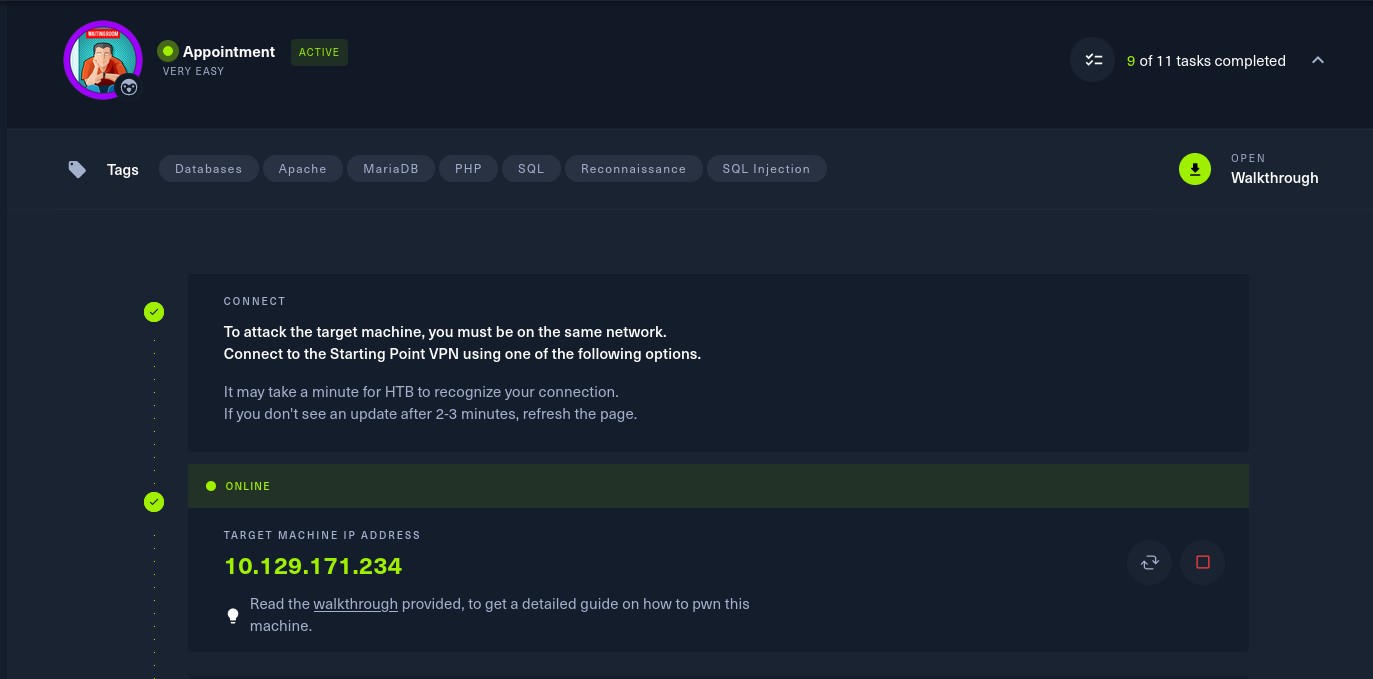
**Tier 1 – Appointment**



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**

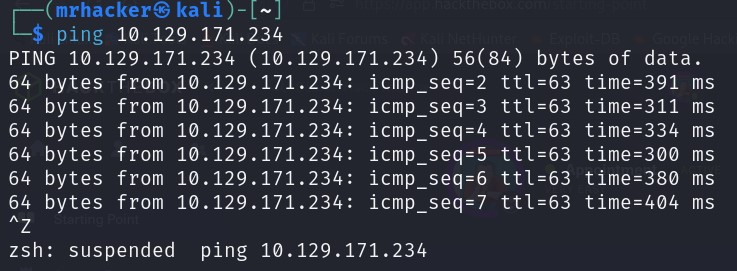
Here we are successfully connected to target network.

**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 up or not. Run the following command to check target machine :

**$ping 10.129.171.234**



* **Task 1:** What does the acronym SQL stand for?

Structured Query Language

* **Task 2:** What is one of the most common type of SQL vulnerabilities?

SQL injection

* **Task 3:** What is the 2021 OWASP Top 10 classification for this vulnerability?

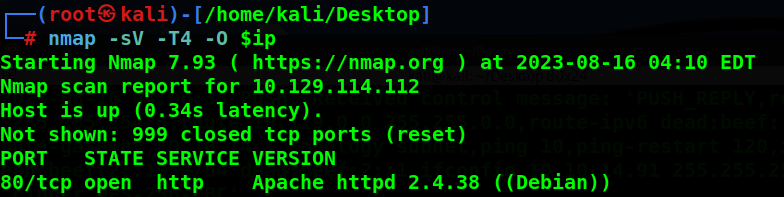
A03:2021-injection

* **Task 4:** What does Nmap report as the service and version that are running on port 80 of the target?

Apache httpd 2.4.38 ((Debian))

Run following for nmap scan:

**$nmap –sV –T4 -O** **10.129.171.234**



* **Task 5:** What is the standard port used for the HTTPS protocol?

443

* **Task 6:** What is the folder called in web-application terminology?

Directory

* **Task 7:** What is the HTTP response code is given for ‘Not found’ error?

404

* **Task 8:** Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we’re looking to discover directories, and not subdomains?

Dir

* **Task 9:** What single character can be used to comment out the rest of a line in MySQL?

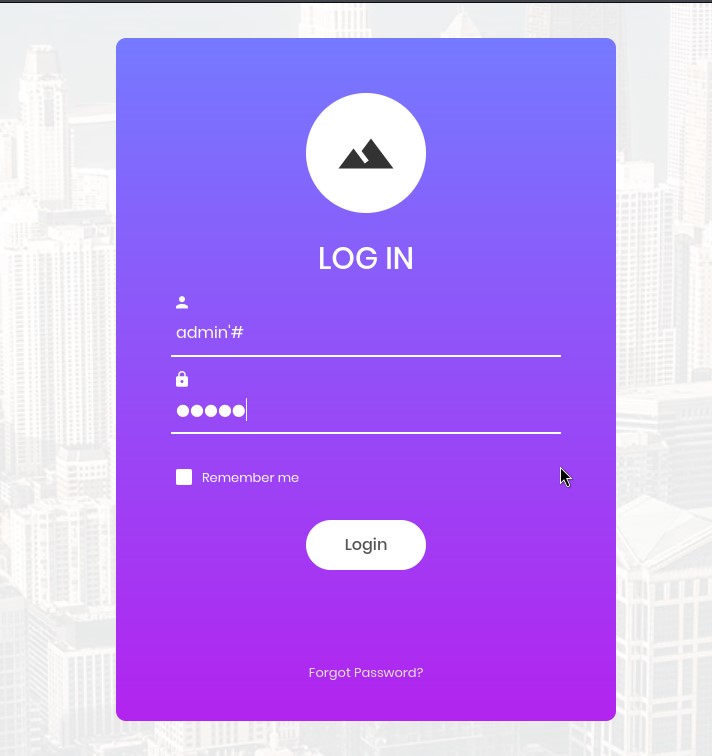
#

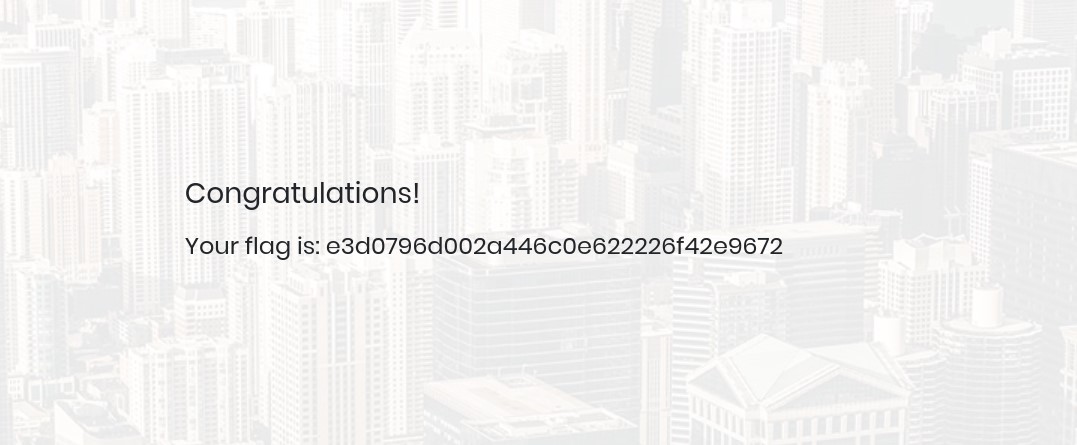
* **Task 10:** If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

Congratulations

Open new tab in fire fox and type “**IP address of target machine**”, Then you will be redirected into the login webpage.

For username type “**admin’#**” and give anything for password. Click on login ,You will successfully login to target machine.



After login, we can see this page.

**Submit the flag:**

Submit the flag displayed in above default webpage. Finally the target machine is pwned!

