Lab 1: HTB Starting Point Machines

Machine 2: Fawn

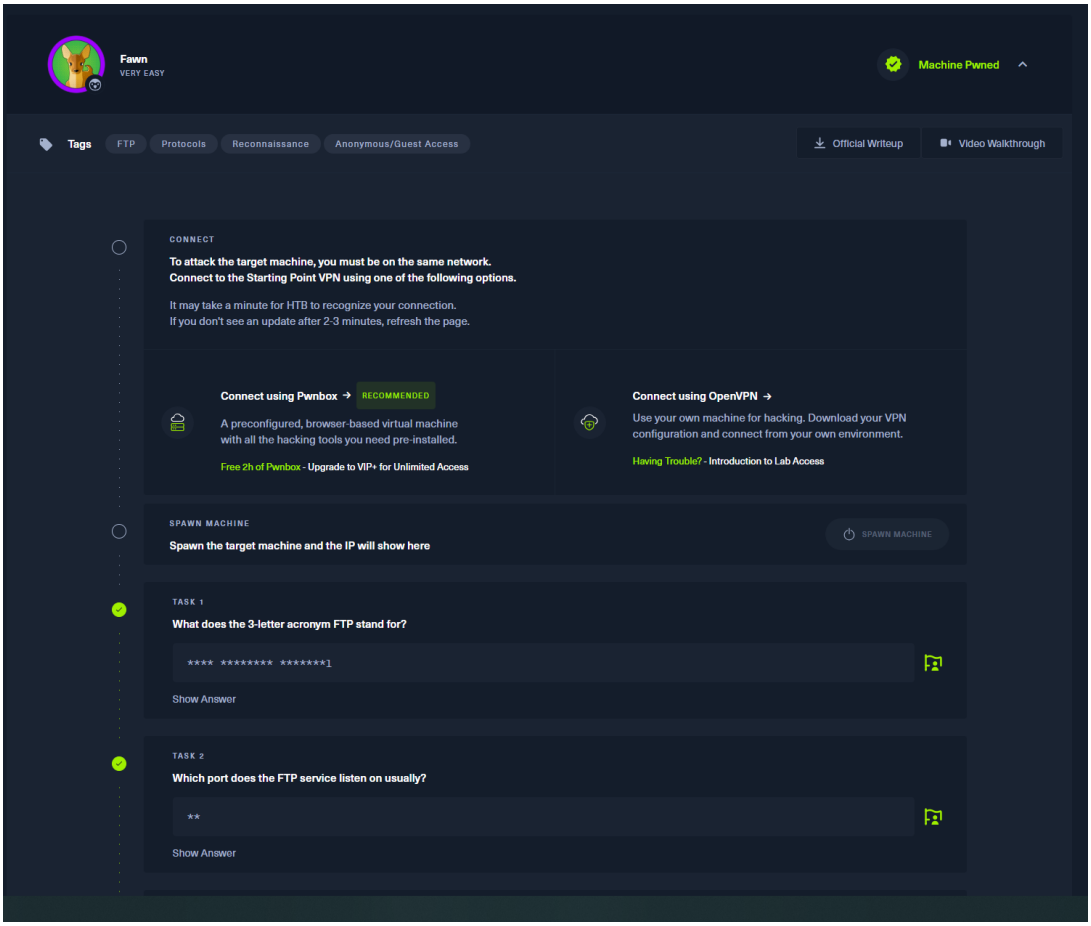
Technical Details:

- Open Ports: 21 (FTP)
- Service: vsftpd 3.0.3
- Vulnerability: Anonymous FTP login enabled

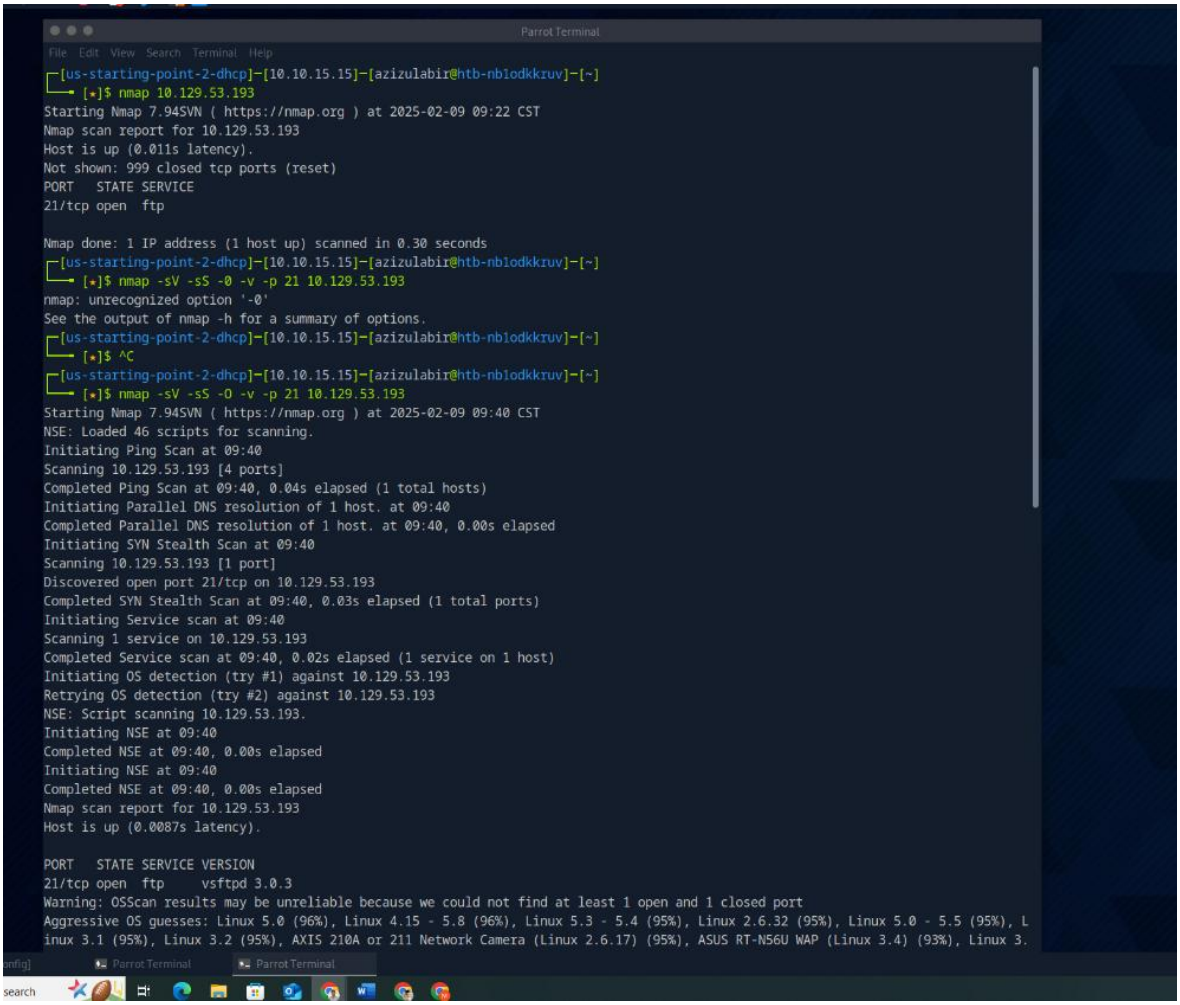
Network connectivity was verified using the **ping** command. An **Nmap** scan was conducted to identify open ports, revealing that the FTP service was running on **port 21**.

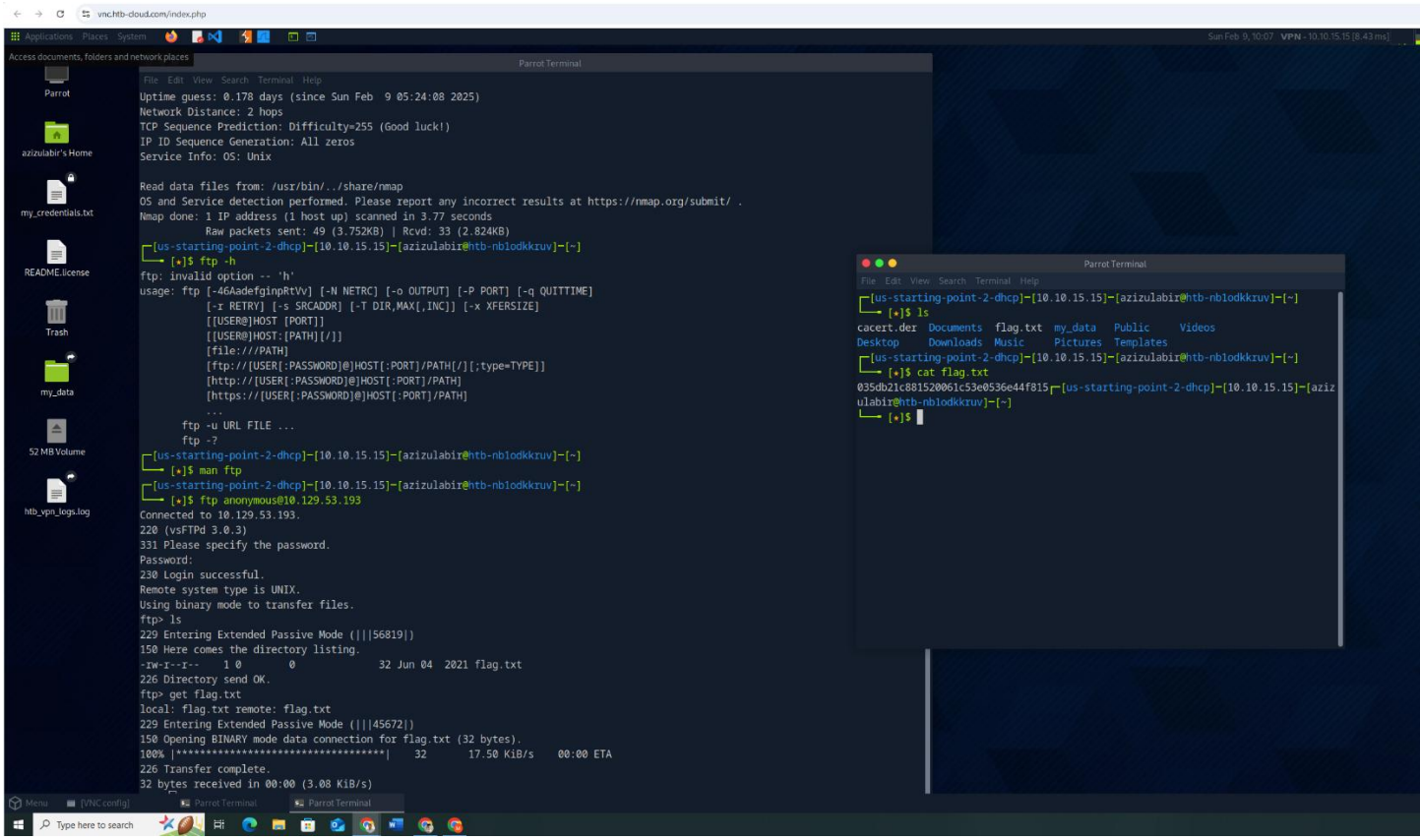
Anonymous login access was found to be enabled on the FTP service, allowing unauthorized entry. The **ls** command was used to enumerate the contents of the directory, leading to the discovery of the **flag.txt** file. The **get** command was executed to retrieve the flag, successfully completing the task.

Screenshot of the machine:



Screenshot showing the retrieved flag:




vnc.htb-cloud.com/index.php
Applications Places System
Sun Feb 9, 10:07 VPN - 10.10.15.15 [8.43 ms]
Access documents, folders and network places
Parrot
azizulabir's Home
my_credentials.txt
README.license
Trash
my_data
52 MB Volume
htb_vpn_logs.log
Parrot Terminal
File Edit View Search Terminal Help
Uptime guess: 0.178 days (since Sun Feb 9 05:24:08 2025)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.77 seconds
Raw packets sent: 49 (3.752KB) | Rcvd: 33 (2.824KB)
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$ ftp -h
ftp: invalid option -- 'h'
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
[[USER@]HOST [PORT]]
[[USER@]HOST:[PATH][/]]
[file:///PATH]
[ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
[http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
[https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
...
ftp -u URL FILE ...
ftp -?
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$ man ftp
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$ ftp anonymous@10.129.53.193
Connected to 10.129.53.193.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||56819|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||45672|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |**********| 32 17.50 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (3.08 KiB/s)
Parrot Terminal
File Edit View Search Terminal Help
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$ ls
cacert.der Documents flag.txt my_data Public Videos
Desktop Downloads Music Pictures Templates
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$ cat flag.txt
035db21c881520061c53e0536e44f815[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[*]$
Menu [VNC config] Parrot Terminal Parrot Terminal
Type here to search

Machine 3: Dancing

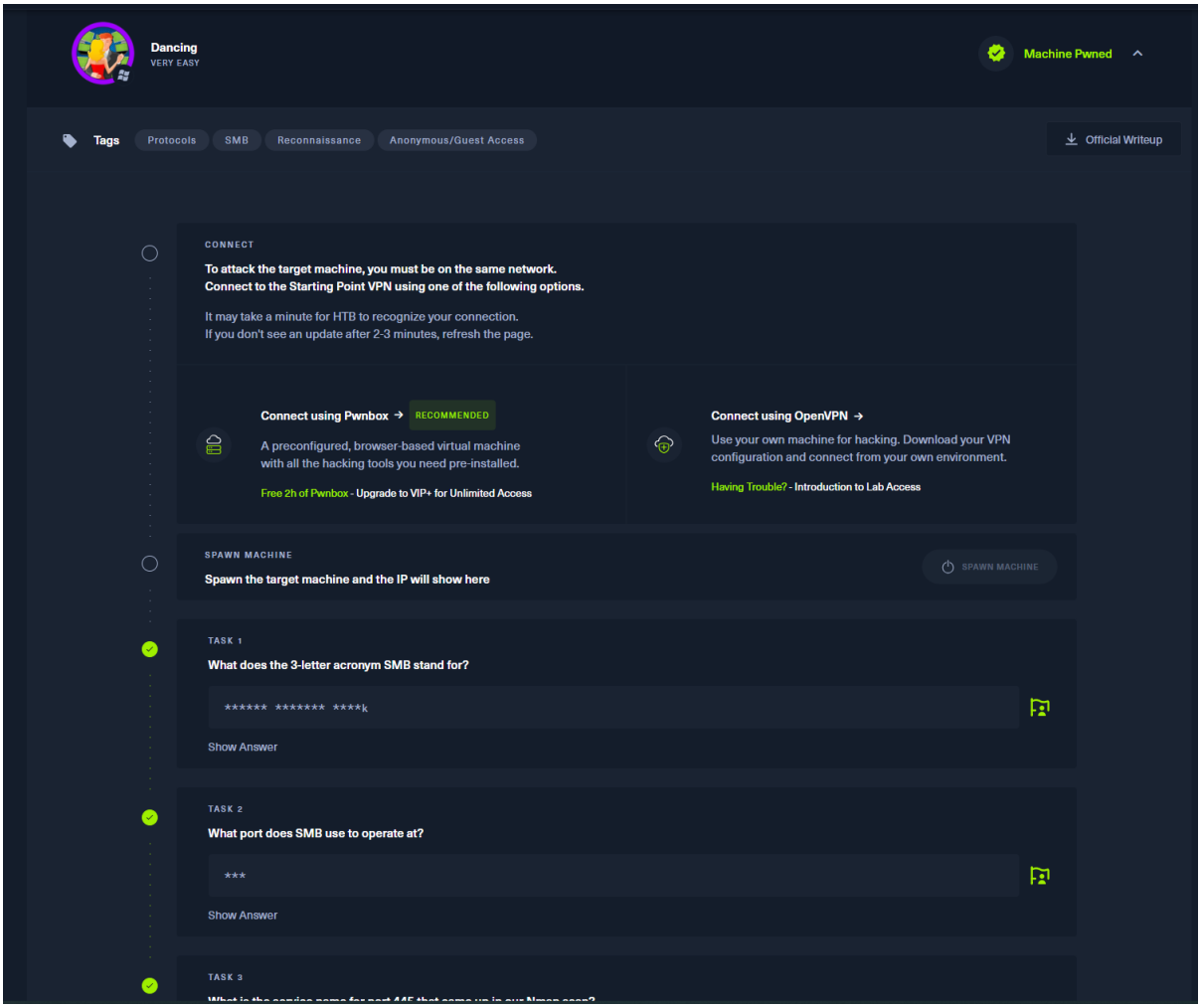
Technical Details:

- Open Ports: 445 (SMB)
- Service: Microsoft SMB (NetBIOS & Microsoft-ds)
- Vulnerability: Anonymous SMB access enabled

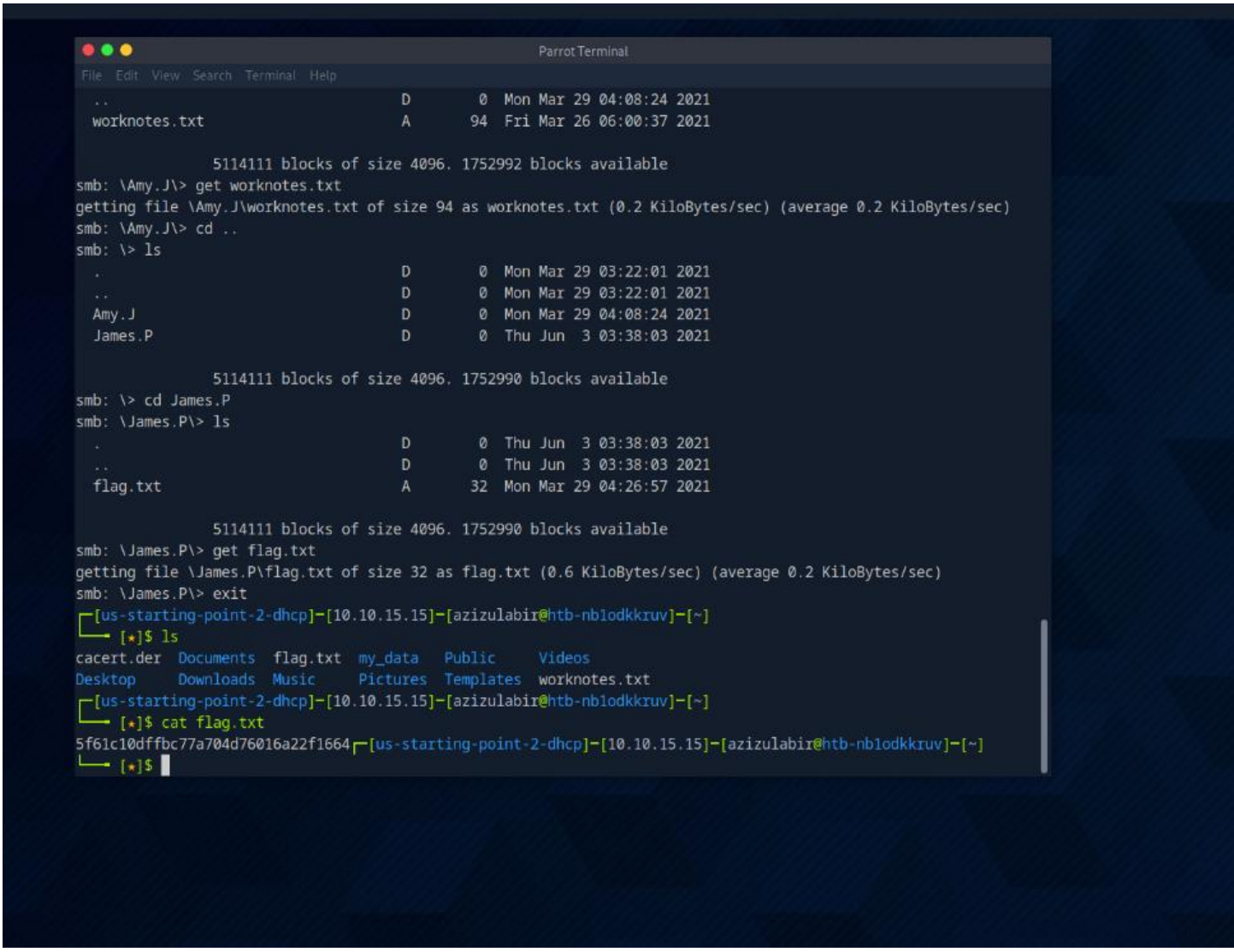
A connectivity check was performed using the **ping** command, confirming that the victim machine was reachable. An **nmap** scan revealed that the SMB service was running on **port 445**, identified as **Microsoft SMB (NetBIOS & Microsoft-ds)**.

Anonymous access was found to be enabled on the SMB service. Exploiting this misconfiguration, the smbclient tool was used to list available shares. The **ls** command was then used to enumerate shared files, leading to the discovery of the **flag.txt** file. The **get** command was executed to retrieve the flag, marking the completion of the task.

<u>Screenshot of the machine:</u>



Screenshot showing the retrieved flag:



Machine 4: Redeemer

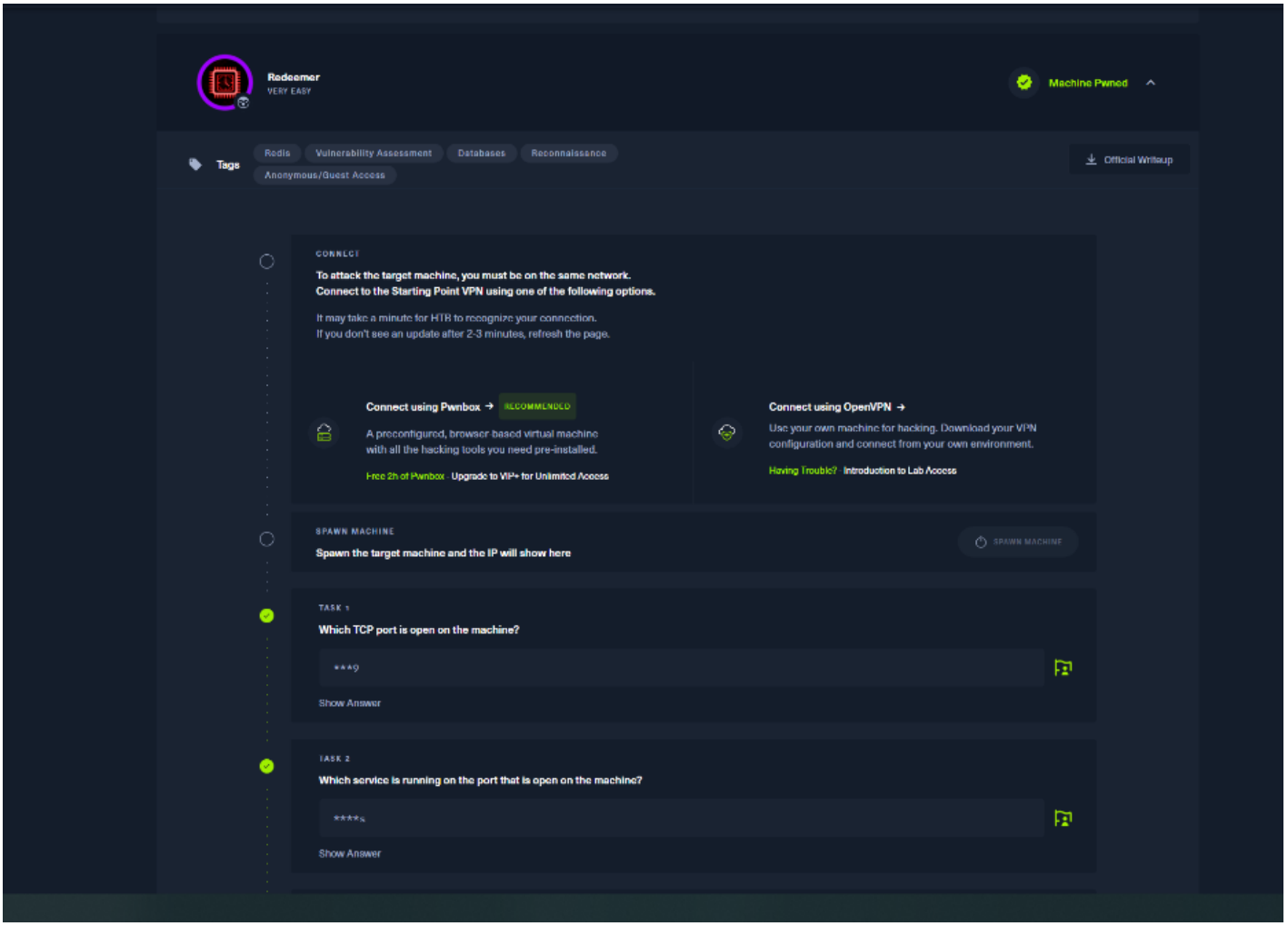
Technical Details:

- Open Ports: 6379 (Redis)
- Service: Redis key-value store
- Vulnerability: Unsecured Redis instance

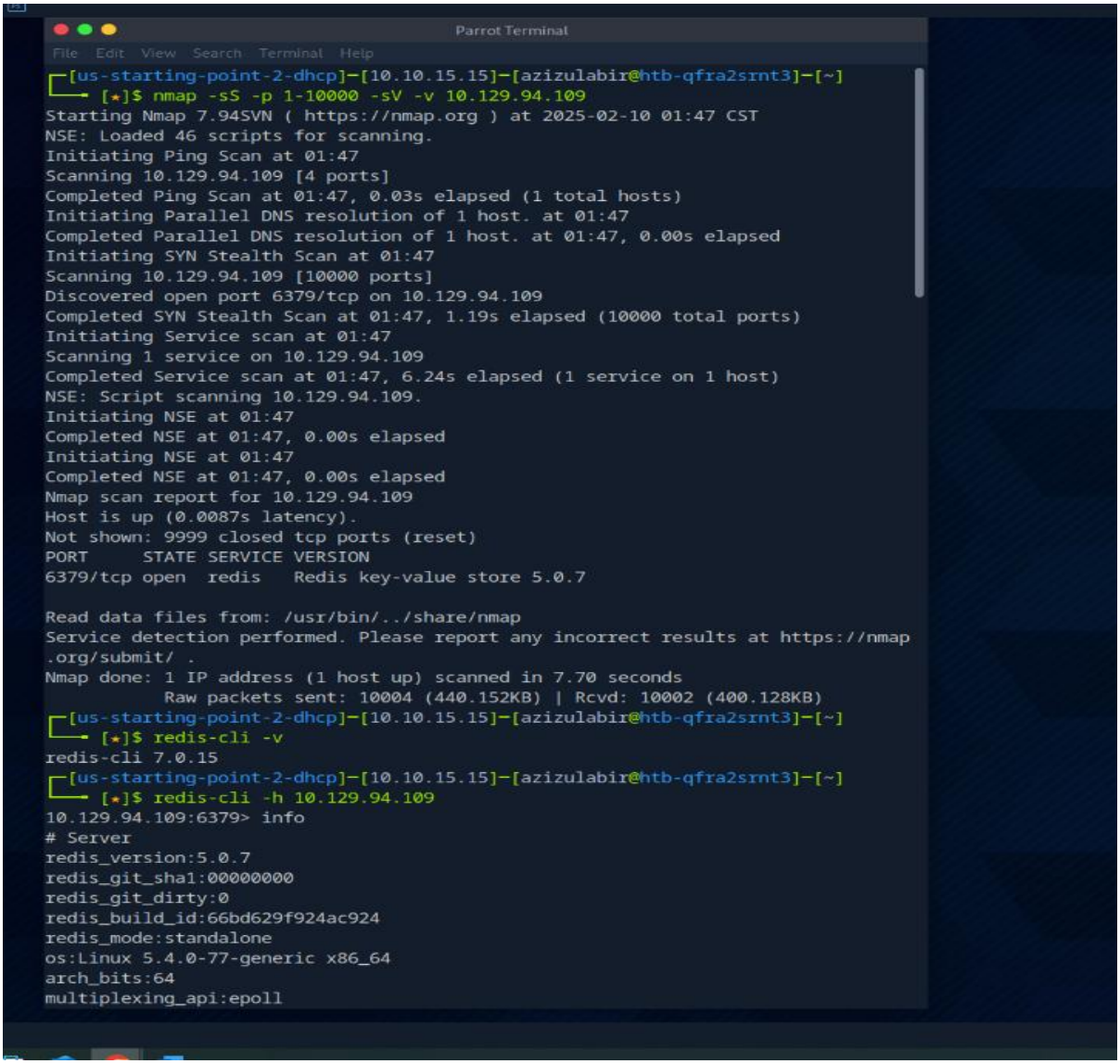
The **ping** command was used to ensure network connectivity. An **Nmap** scan was performed, which detected that the Redis service was running on **port 6379**.

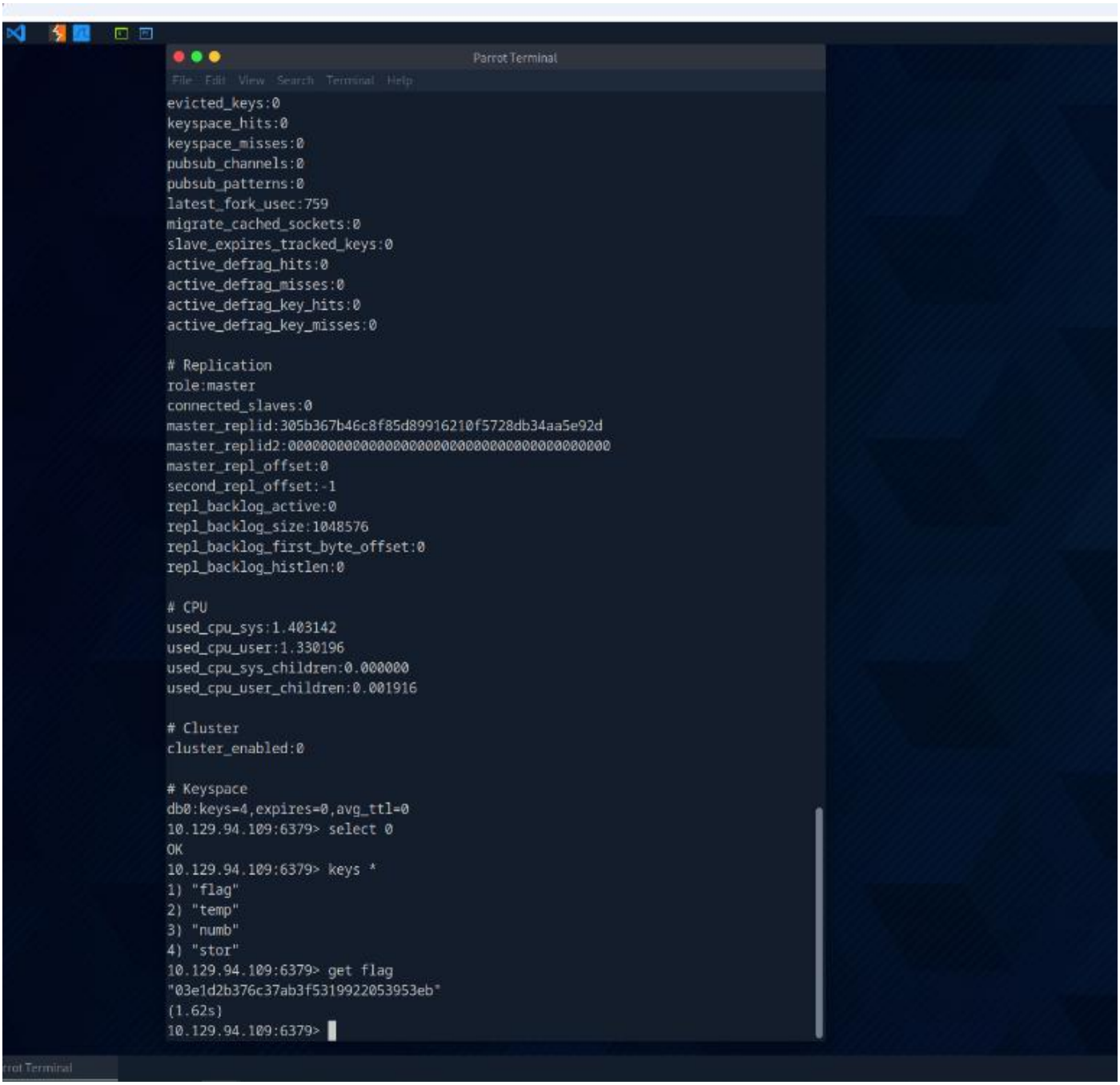
Unauthenticated access to the Redis instance was identified. Using the **KEYS *** command, all available keys were listed, revealing a key containing the flag. The **GET** command was executed to extract the flag, successfully concluding the test.

<u>Screenshot of the machine.</u>



Screenshot showing the retrieved flag:





Conclusion:

The three machines demonstrated vulnerabilities in FTP anonymous access, SMB file-sharing permissions, and unsecured Redis instances. These findings highlight the importance of disabling unnecessary services, enforcing strong authentication, and securing network shares to prevent unauthorized access.