**🐱 Meow Lab – Enumeration and Telnet Access**

**Platform**: Hack The Box  
**Focus**: Enumeration, Open Ports Scanning, Telnet Service Access  
**Tools Used**: Nmap, Telnet

**🧠 Introduction – Why Enumeration?**

When beginning any penetration test or security evaluation, the first step is **enumeration**.  
This step is about **gathering information** about the target system and its services.

**🔑 Key Concepts**

* Every server uses **ports** to communicate with clients.
* **Enumeration** discovers which services are running and which might be vulnerable.
* Tools like **Nmap** help automate port scanning and service detection.
* Each service may require a **different tool** or **manual research** to interact with.
* **90% of real-world pentesting is research** – no one knows everything, but skilled testers know how to **look things up** efficiently.

**⚙️ Step 1: Basic Connectivity Check**

**📍 Ping the Target**

First, we check if the target is live:

ping 10.129.63.149

* If it's responsive, stop it with Ctrl + C.

**🔍 Step 2: Nmap Port Scan**

**🛠️ Command Used**

sudo nmap -sV 10.129.63.149

* -sV: Attempts to detect service versions.

**🖥️ Scan Result (Summary)**

PORT STATE SERVICE VERSION

23/tcp open telnet Linux telnetd

* **Port 23 (Telnet)** is open.
* The system is running **Linux telnetd**, indicating a Telnet service is active.

**🔍 Step 3: Understanding Telnet**

**📚 Quick Research – What is Telnet?**

* Telnet is an **older remote management protocol**, operating over **port 23**.
* It allows a user to connect to another host and issue commands **remotely**.
* **Not secure by design** – usually needs **username/password authentication**.

**🧪 Step 4: Accessing Telnet**

**💻 Command Used**

telnet 10.129.63.149

**✅ Response from Target**

Trying 10.129.63.149...

Connected to 10.129.63.149.

Escape character is '^]'.

█ █ ▐▌ ▄█▄ █ ▄▄▄▄

█▄▄█ ▀▀█ █▀▀ ▐▌▄▀ █ █▀█ █▀█ █▌▄█ ▄▀▀▄ ▀▄▀

█ █ █▄█ █▄▄ ▐█▀▄ █ █ █ █▄▄ █▌▄█ ▀▄▄▀ █▀█

Meow login:

**🔐 Observation**

* Banner shows **Hack The Box (HTB)** logo.
* A **login prompt** indicates **authentication is required**.
* Since no other ports are open, we need **valid credentials** to proceed.

**📝 Summary**

| **Phase** | **Tool** | **Command/Action** | **Purpose** |
| --- | --- | --- | --- |
| Connectivity | ping | ping 10.129.63.149 | Check if host is alive |
| Port Scanning | nmap | sudo nmap -sV 10.129.63.149 | Detect open ports and services |
| Service Review | telnet | Manual research | Understand port 23 (Telnet) |
| Manual Access | telnet | telnet 10.129.63.149 | Try connecting to Telnet |
| Barrier | - | Login prompt | Need credentials to proceed |

**🔐 Step 5: Attempting Login via Telnet**

After identifying an open Telnet service, the next logical step is **authentication attempts**. In this lab, we manually tried some **default usernames**.

**🛠️ Commands & Output**

telnet 10.129.63.149

**Connection Established**  
Received HTB banner → Prompted for credentials.

**Tried Usernames:**

Meow login: admin

Password:

> Login incorrect

Meow login: administrator

Password:

> Login incorrect

Meow login: root

✅ **Success with root (no password required)**  
System granted access with a welcome message and shell.

**💡 Real-World Tip**

🔑 Always try **default or weak credentials** on old or legacy services like Telnet, FTP, or MySQL.

In real scenarios, you'll need **automated tools** (like hydra, ncrack, or custom scripts) to brute-force or fuzz valid credential pairs from wordlists.

You could write a brute-force loop like:

for user in admin administrator root test guest; do

echo Trying $user...

# Manual or expect script for automation

done

**🖥️ Step 6: Exploring System After Login**

Once logged in, we get **root access** – indicating no password was required for root.

Welcome to Ubuntu 20.04.2 LTS

**🧭 Basic Commands Used**

root@Meow:~# ls

flag.txt snap

root@Meow:~# cat flag.txt

b40abdfe23665f766f9c61ecba8a4c19

✅ **Captured Flag**: b40abdfe23665f766f9c61ecba8a4c19

**🎯 Lab Goal vs Real-World Actions**

| **Lab Scenario** | **Real-World Equivalent** |
| --- | --- |
| Capture flag from root directory | Identify and extract sensitive files |
| Telnet login with root (no password) | Default or weak credential exploitation |
| cat flag.txt | Inspect .ssh, .bash\_history, passwd, logs, etc. |

**🔍 Real Files to Look for in Live Pentests:**

* .ssh/ (keys)
* /etc/passwd and /etc/shadow
* config.php, .env, or credential files
* Database dumps or customer records

**📘 Summary**

| **Action** | **Command / Output** | **Result** |
| --- | --- | --- |
| Telnet to target | telnet 10.129.63.149 | Connected to service |
| Login as admin | Login incorrect | ❌ |
| Login as administrator | Login incorrect | ❌ |
| Login as root | Shell granted | ✅ Got root shell |
| List files | ls | Found flag.txt |
| Read flag | cat flag.txt | Captured: b40abdfe23665f766f9c61ecba8a4c19 |

**🔚 Final Thoughts**

* 🧠 **Persistence pays off** – trial-and-error worked in this lab, but in real cases, enumeration and brute force automation will be key.
* 📚 **Practice default credentials** – for Telnet, FTP, MySQL, and more.
* 🧰 **Post-access enumeration** is just as important – go beyond flags, find real data.