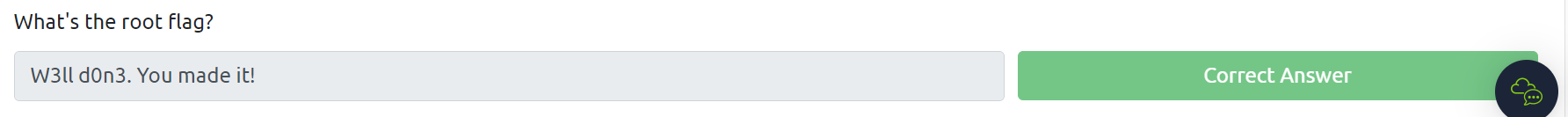


Vim can be used to spawn a shell using the command: **vim -c ':!/bin/sh'**



Congratulations we are root! We will find our flag in /root directory.





A fun and simple ctf for beginners, hope you had a banger of a time completing this. Onto the next.