

HTB Meow – CTF Report

Introduction

The *Meow* machine on Hack The Box is an introductory-level CTF designed to help users familiarize themselves with basic reconnaissance and service exploitation. This report outlines the enumeration and exploitation process, followed by direct answers to specific assessment questions.

Enumeration and Access

Upon scanning the target machine, it was observed that **Telnet** was running on **port 23** — a known insecure and outdated protocol. Connecting to the service presented a login prompt. Using the username **root**, access was granted **without requiring a password**.

This indicates a severe security misconfiguration: a remote service offering root access with no authentication over an unencrypted channel.

Flag Retrieval

After logging in as root, the **flag.txt** file was located in the root user's home directory. Reading this file revealed the final flag string required to complete the challenge.

Answers to Assessment Questions

1. **What is the name of the vulnerable service running on the target system?**
telnet
2. **What is the port number the service is running on?**
23
3. **What is the username used to gain access to the system?**
root

The screenshot shows a digital interface with a dark background and light-colored boxes for each task. Each task box contains a question, a text input field with a placeholder, a 'Show Answer' button, and a refresh icon.

- TASK 1**
What does the acronym VM stand for?
*****e
Show Answer
- TASK 2**
What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.
*****l
Show Answer
- TASK 3**
What service do we use to form our VPN connection into HTB labs?
*****n
Show Answer
- TASK 4**
What tool do we use to test our connection to the target with an ICMP echo request?
***g
Show Answer

4. Was a password required to access the system?

No

The screenshot shows a digital interface with a dark background and light-colored boxes for each task. Each task box contains a question, a text input field with a placeholder, a 'Hide Answer' button, and a refresh icon.

- nmap**
Hide Answer
- TASK 6**
What service do we identify on port 23/tcp during our scans?
*****t
telnet
Hide Answer
- TASK 7**
What username is able to log into the target over telnet with a blank password?
***t
root
Hide Answer
- SUBMIT FLAG**
Submit root flag

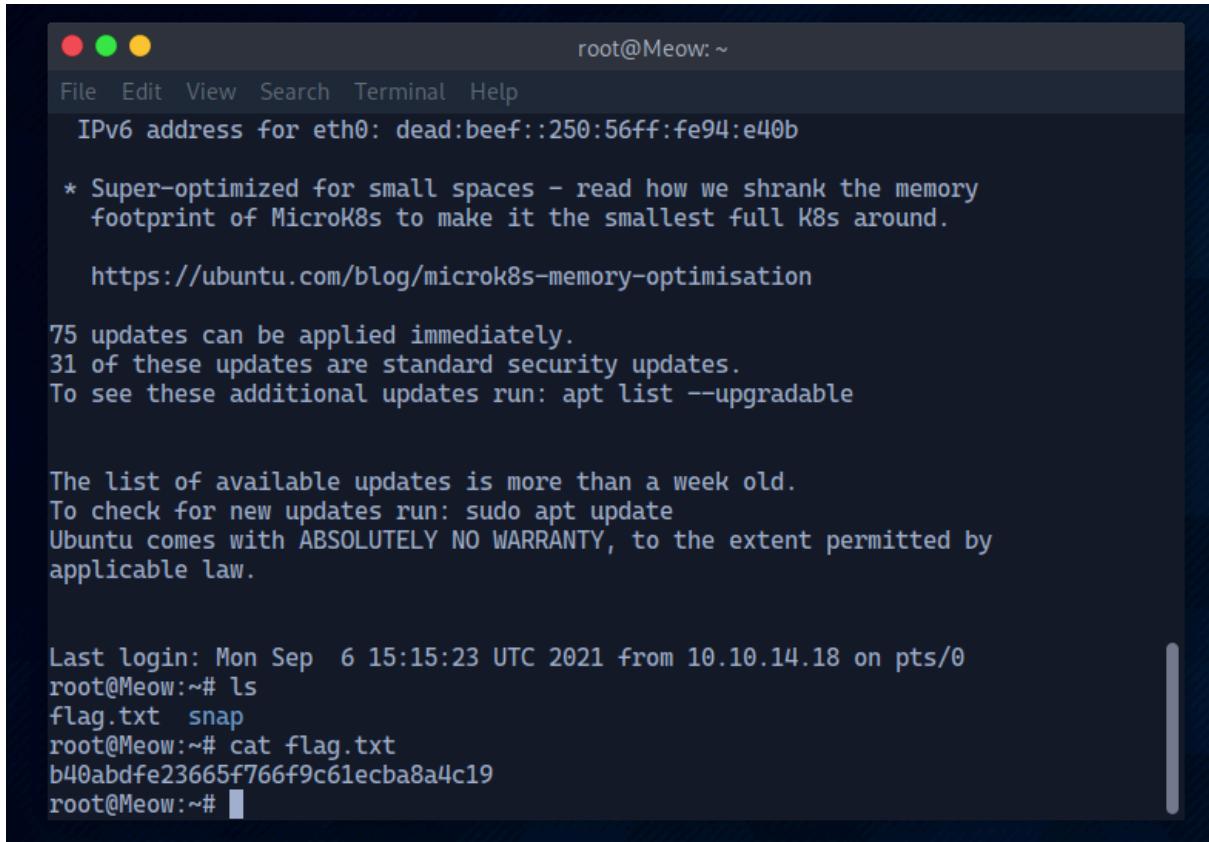
b40abdf23665f766f9c61ecba8a4c19
Hide Answer

5. What file contains the final flag on the target system?

flag.txt

6. What is the flag value retrieved from the target system?

b40abdf23665f766f9c61ecba8a4c19



The screenshot shows a terminal window with a dark theme. At the top, there's a header bar with three colored dots (red, green, yellow) on the left and the text "root@Meow: ~" on the right. Below the header is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal shows the following output:

```
IPv6 address for eth0: dead:beef::250:56ff:fe94:e40b
* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.
  https://ubuntu.com/blog/microk8s-memory-optimisation
75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdf23665f766f9c61ecba8a4c19
root@Meow:~#
```

7. What was the main vulnerability that allowed access to the system?

Misconfigured Telnet service allowing root login without a password

Conclusion

The Meow machine serves as a practical example of how legacy services and weak authentication policies can create critical security risks. The exercise reinforces key foundational skills: scanning, identifying services, and testing for common misconfigurations.

