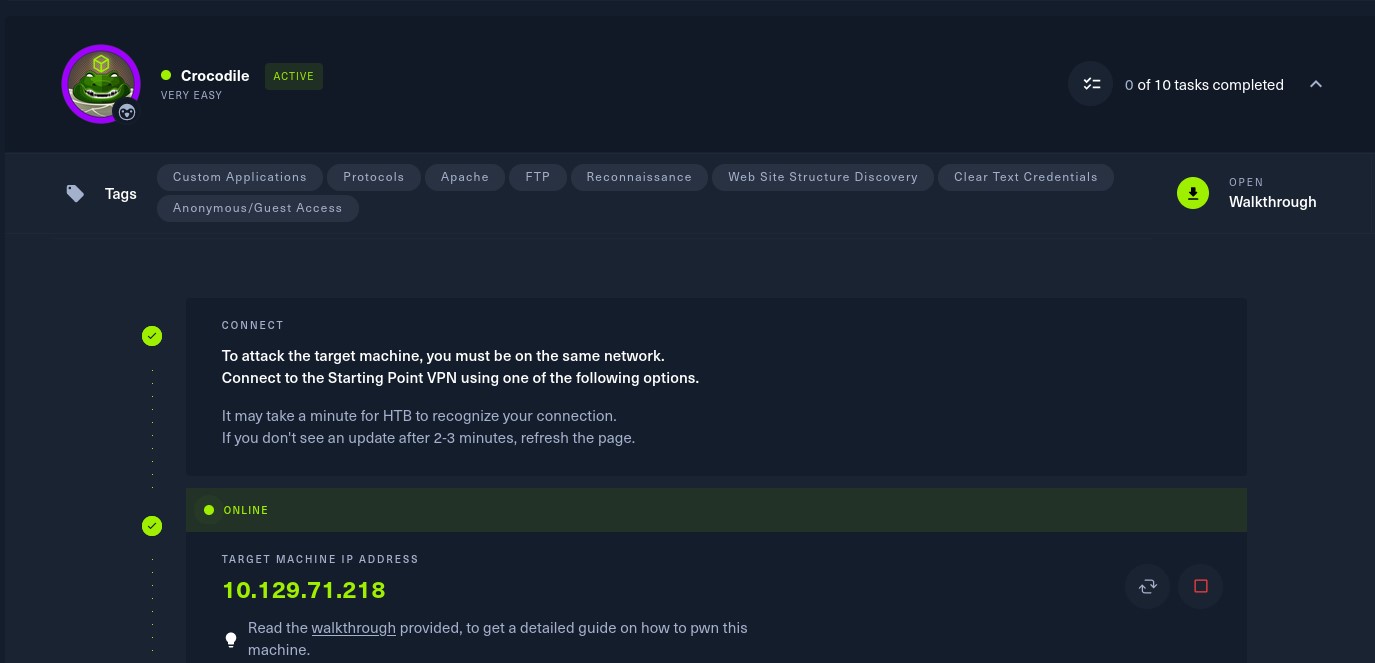
**Tier 1 – Crocodile**



To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:

* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$openvpn starting\_point\_ChaithanyaM4**

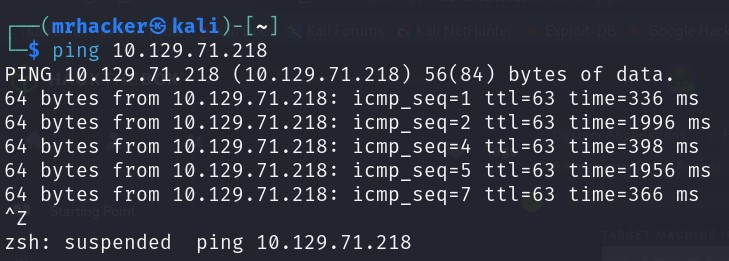
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

Check whether the target machine is active or not. Run the following command to check target machine :

**$ping 10.129.71.218**

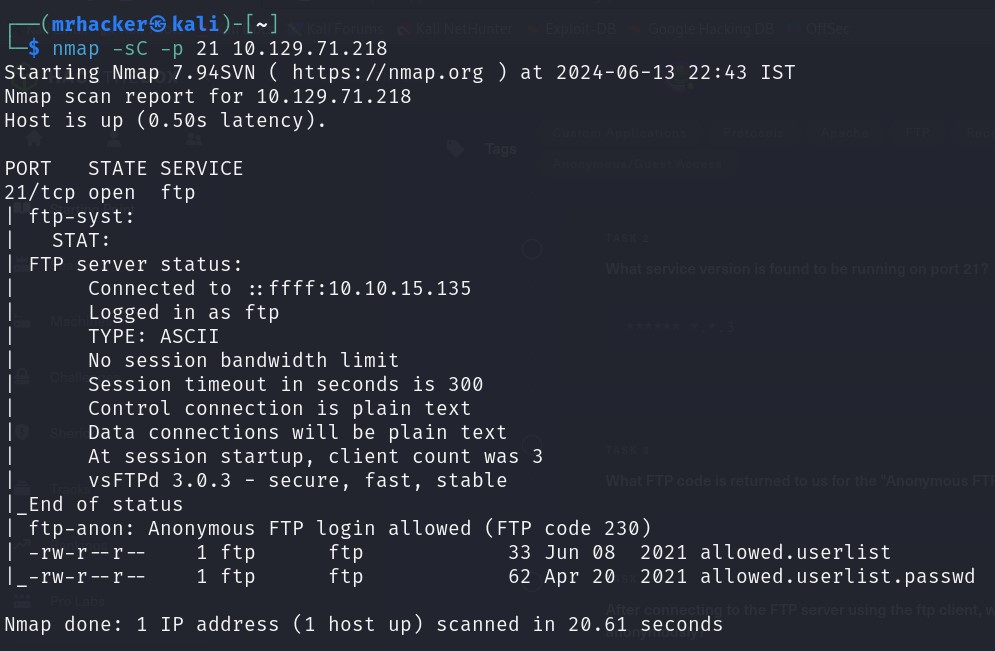


* **Task 1:** **What Nmap scanning switch employs the use of default scripts during a scan?**

-sC

Run the following command to perform nmap scan on target machine:

**$nmap –sC –p 21 10.129.71.218**



* **Task 2:** **What service version is found to be running on port 21?**

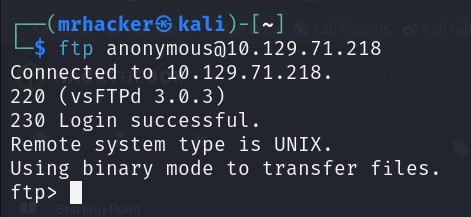
 vsftpd 3.0.3

From the above nmap scan we got the service version of the target machine.

* **Task 3: What FTP code is returned to us for the “Anonymous FTP login allowed” message?**

**230**

**Since ftp port is open, we login anonymously using the username anonymous.Run the following command:**

**$ftp anonymous@10.129.71.218**

* **Task 4:** **After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?**

Anonymous

* **Task 5:** **After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?**

get

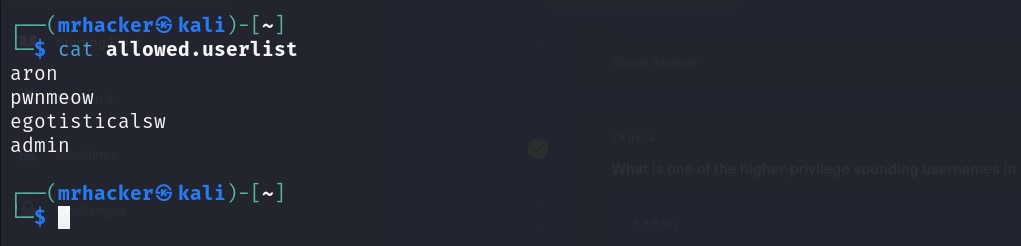
We use “get” command to download the file from FTP server to our local machine:

**>get [filename]**

* **Task 6: What is one of the higher-privilege sounding usernames in ‘allowed.userlist’ that we download from the FTP server?**

**Admin**

**Since we downloaded allowed.userlist to our machine, use “cat” command to display the content in that file:**

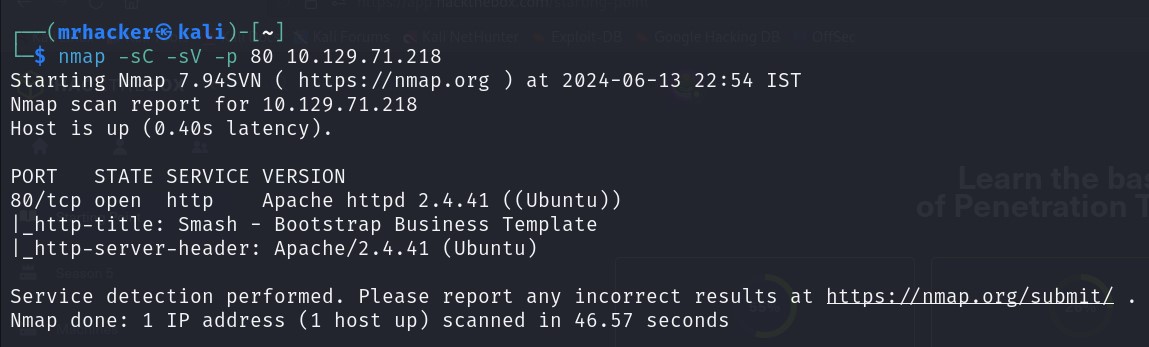
**$cat allowed.userlist**

* **Task 7:** **What version of Apache HTTP Server is running on the target host?**

apache httpd 2.4.41

Run following command to know HTTP server in target machine:

**$nmap –sC –sV –p 80 10.129.71.218**



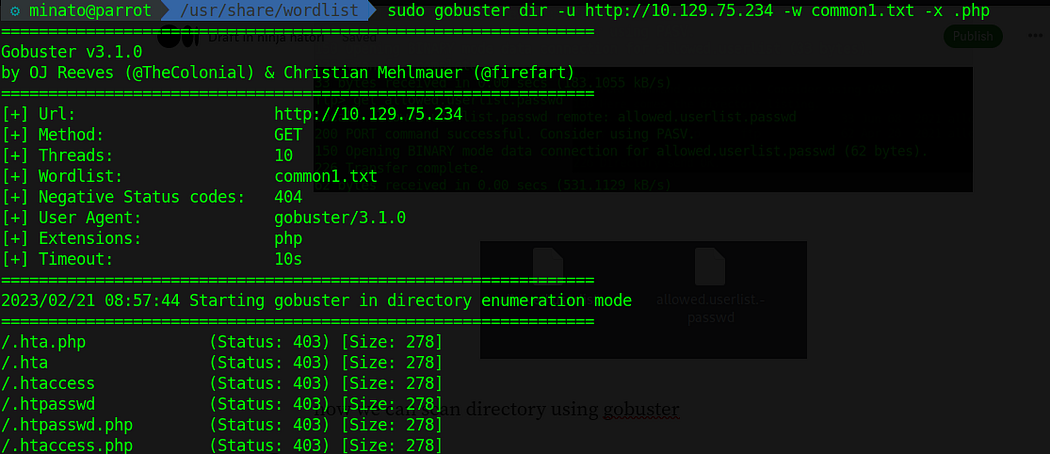
* **Task 8: What switch can we use with Gobuster to specify we are looking for specific filetypes?**

-x

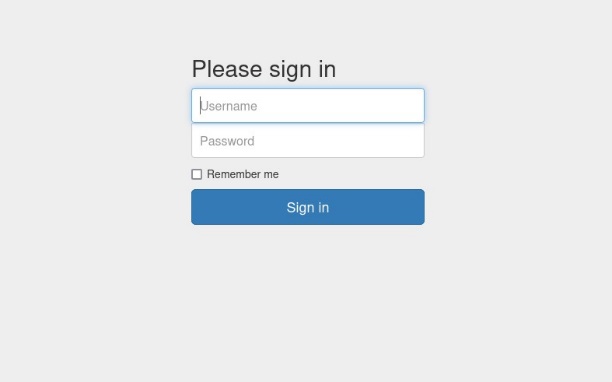
* **Task 9: Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?**

login.php

Scan the directory using durbuster:

**$sudo gobuster dir –u** [**http://10.129.71.218**](http://10.129.71.218) **–w common1.txt .php**

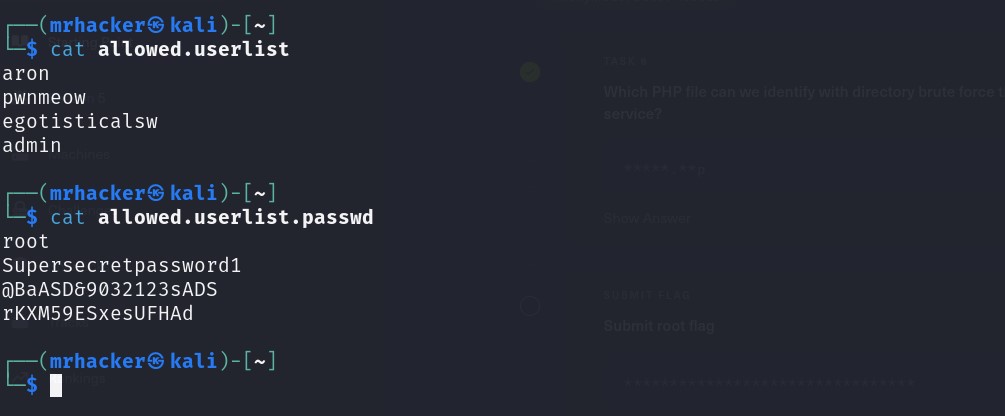
now open <http://10.129.71.218/>login.php in browser and we can try login.



**Submit the flag:**

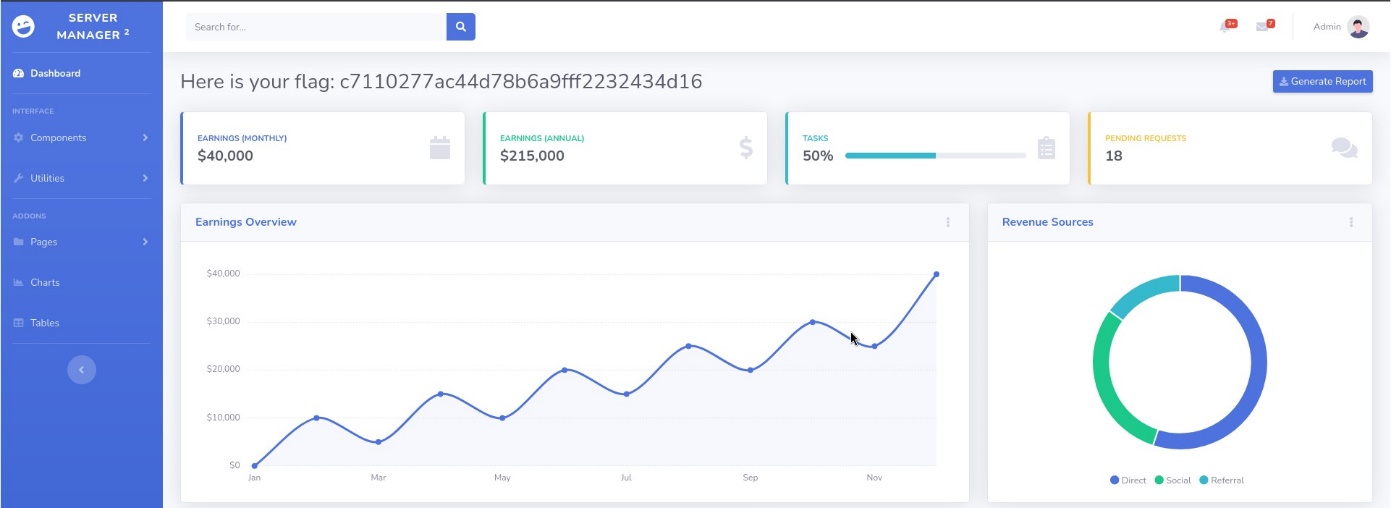
Display the content present in the **allowed.userlist and allowed.userpass file to get the username and password to login into the above browser:**

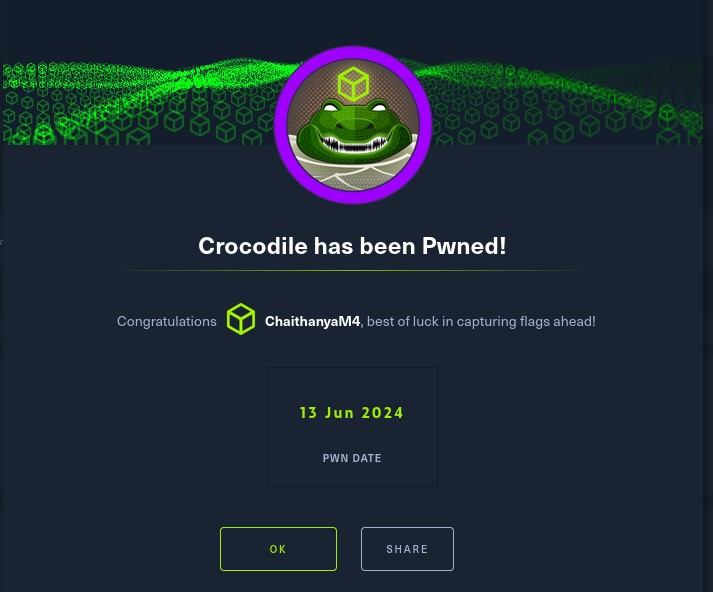
**$cat allowed.userlist**

**$cat allowed.userlist**

Here we found the username: **admin** and password: **rKXM59ESxesUFHAd**

Enter the above username and pawword in login page. Click on “login” , nw we finally logged into the target machine. In this webpage we got the flag.

****

**Finally the machine is pwned!!**