MEOW

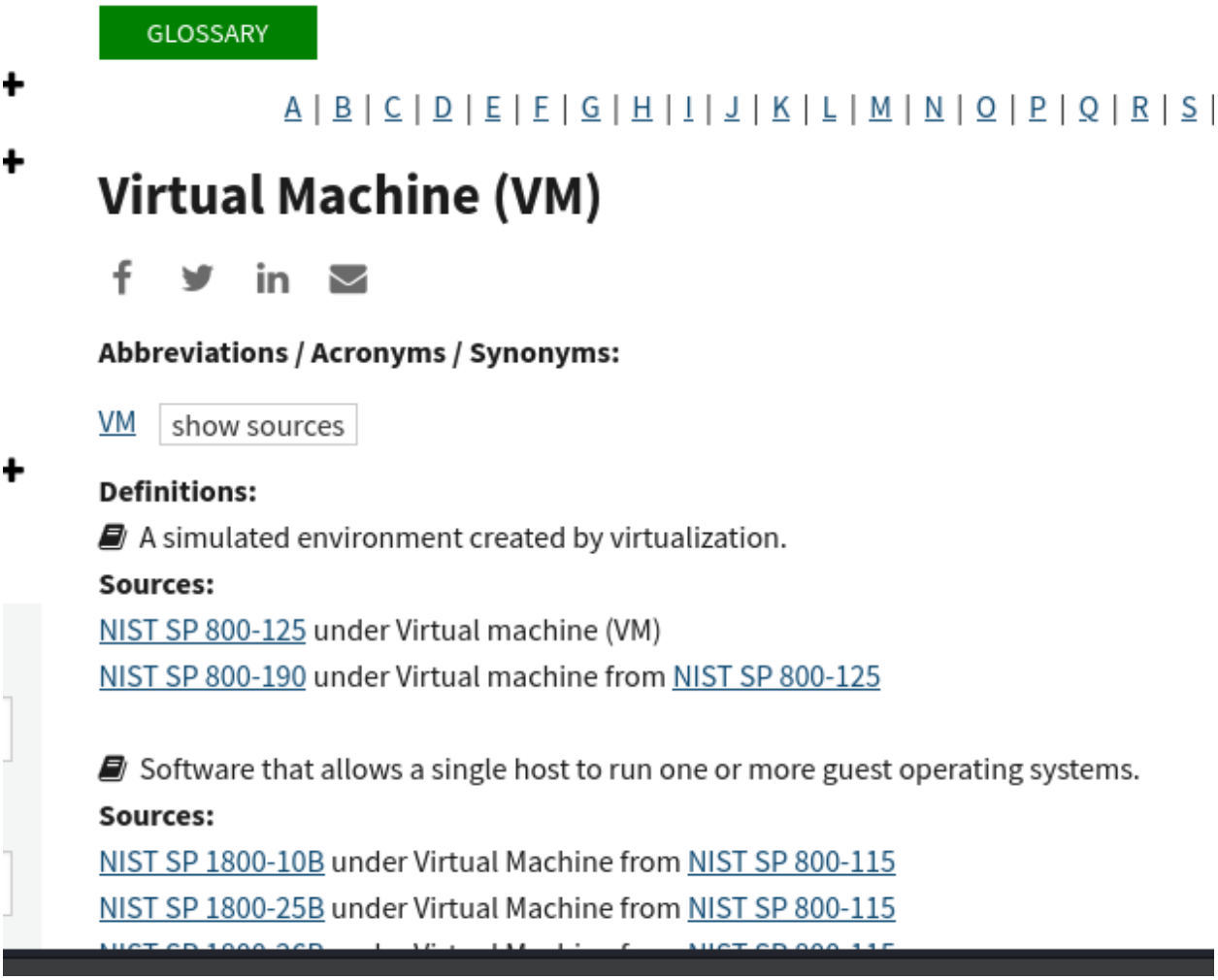
Introduction

This report documents the findings and activities conducted during a series of tasks in a Hack the Box meow lab environment. The objective was to understand and apply basic concepts of network security and penetration testing.

Tasks and Findings

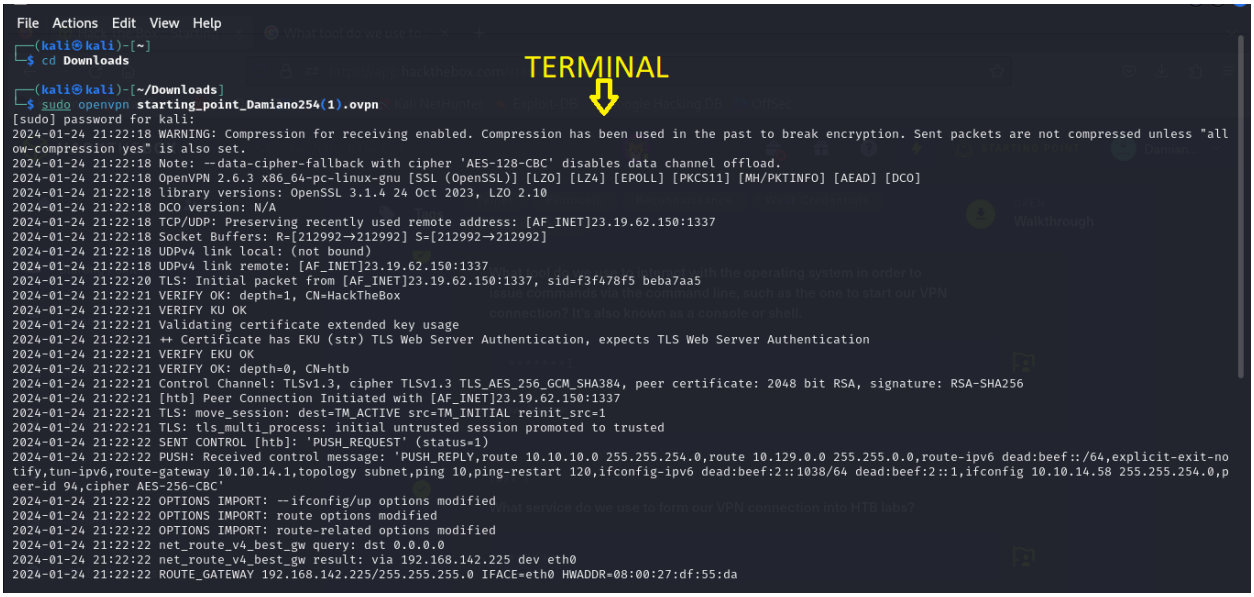
Task 1: Understanding Basic Concepts

- **Question:** What does the acronym VM stand for?
- **Answer:** Virtual Machine
- **Details:** A Virtual Machine (VM) is an emulation of a computer system, providing the functionality of a physical computer.



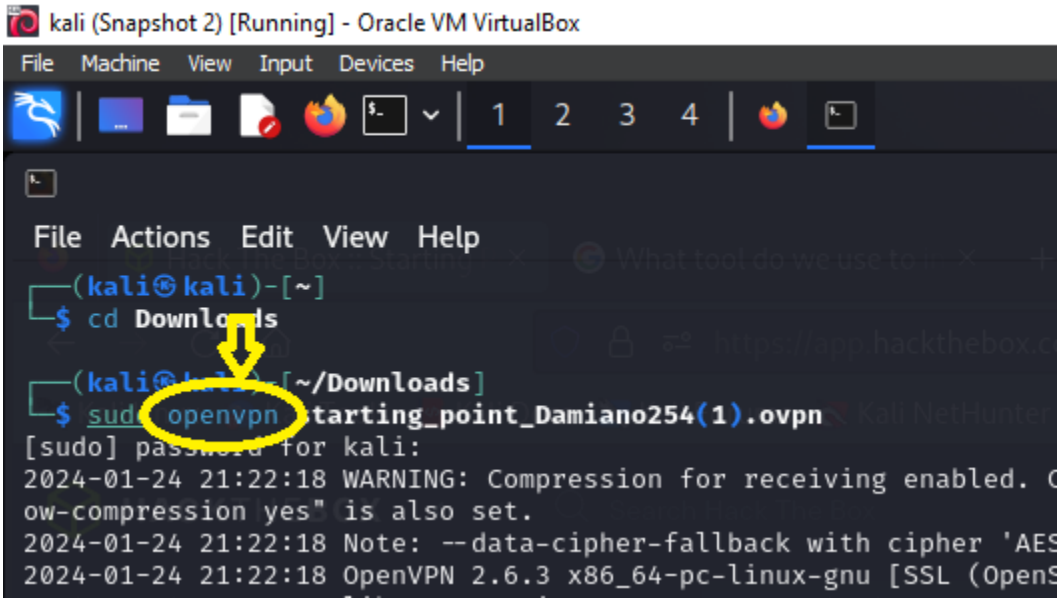
Task 2: Command Line Interaction

- **Question:** What tool is used to interact with the operating system to issue commands via the command line?
- **Answer:** Terminal
- **Details:** The terminal, also known as a console or shell, is a text-based interface used to run commands on the operating system.



Task 3: VPN Connection

- **Question:** What service is used to form a VPN connection into HTB labs?
- **Answer:** OpenVPN
- **Details:** OpenVPN is a tool for creating secure point-to-point or site-to-site connections in routed or bridged configurations.

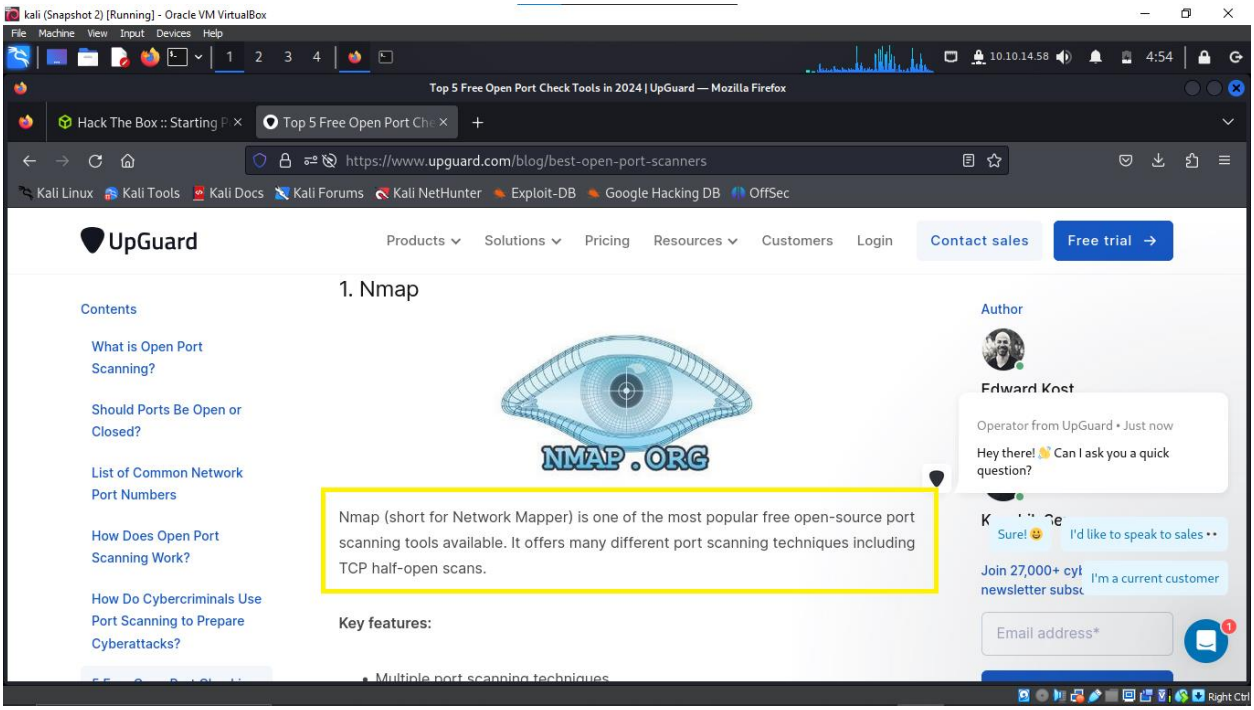


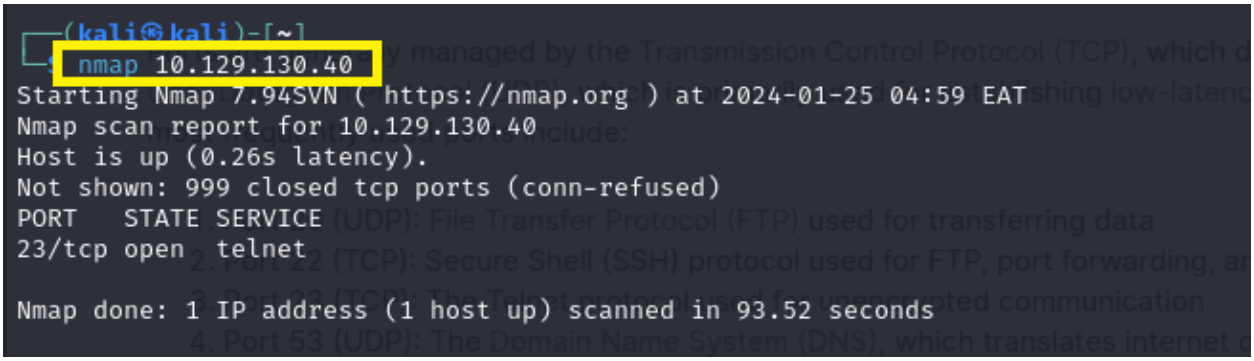
Task 4: Testing Network Connection

- **Question:** What tool is used to test the connection to the target with an ICMP echo request?
- **Answer:** Ping
- **Details:** Ping is a diagnostic tool used to test the reachability of a host on an Internet Protocol (IP) network.

Task 5: Port Scanning

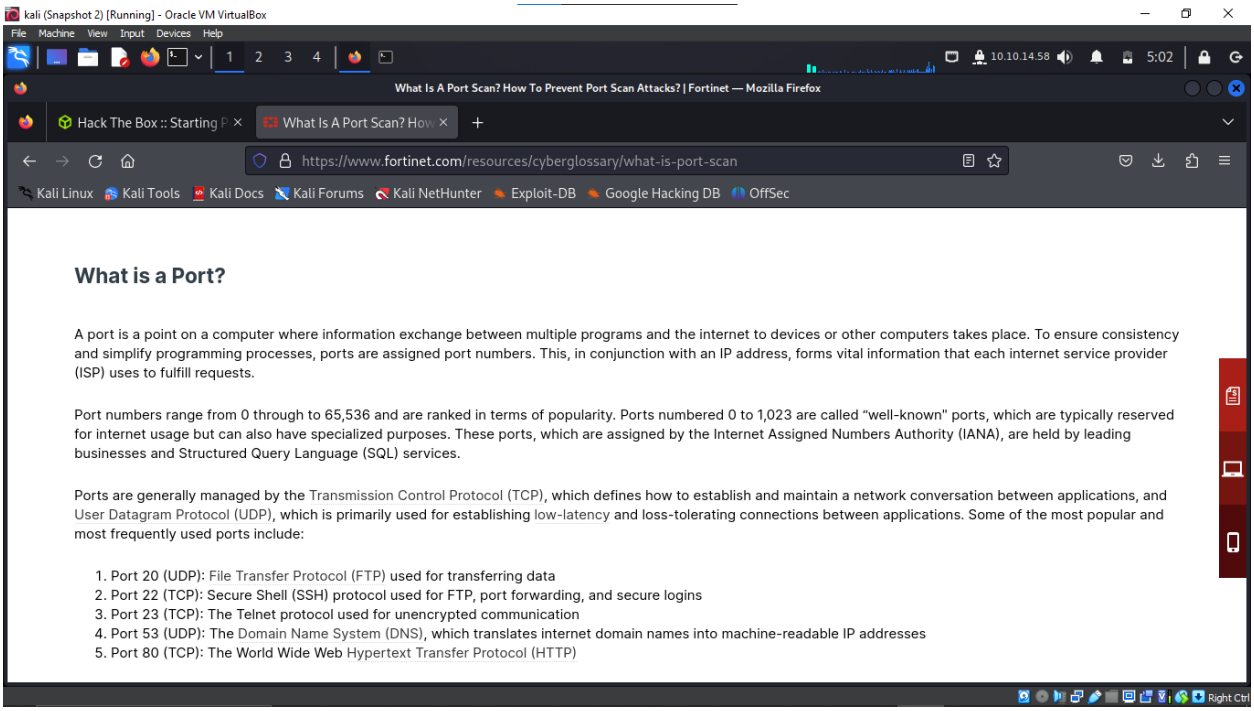
- **Question:** What is the most common tool for finding open ports on a target?
- **Answer:** Nmap
- **Details:** Nmap is a network scanning tool used to discover hosts and services on a computer network by sending packets and analyzing responses.

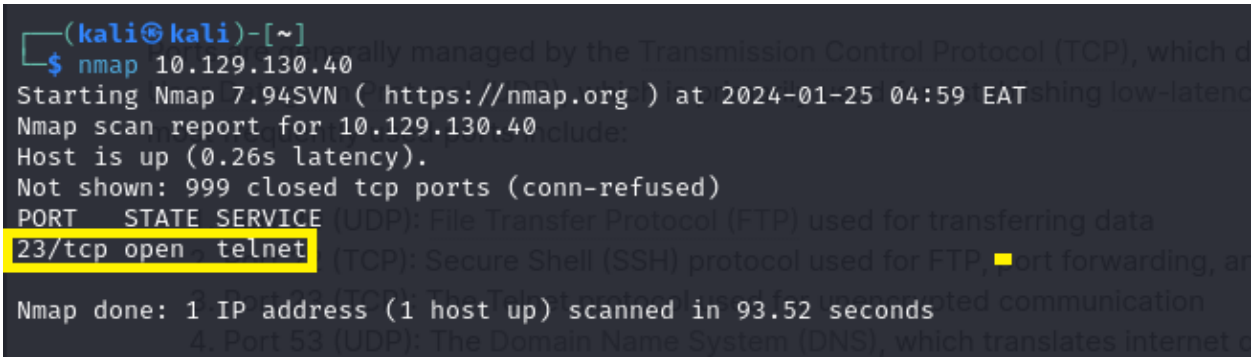




Task 6: Identifying Services

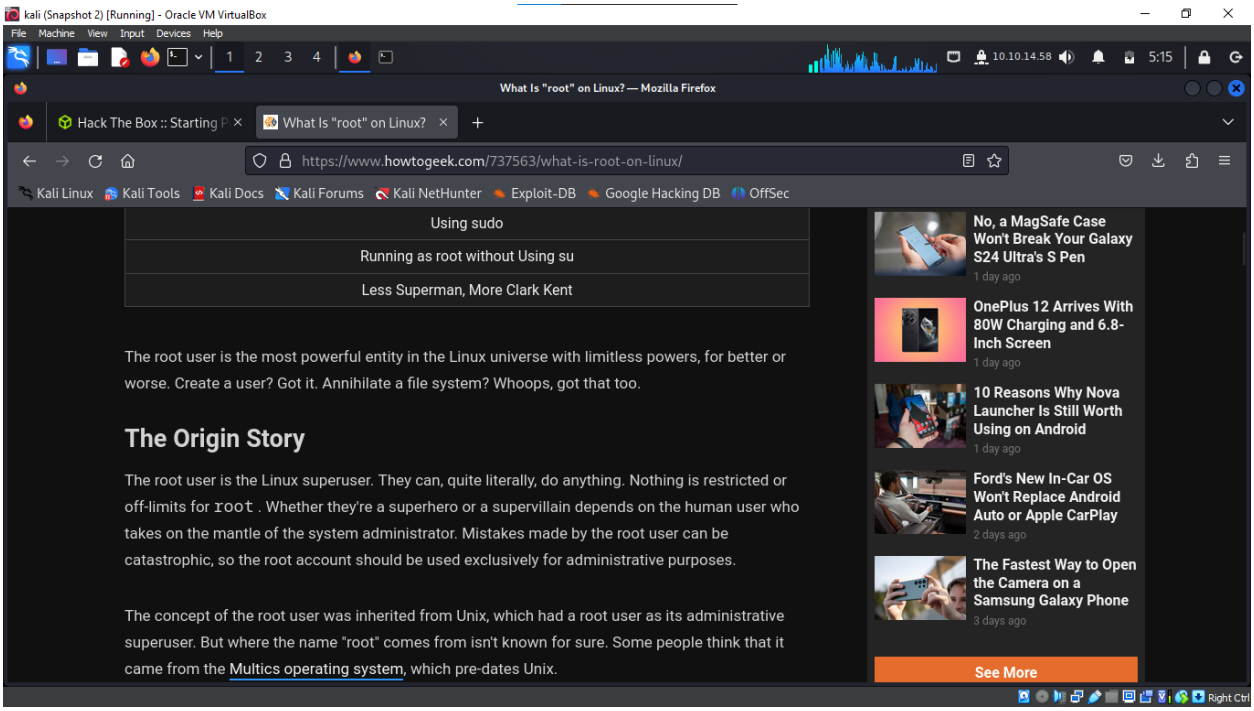
- **Question:** What service was identified on port 23/tcp during scans?
- **Answer:** Telnet
- **Details:** Telnet is a network protocol used on the internet or local area networks to provide a bidirectional interactive text-oriented communication facility.

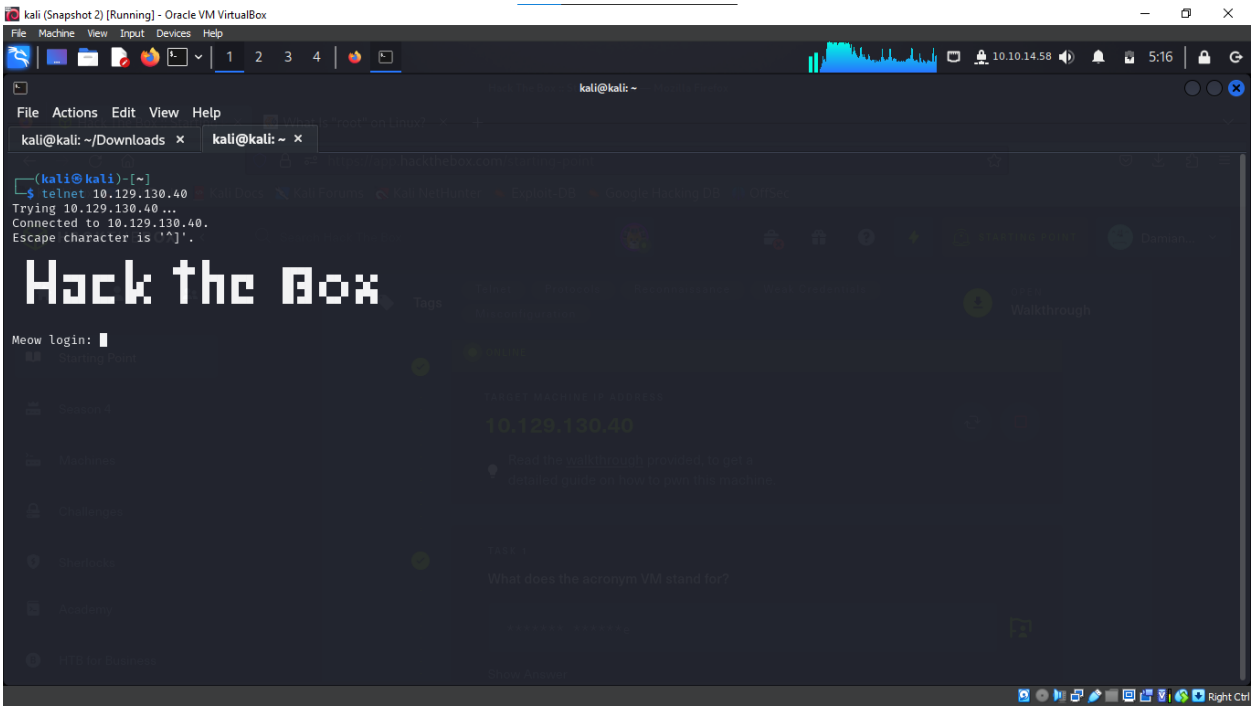
- 

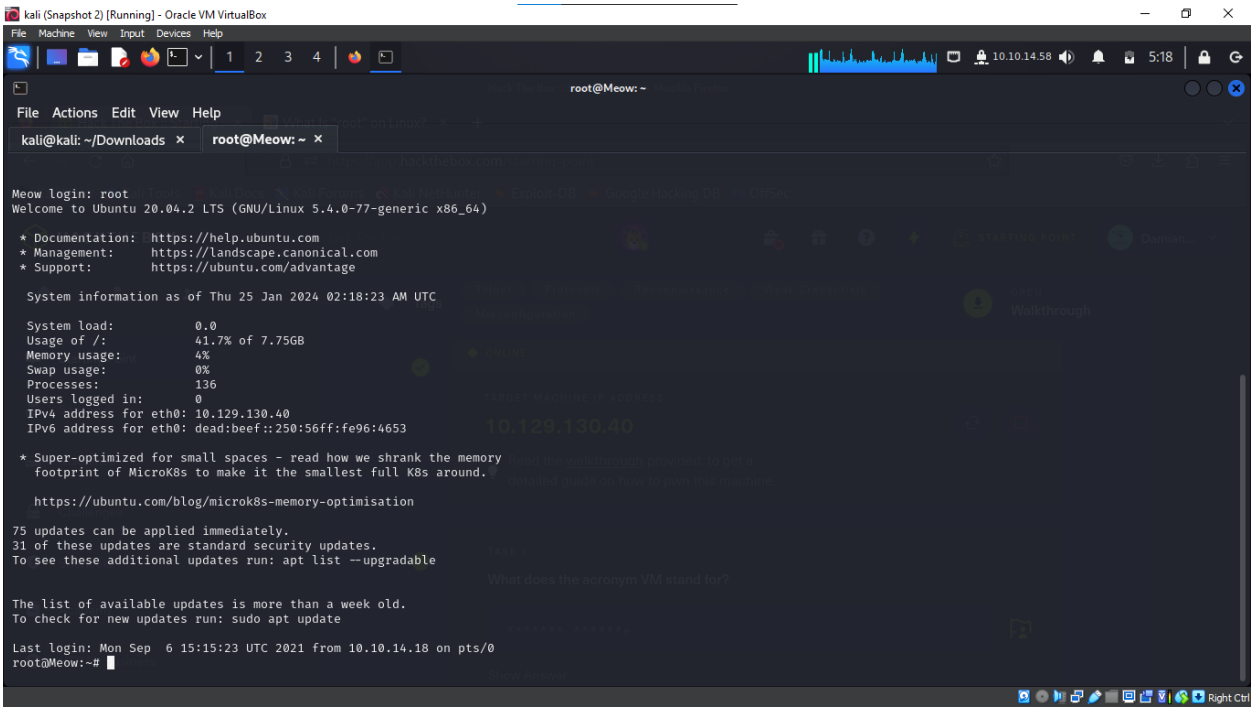
- 

Task 7: Gaining Access

- **Question:** What username can log into the target over telnet with a blank password?
- **Answer:** Root
- **Details:** Root is a username that typically has the highest access rights on the system. Logging in as root with a blank password indicates a severe security vulnerability.

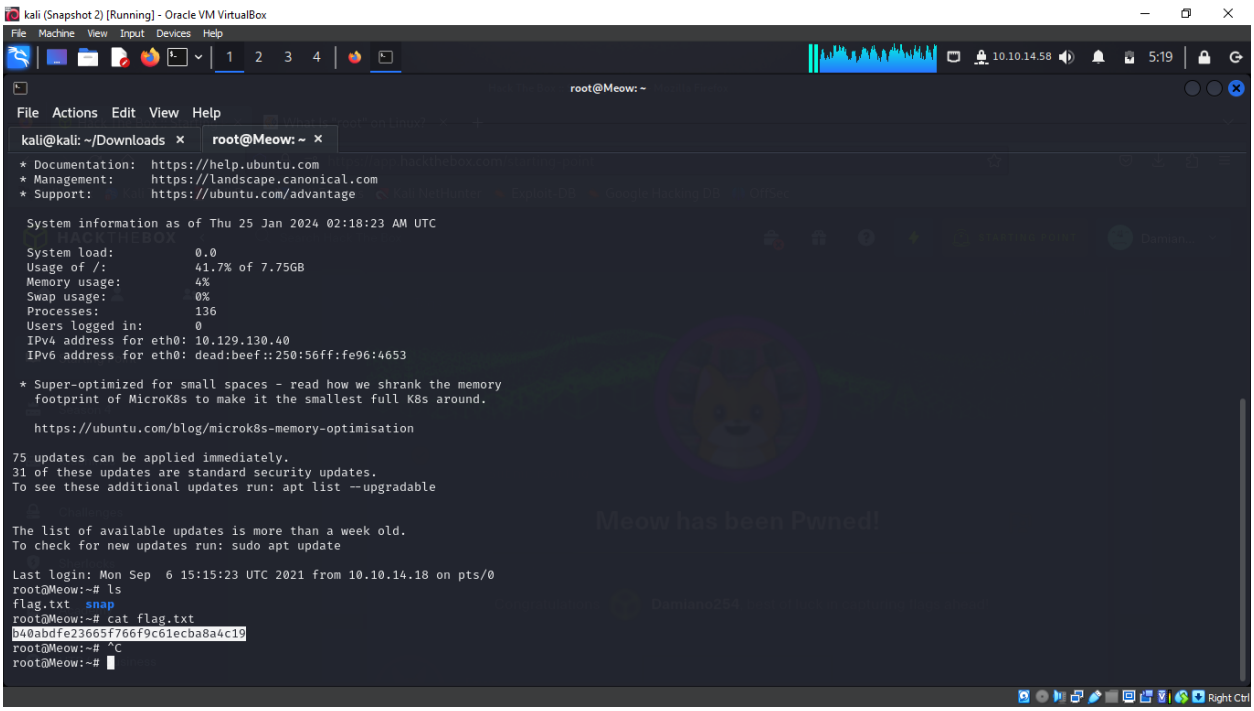

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
What Is "root" on Linux? — Mozilla Firefox
Hack The Box :: Starting P
What Is "root" on Linux?
https://www.howtogeek.com/737563/what-is-root-on-linux/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Using sudo
Running as root without Using su
Less Superman, More Clark Kent
The root user is the most powerful entity in the Linux universe with limitless powers, for better or worse. Create a user? Got it. Annihilate a file system? Whoops, got that too.
The Origin Story
The root user is the Linux superuser. They can, quite literally, do anything. Nothing is restricted or off-limits for root . Whether they're a superhero or a supervillain depends on the human user who takes on the mantle of the system administrator. Mistakes made by the root user can be catastrophic, so the root account should be used exclusively for administrative purposes.
The concept of the root user was inherited from Unix, which had a root user as its administrative superuser. But where the name "root" comes from isn't known for sure. Some people think that it came from the Multics operating system, which pre-dates Unix.
No, a MagSafe Case Won't Break Your Galaxy S24 Ultra's S Pen
1 day ago
OnePlus 12 Arrives With 80W Charging and 6.8-Inch Screen
1 day ago
10 Reasons Why Nova Launcher Is Still Worth Using on Android
1 day ago
Ford's New In-Car OS Won't Replace Android Auto or Apple CarPlay
2 days ago
The Fastest Way to Open the Camera on a Samsung Galaxy Phone
3 days ago
See More
Right Ctrl


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~
(kali㉿kali)-[~]
$ telnet 10.129.130.40
Trying 10.129.130.40 ...
Connected to 10.129.130.40.
Escape character is '^]'.
Hack the Box
Meow login:
Right Ctrl

- 

Task 8: Submit Flag

- **Flag:** b40abdfe23665f766f9c61ecba8a4c19
- **Details:** Successfully retrieved the root flag, indicating full control over the target system.

- 

Conclusion

This lab provided a practical experience in penetration testing techniques, emphasizing the importance of understanding network protocols, security vulnerabilities, and ethical hacking practices.

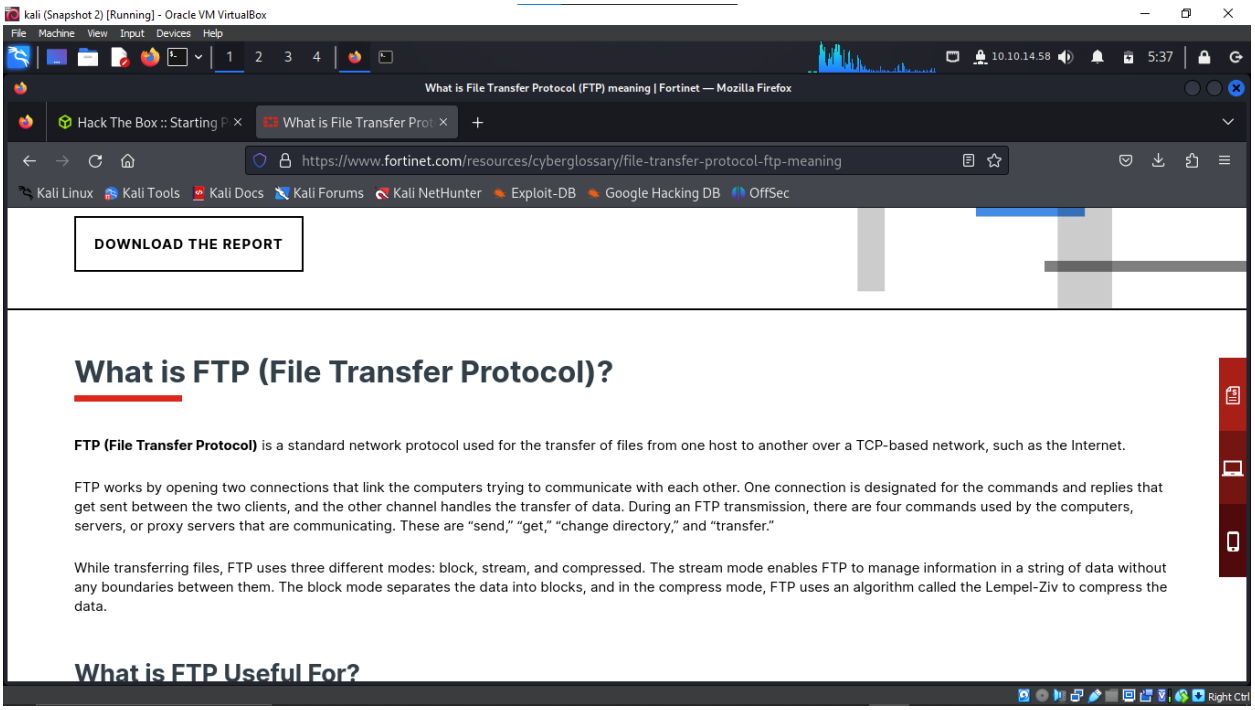
FAWN

Introduction

This report summarizes the findings from a Hack The Box Fawn exercise, where the focus was on understanding and interacting with the File Transfer Protocol (FTP) service.

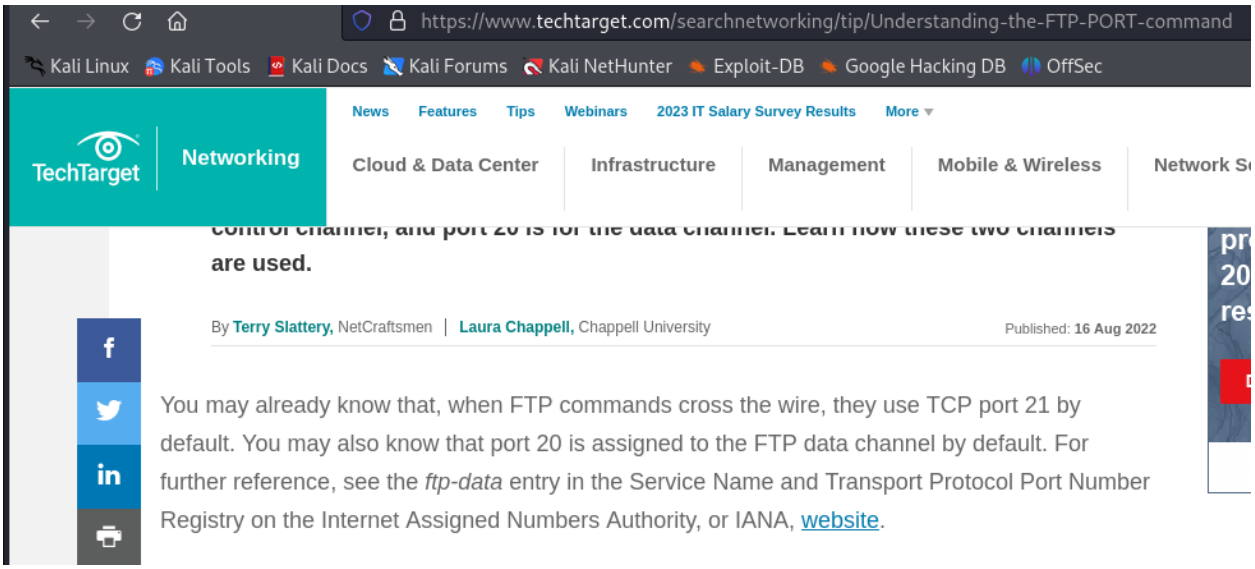
Tasks and Findings

Task 1: Understanding FTP

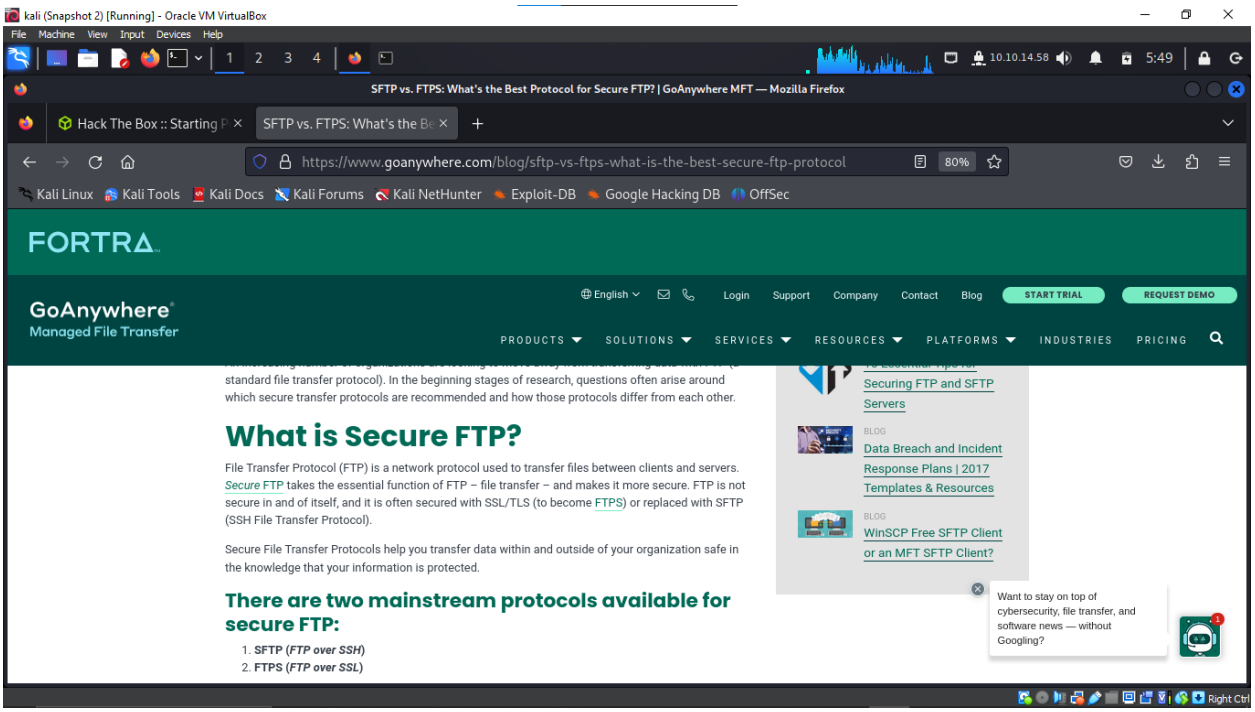
- **Question:** What does the 3-letter acronym FTP stand for?
- **Answer:** File Transfer Protocol
- **Details:** FTP is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
- 

Task 2: FTP Service Port

- **Question:** Which port does the FTP service listen on usually?
- **Answer:** 21

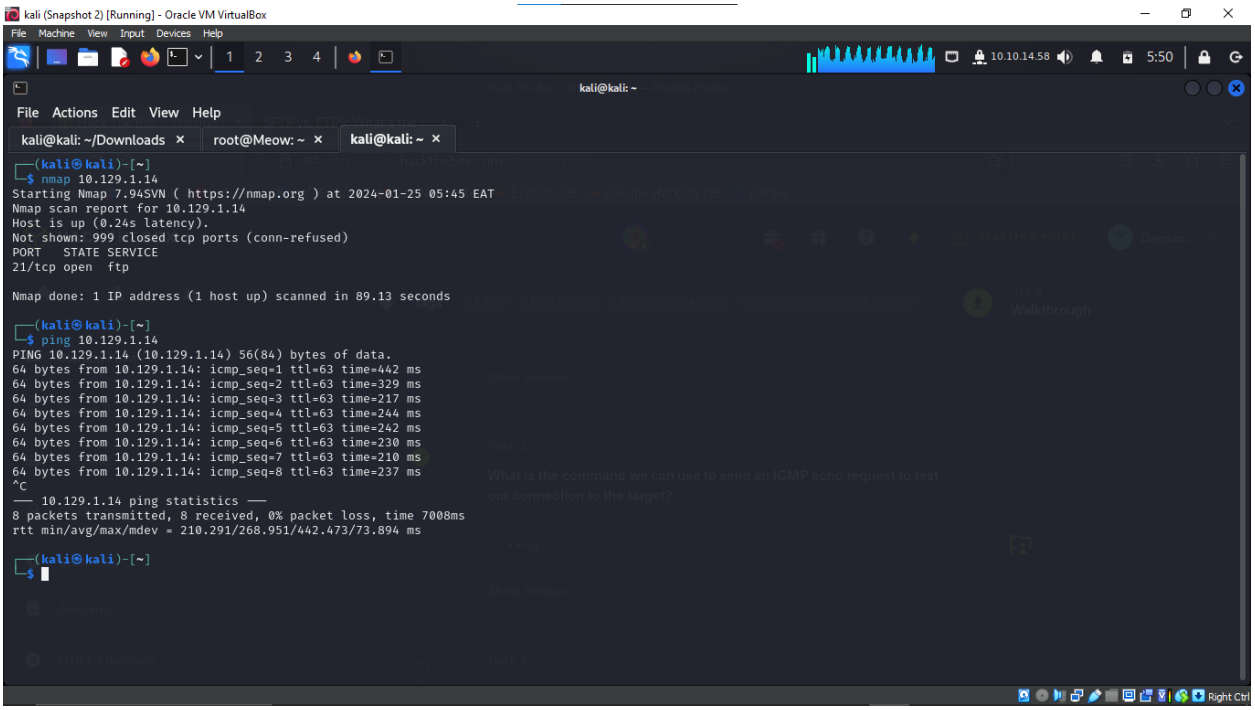
- **Details:** Port 21 is the standard TCP port reserved with IANA for FTP communication.
- 

Task 3: Secure FTP

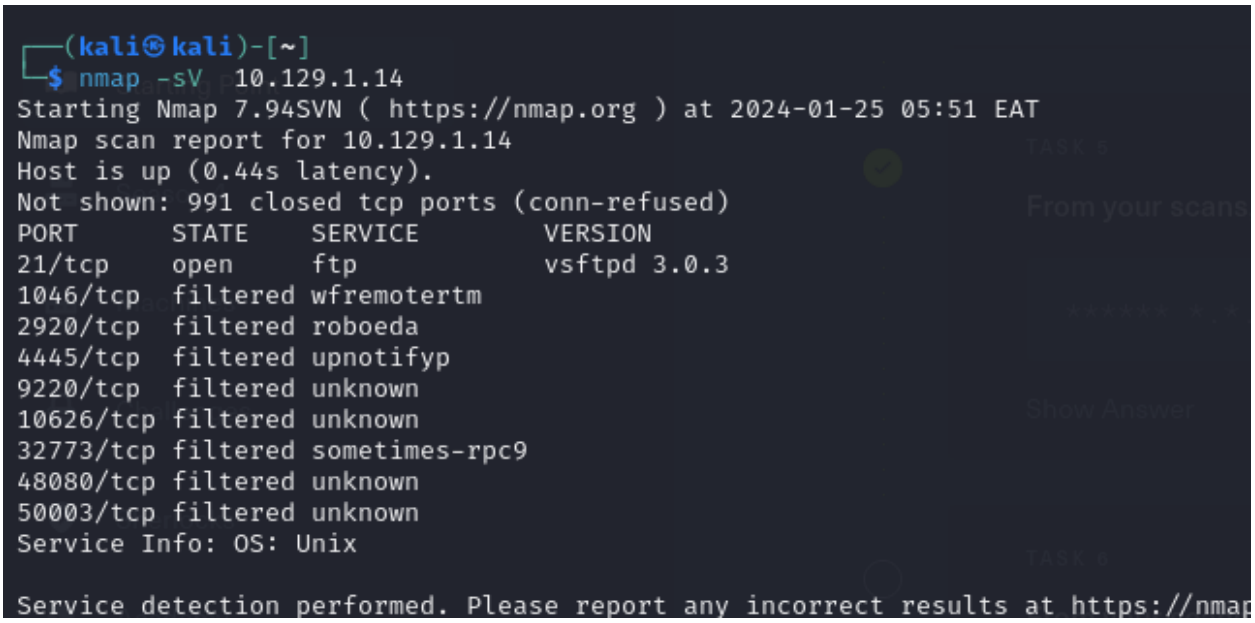
- **Question:** What acronym is used for the secure version of FTP?
- **Answer:** SFTP
- **Details:** SFTP stands for SSH File Transfer Protocol or Secure File Transfer Protocol, and it provides a secure method to transfer files.
- 

Task 4: Network Connection Testing

- **Question:** What is the command to send an ICMP echo request to test our connection to the target?
- **Answer:** ping

- **Details:** The ping command is used to test the reachability of a host on an IP network.
- 

Task 5: FTP Version Identification

- **Question:** What version is FTP running on the target?
- **Answer:** vsftpd 3.0.3
- **Details:** vsftpd (Very Secure FTP Daemon) 3.0.3 is identified as the FTP version on the target, indicating a secure and stable FTP server software.
- 

Task 6: Operating System Identification

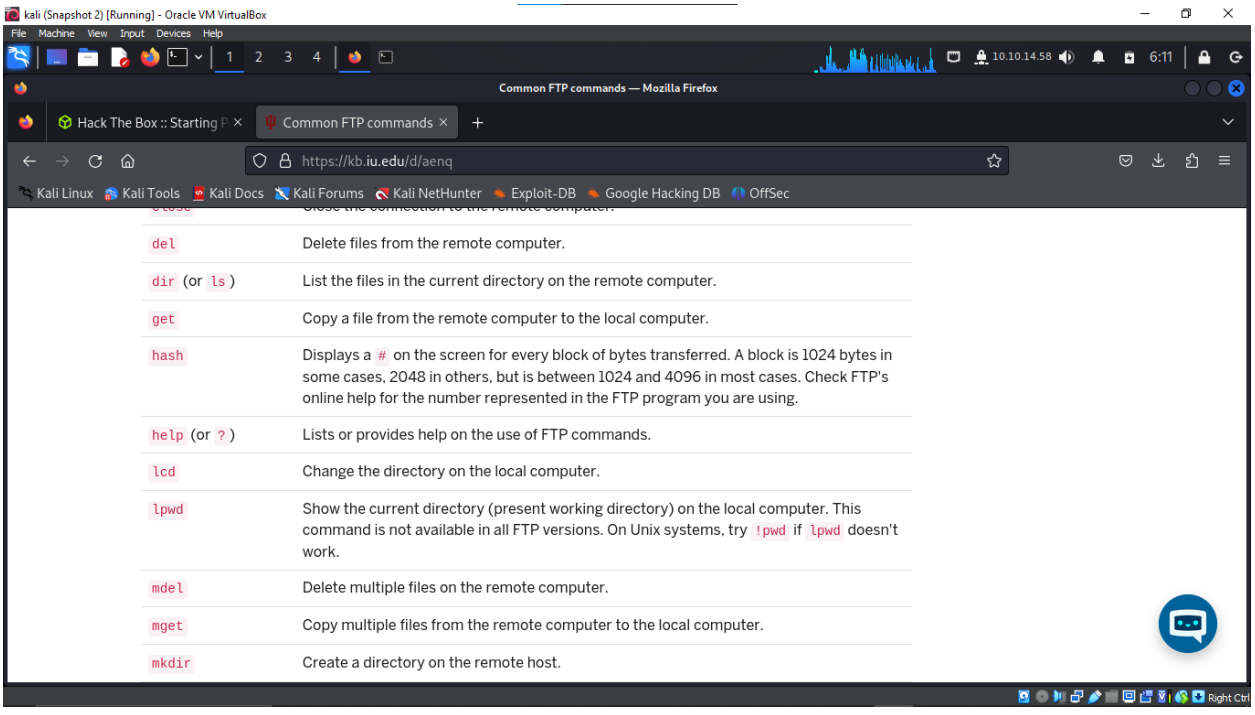
- **Question:** What OS type is running on the target?
- **Answer:** Unix

- **Details:** The target is running a Unix-type operating system, known for its robustness in network environments.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 05:51 EAT
Nmap scan report for 10.129.1.14
Host is up (0.44s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp            vsftpd 3.0.3
1046/tcp  filtered wfremotertm
2920/tcp  filtered roboeda
4445/tcp  filtered upnotifyp
9220/tcp  filtered unknown
10626/tcp filtered unknown
32773/tcp filtered sometimes-rpc9
48080/tcp filtered unknown
50003/tcp filtered unknown
Service Info: OS: Unix
```

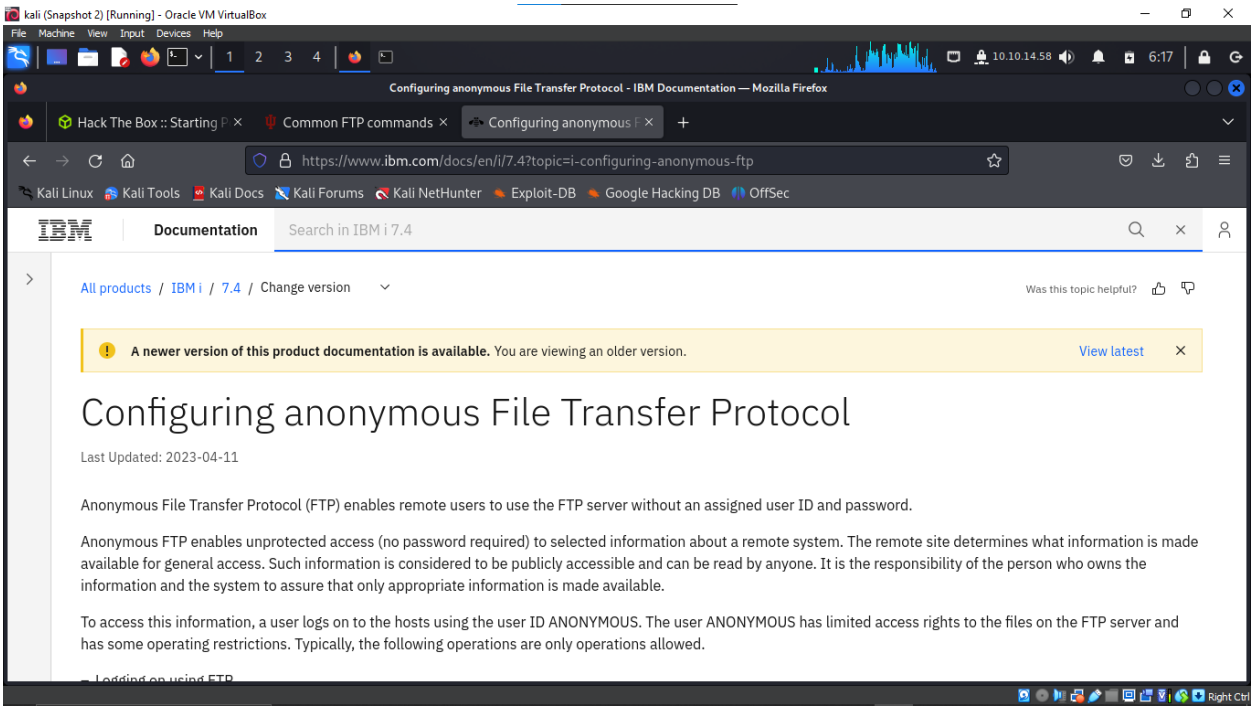
Task 7: FTP Client Help Menu

- **Question:** What is the command to display the 'ftp' client help menu?
- **Answer:** ftp -h
- **Details:** The command ftp -h is used to display the help menu for the FTP client, providing a list of available commands and options.

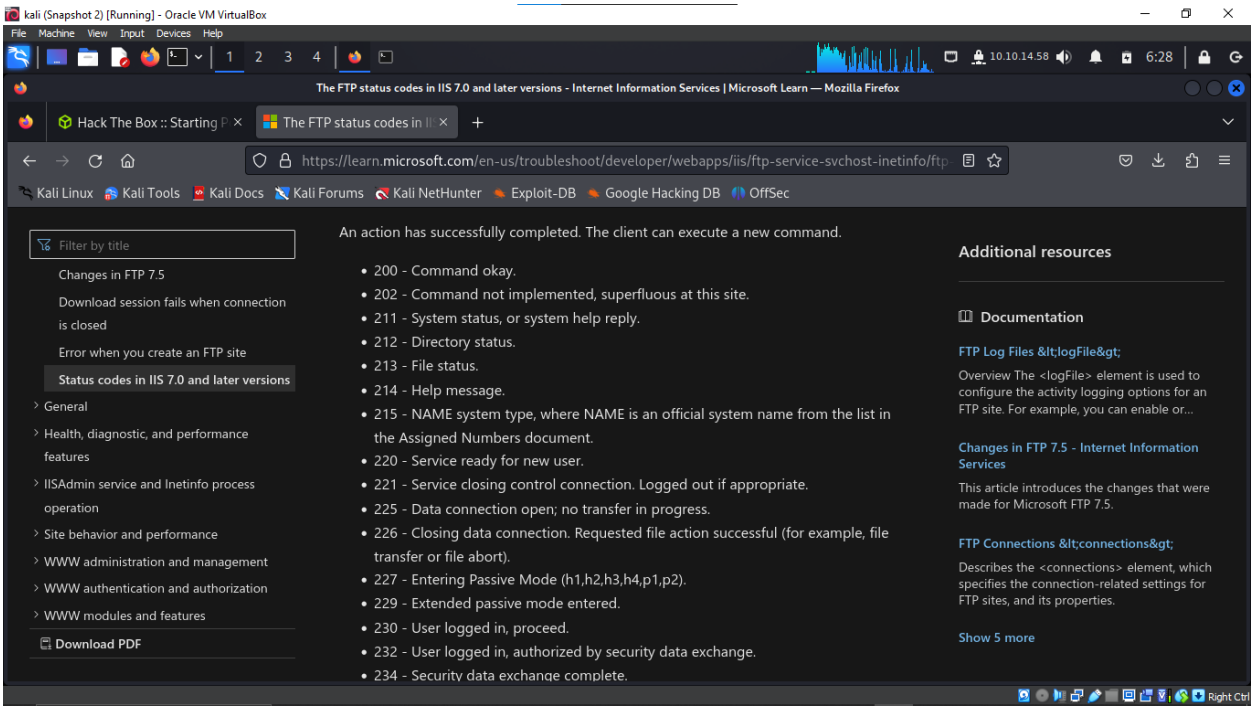


Task 8: Anonymous FTP Login

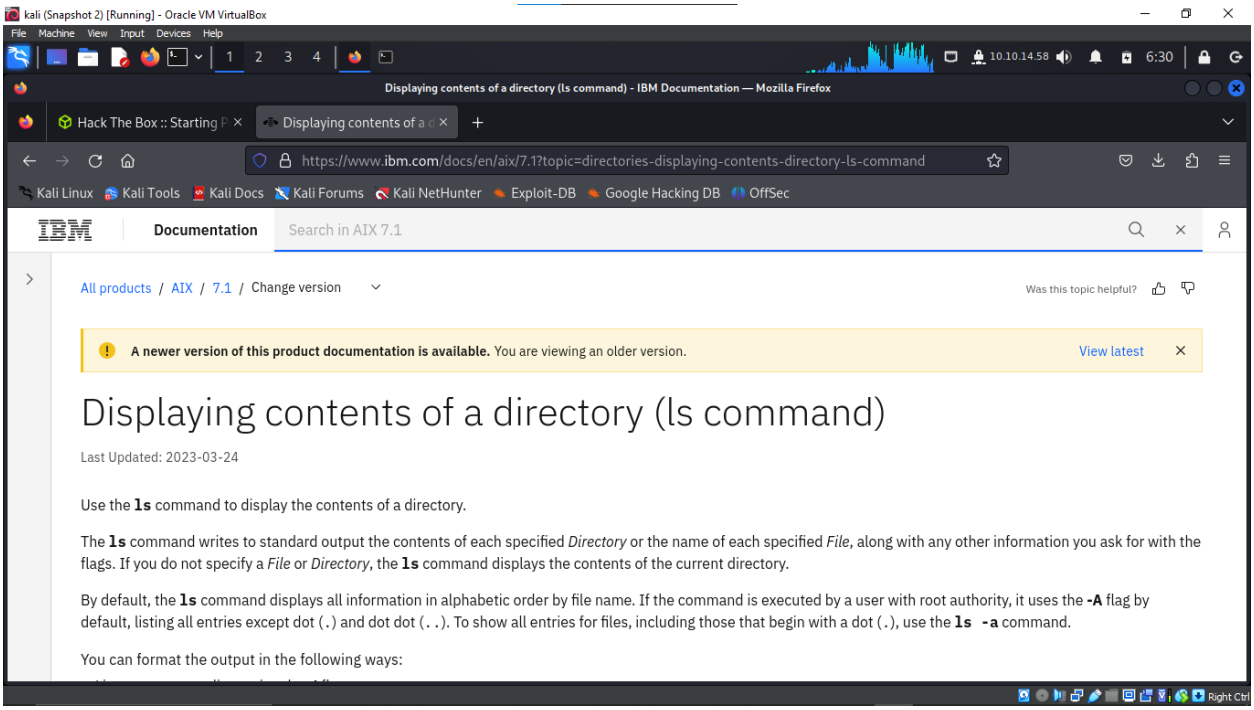
- Question: What is the username used over FTP for anonymous login?
- **Answer:** anonymous

- **Details:** The username 'anonymous' is commonly used to access an FTP server without a personal account.
- 

Task 9: FTP Login Response Code

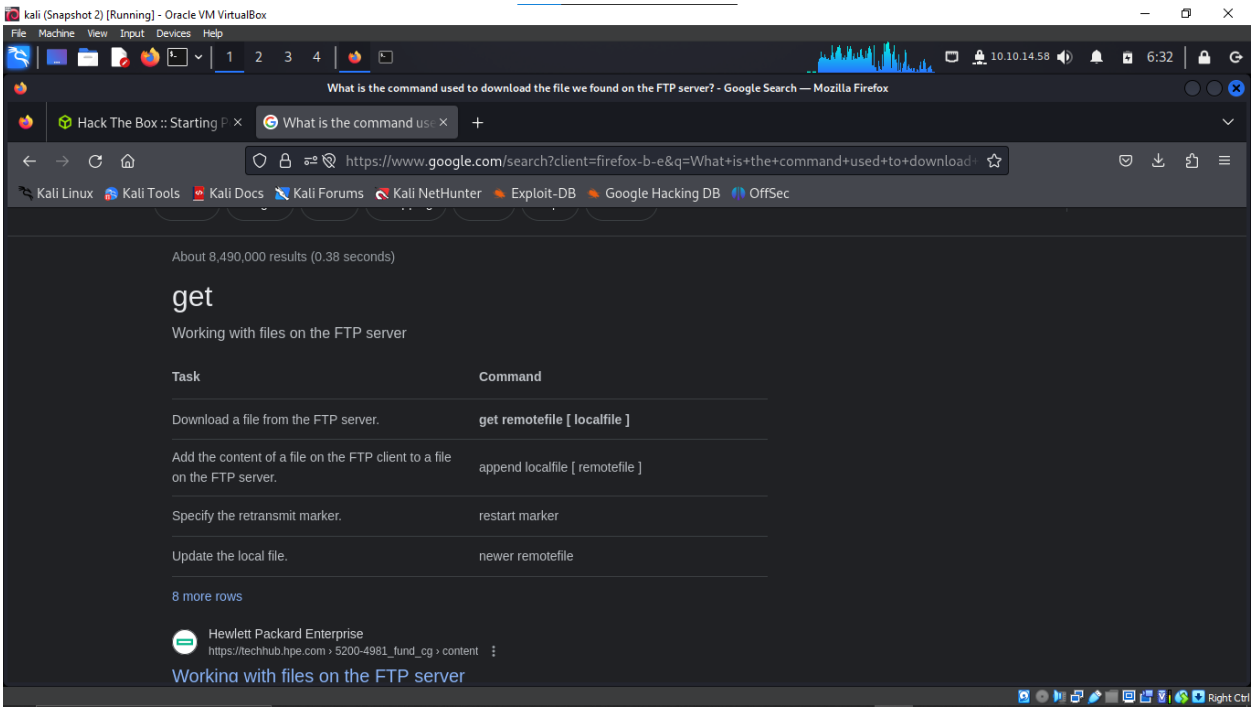
- **Question:** What is the response code for 'Login successful' in FTP?
- **Answer:** 230
- **Details:** The response code 230 indicates a successful login to the FTP server.
- 

Task 10: Listing Files and Directories

- **Question:** Besides 'dir', what is another common command to list files on a Linux system?
- **Answer:** ls
- **Details:** The 'ls' command is commonly used in Unix and Linux environments to list files and directories.
- 

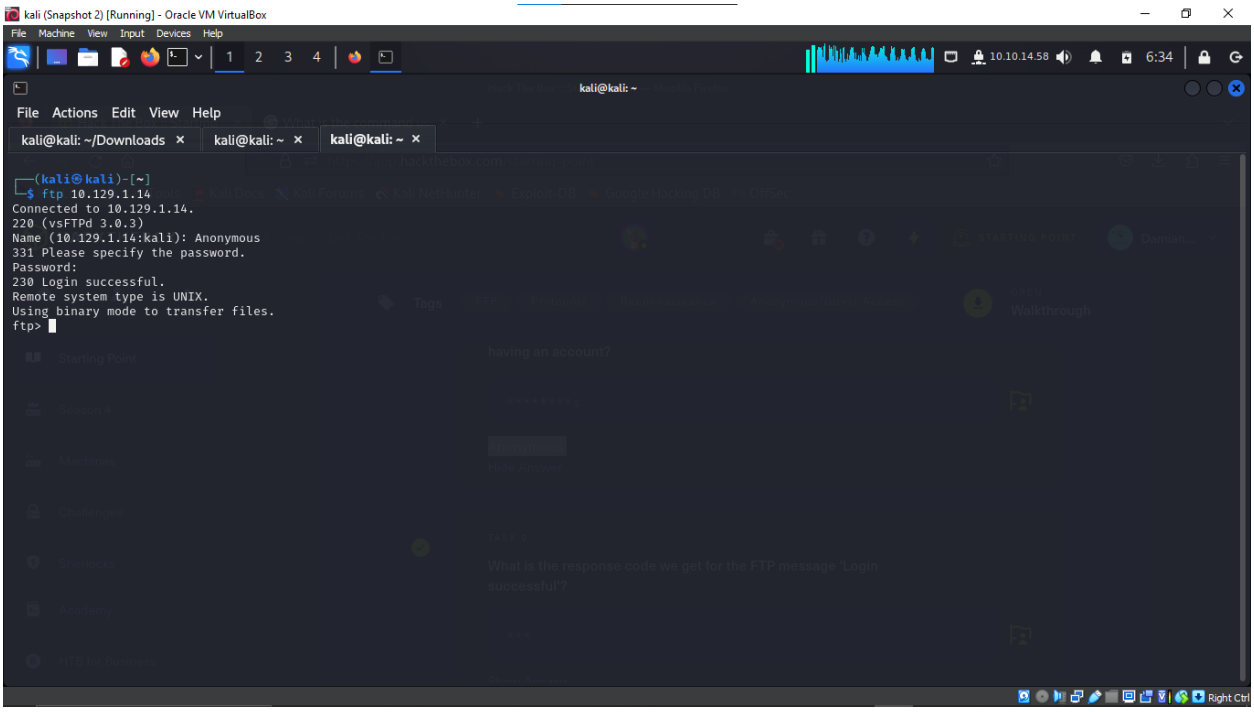
Task 11: Downloading Files via FTP

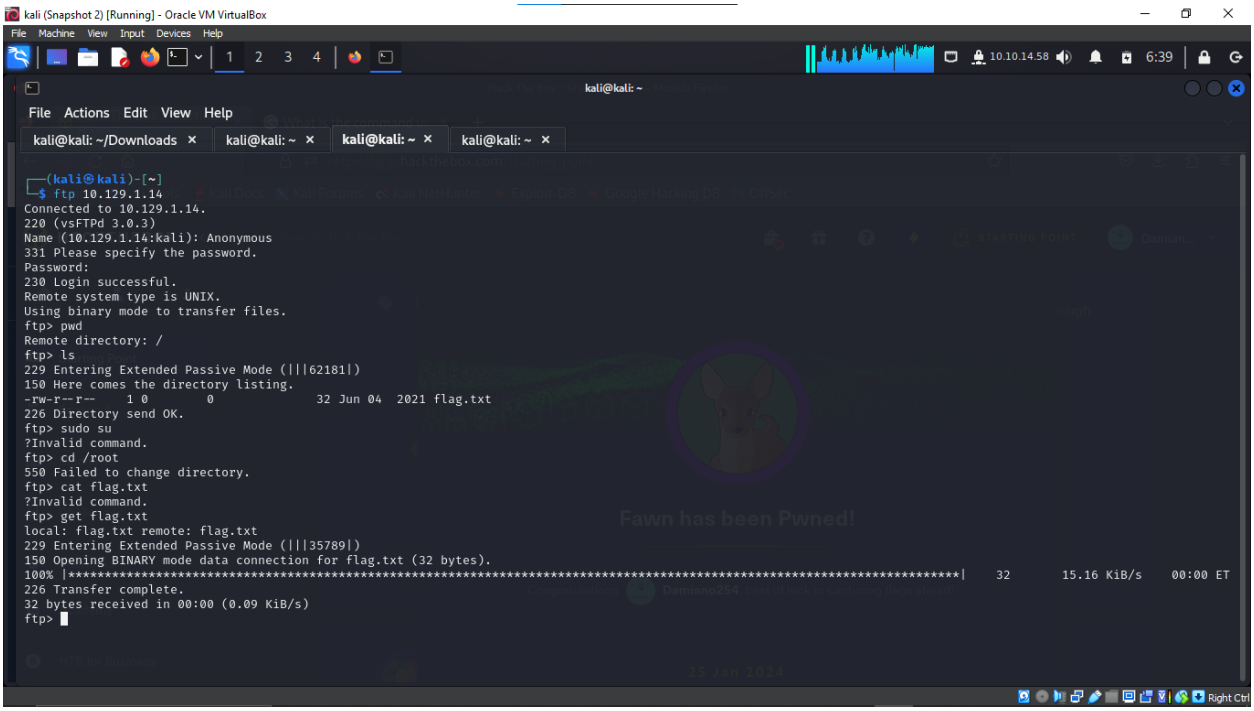
- **Question:** What is the command used to download files from the FTP server?
- **Answer:** get
- **Details:** The 'get' command in FTP is used to download files from the server to the local machine.

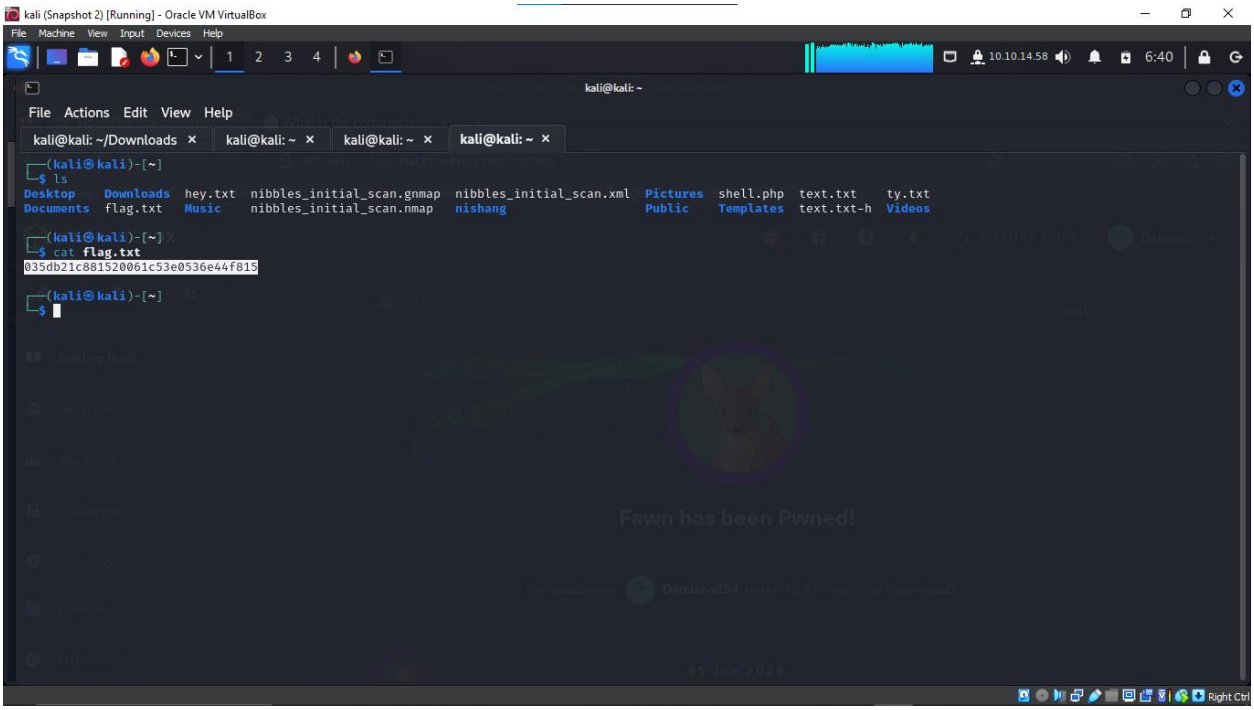
- 

Task 12: Root Flag Submission

- **Flag:** 035db21c881520061c53e0536e44f815
- **Details:** Successfully retrieved the root flag, indicating full administrative control over the target system.

- 

- 

- 

Conclusion

This exercise provided practical experience in interacting with FTP services, including identifying service versions, testing connections, and transferring files securely. The tasks underscored the importance of understanding network protocols and their security implications.

Dancing

Introduction

This report outlines the findings and activities from the "Dancing" lab in Hack The Box, focusing on the Server Message Block (SMB) protocol used in Windows environments.

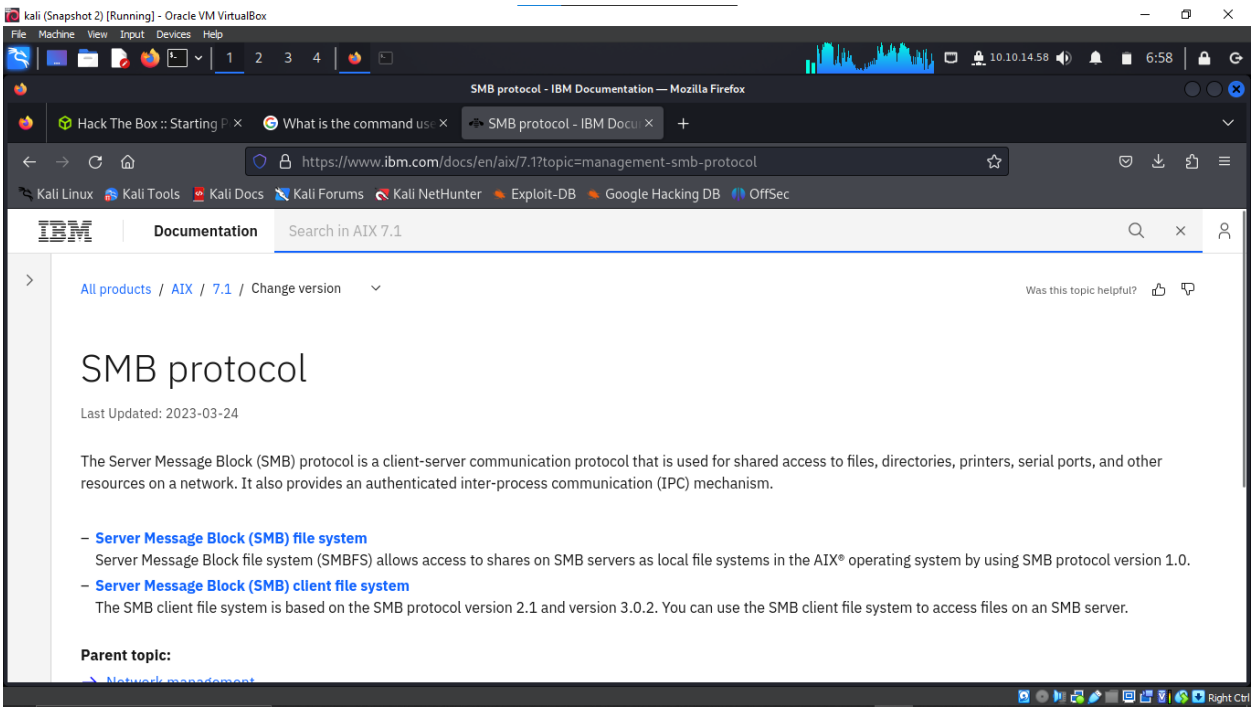
Tasks and Findings

Task 1: Understanding SMB

Question: What does SMB stand for?

Answer: Server Message Block

Details: SMB is a network file sharing protocol allowing applications on a computer to read and write to files and request services from server programs in a computer network.



Task 2: SMB Operating Port

Question: What port does SMB use?

Answer: 445

Details: SMB operates on TCP port 445, facilitating file sharing, network browsing, printing services, and interprocess communication over a network.

What is the use of port 445?

Port 445 is a Microsoft networking port which is also linked to the NetBIOS service present in earlier versions of Microsoft Operating Systems. It runs Server Message Block (SMB), which allows systems of the same network to share files and printers over TCP/IP.

This port shouldn't be opened for external network. All microsoft devices mostly have port 445 open as the port is used for LAN communication.

Task 3: Service Name for Port 445

- **Question:** What is the service name for port 445 found in the Nmap scan?

  Answer: microsoft-ds

- **Details:** The service 'microsoft-ds' on port 445 is associated with Windows Server's directory services.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.129.170.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 07:22 EAT
Warning: 10.129.170.18 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.170.18
Host is up (0.30s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
33/tcp    filtered dsp
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
179/tcp   filtered bgp
445/tcp   open     microsoft-ds?
513/tcp   filtered login
1107/tcp  filtered isoipsigport-2
1113/tcp  filtered ltp-deepspace
1123/tcp  filtered murray
1244/tcp  filtered isbconference1
2393/tcp  filtered ms-olap1
4002/tcp  filtered mlchat-proxy
5102/tcp  filtered admeng
5959/tcp  filtered unknown
6001/tcp  filtered X11:1
18040/tcp filtered unknown
24800/tcp filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 261.78 seconds
```

Task 4: Listing SMB Shares

Question: What flag is used with smbclient to list available shares?

Answer: -L

- **Details:** The '-L' switch in smbclient is used to list all available shares on the SMB server.

The **smbclient** command with the **-L or --list** option can be used to list the current shares. By default, when the **-U or --user** option is not included, the logon will be performed as a guest. If guest logins are permitted, something like this should be returned.

In this example, the "share" directory is being shared.

```
~]# smbclient --list $(hostname -s)
Enter SAMBA\GUEST's password: Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        share           Disk
        IPC$            IPC       IPC Service (Samba 4.12.2)
SMB1 disabled -- no workgroup available
```

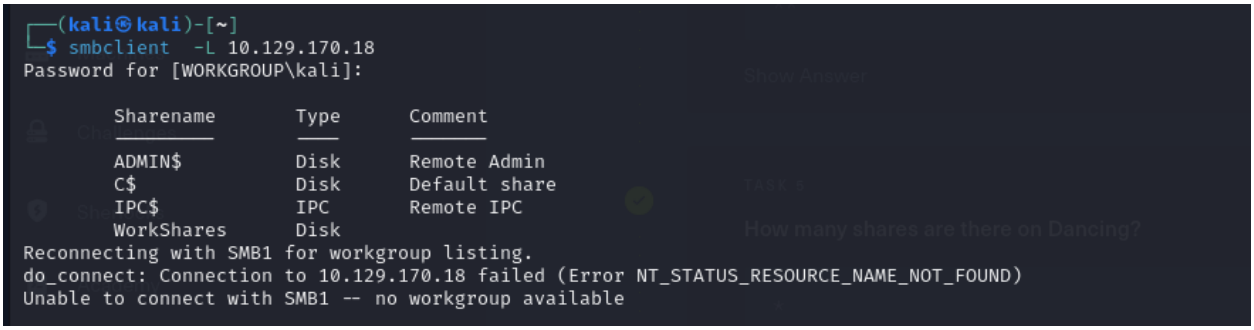
-

Task 5: Number of Shares on Dancing

Question: How many shares are there on Dancing?

Answer: 4

- **Details:** The scan revealed 4 shares, indicating multiple points of potential interaction or data access on the server.



```
┌──(kali㉿kali)-[~]
└─$ smbclient  -L 10.129.170.18
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ─────────       ────      ───────
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.170.18 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

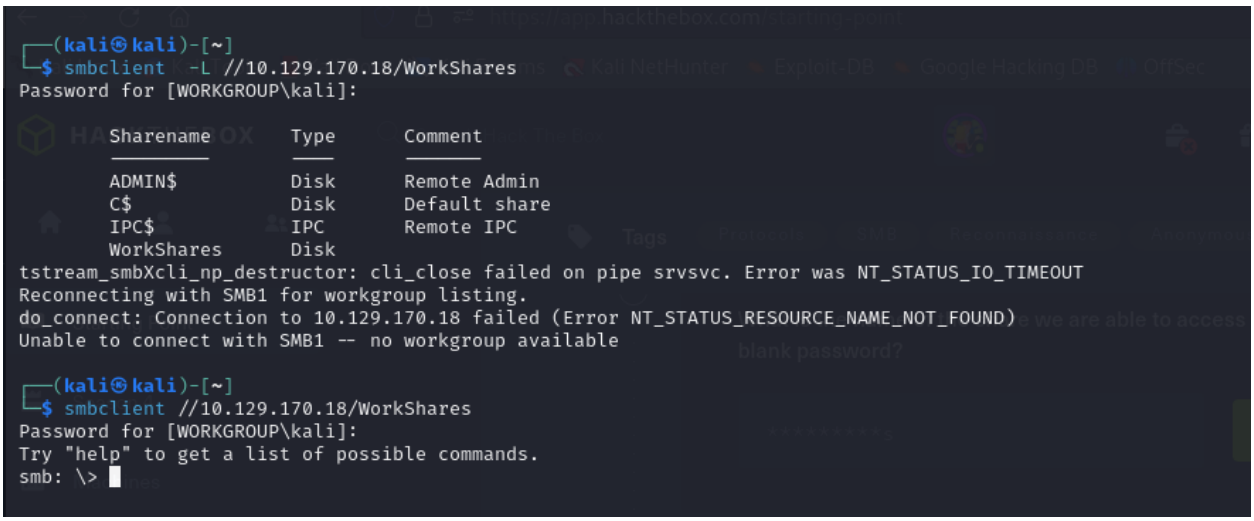
-

Task 6: Accessible Share with Blank Password

Question: Name of the share accessible with a blank password?

Answer: WorkShares

Details: The 'WorkShares' share was accessible with a blank password, highlighting a security vulnerability.



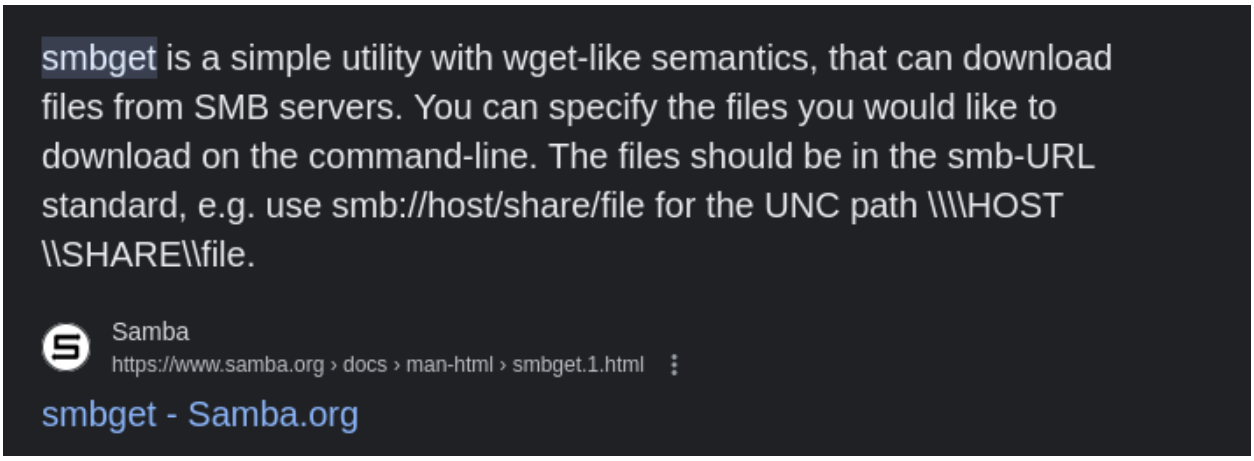
```
┌──(kali㉿kali)-[~]
└─$ smbclient  -L //10.129.170.18/WorkShares
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ─────────       ────      ───────
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
tstream_smbXcli_np_destructor: cli_close failed on pipe srvsvc. Error was NT_STATUS_IO_TIMEOUT
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.170.18 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~]
└─$ smbclient //10.129.170.18/WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \>
```

Task 7: Downloading Files via SMB

Question: Command to download files in SMB shell?

Answer: get

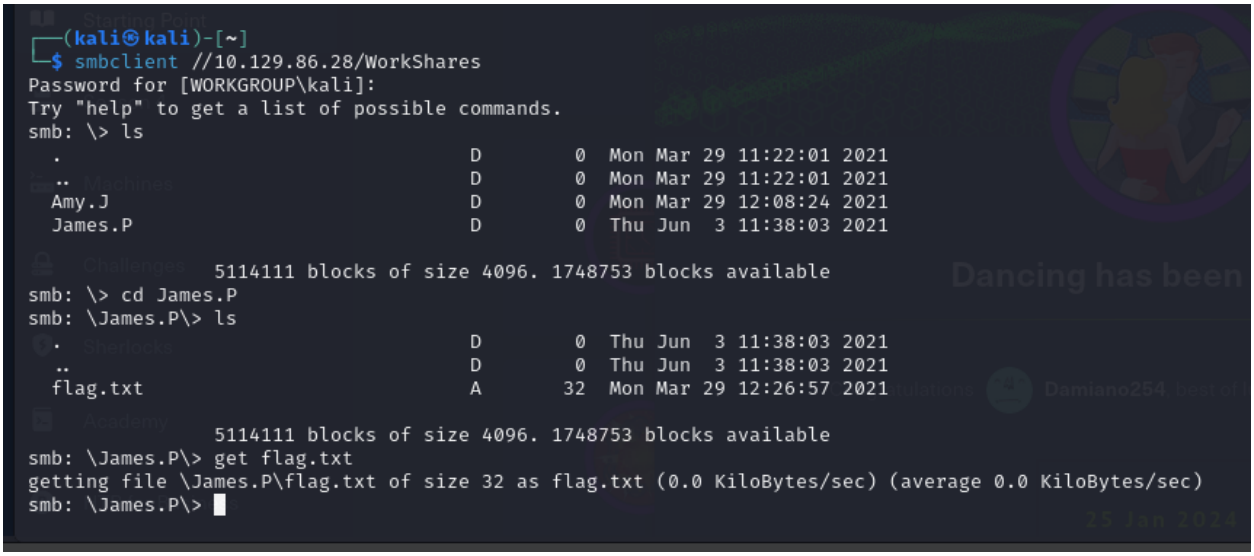
- **Details:** The 'get' command in the SMB shell is used to download files from the share to the local machine.

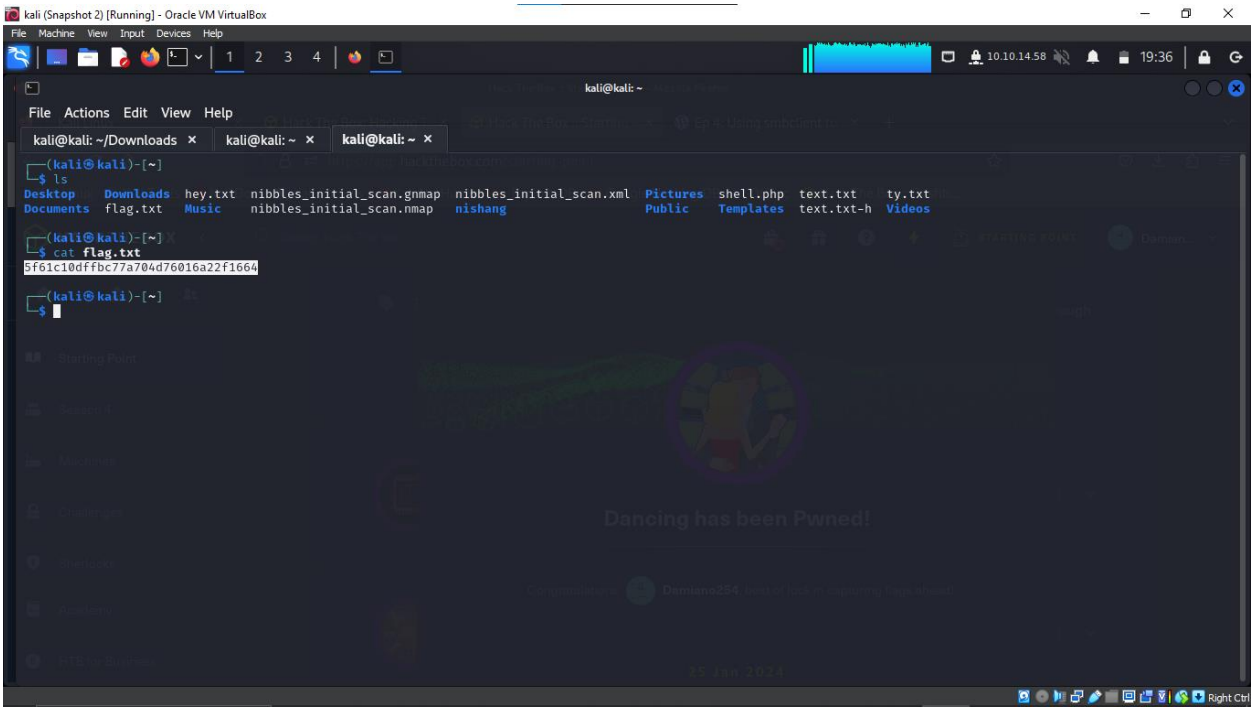


Submit Root Flag

Flag: 5f61c10dffbc77a704d76016a22f1664

Details: Successfully retrieved the root flag from the target system.





Conclusion

The "Dancing" lab provided insights into SMB protocol operations, including scanning for services, enumerating shares, and accessing shared resources. It emphasized the importance of secure configurations to prevent unauthorized access.

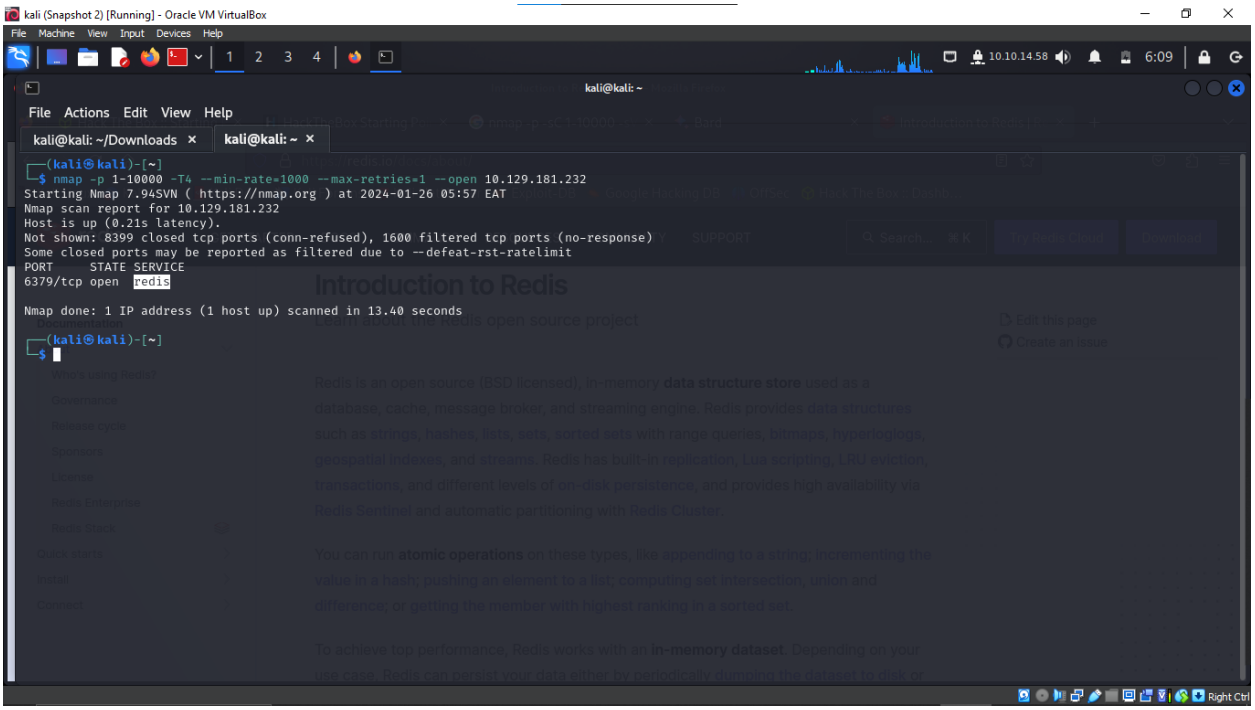
REDEEMER

Introduction

This report details the findings and activities from the "Redeemer" lab in Hack The Box, focusing on the Redis database, a prevalent in-memory data structure store.

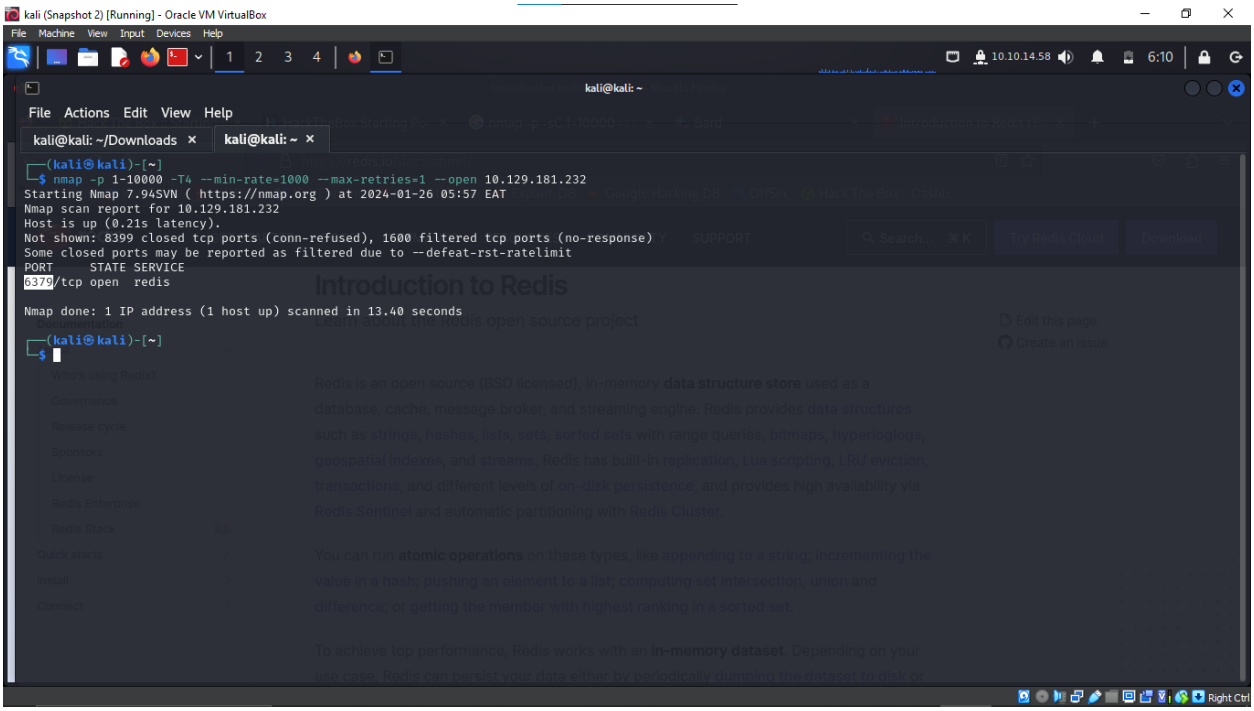
Tasks and Findings

Task 1: Redis Operating Port

- **Question:** Which TCP port is open on the machine?
- **Answer:** 6379
- **Details:** Port 6379 is the default port for Redis, a key-value database.
- 

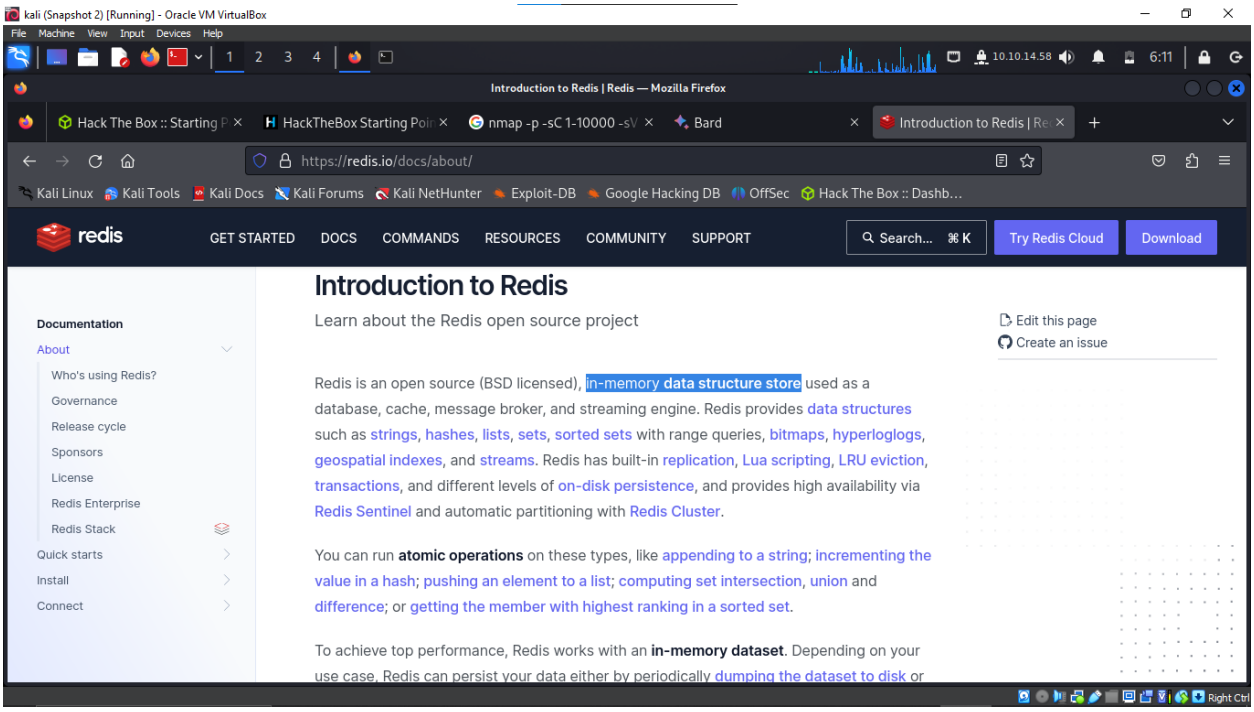
Task 2: Service on Open Port

- **Question:** Which service is running on the open port?
- **Answer:** Redis
- **Details:** Redis, an in-memory data structure store, is running on port 6379.

- 

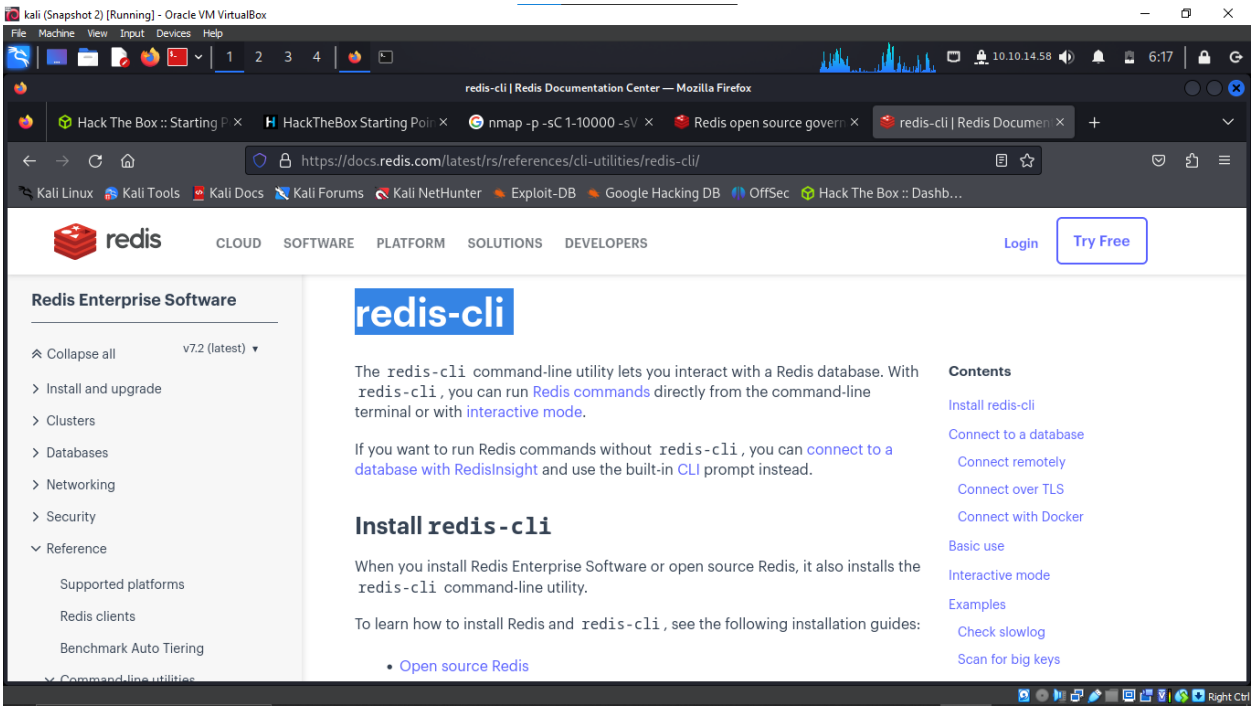
Task 3: Redis Database Type

- **Question:** What type of database is Redis?
- **Answer:** In-memory Database
- **Details:** Redis is an in-memory database, storing data in RAM for high performance.

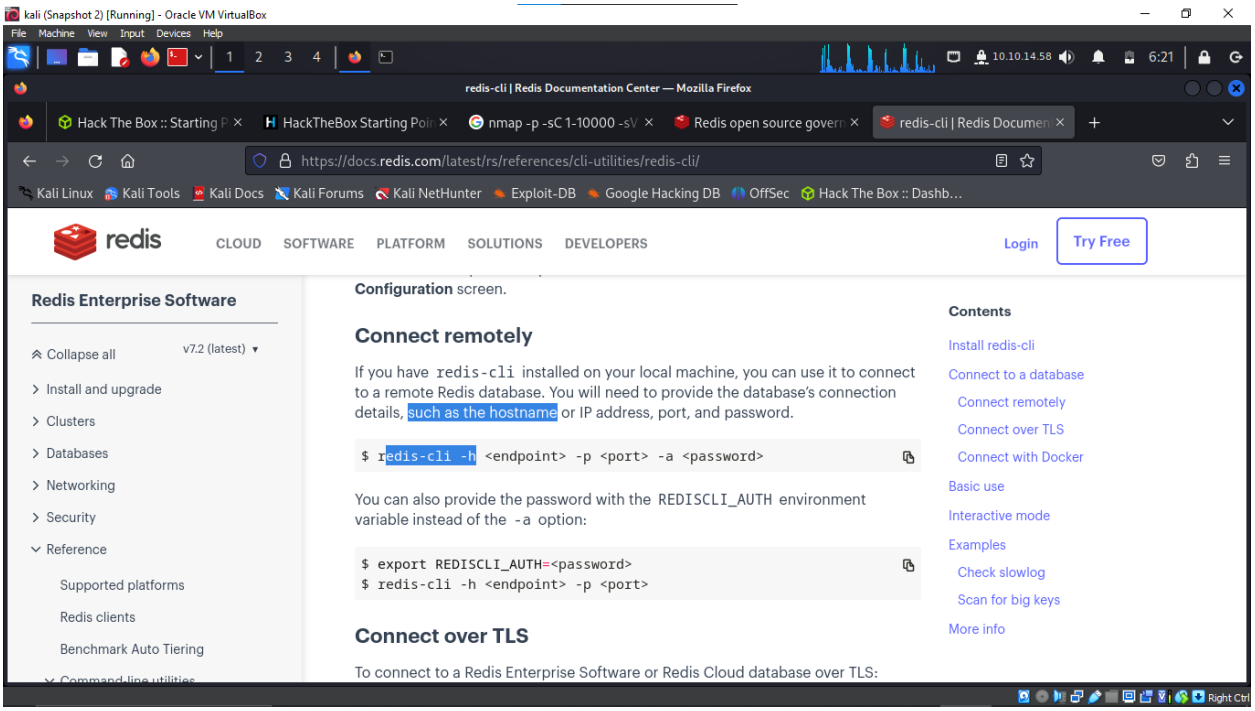
- 

Task 4: Redis Interaction Utility

- **Question:** Which command-line utility is used to interact with Redis?
- **Answer:** Redis-cli

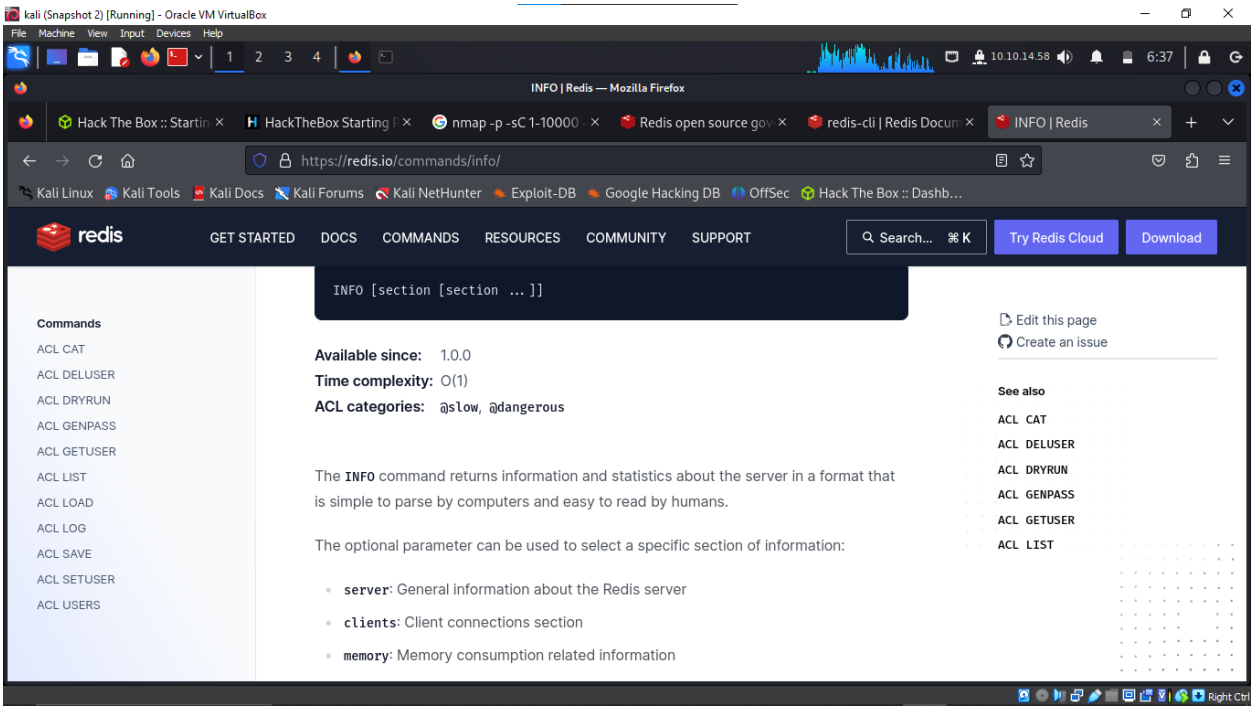
- **Details:** Redis-cli is the command-line utility for interacting with the Redis server.
- 

Task 5: Specifying Hostname in Redis

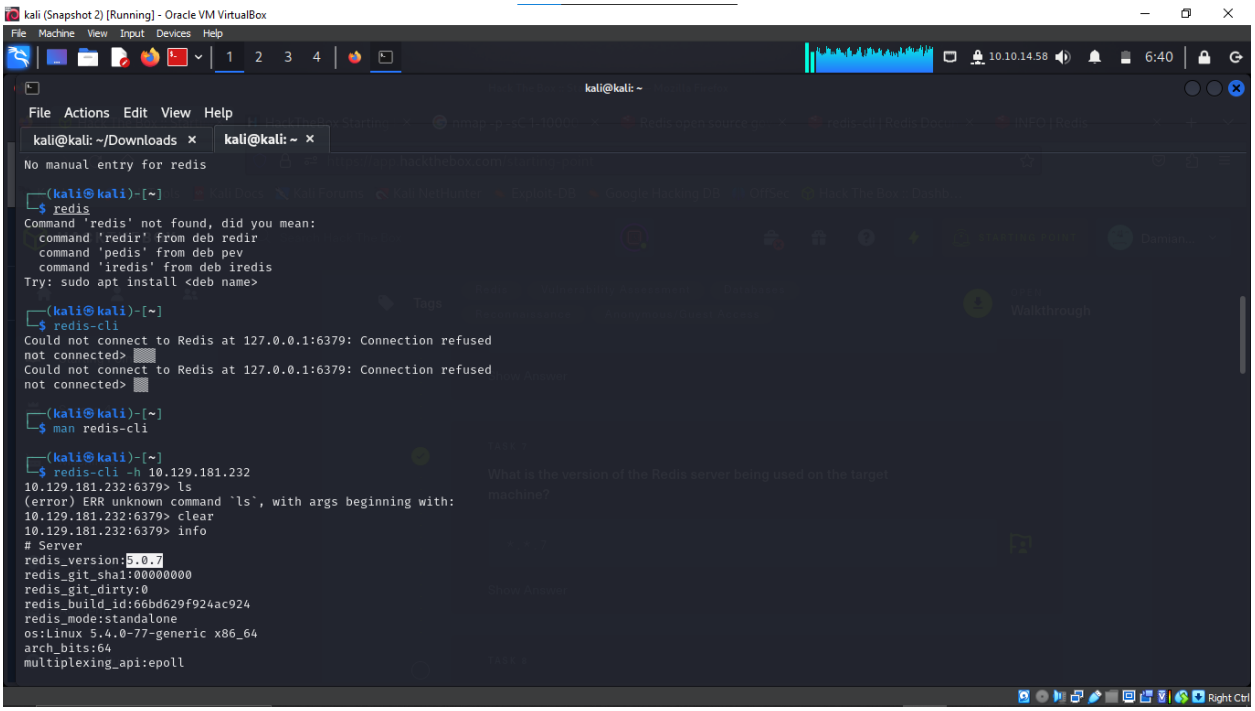
- **Question:** Which flag is used with Redis-cli to specify the hostname?
- **Answer:** -h
- **Details:** The '-h' flag is used to specify the target hostname in Redis-cli.
- 

Task 6: Redis Server Information

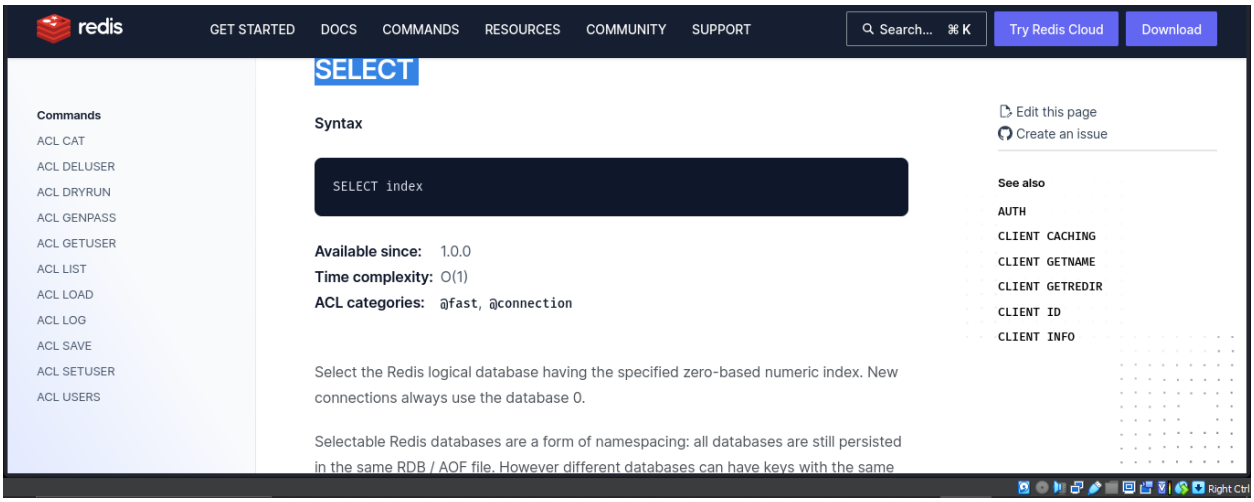
- **Question:** Command to obtain Redis server information?

- **Answer:** info
- **Details:** The 'info' command in Redis-cli provides statistics and information about the Redis server.
- 

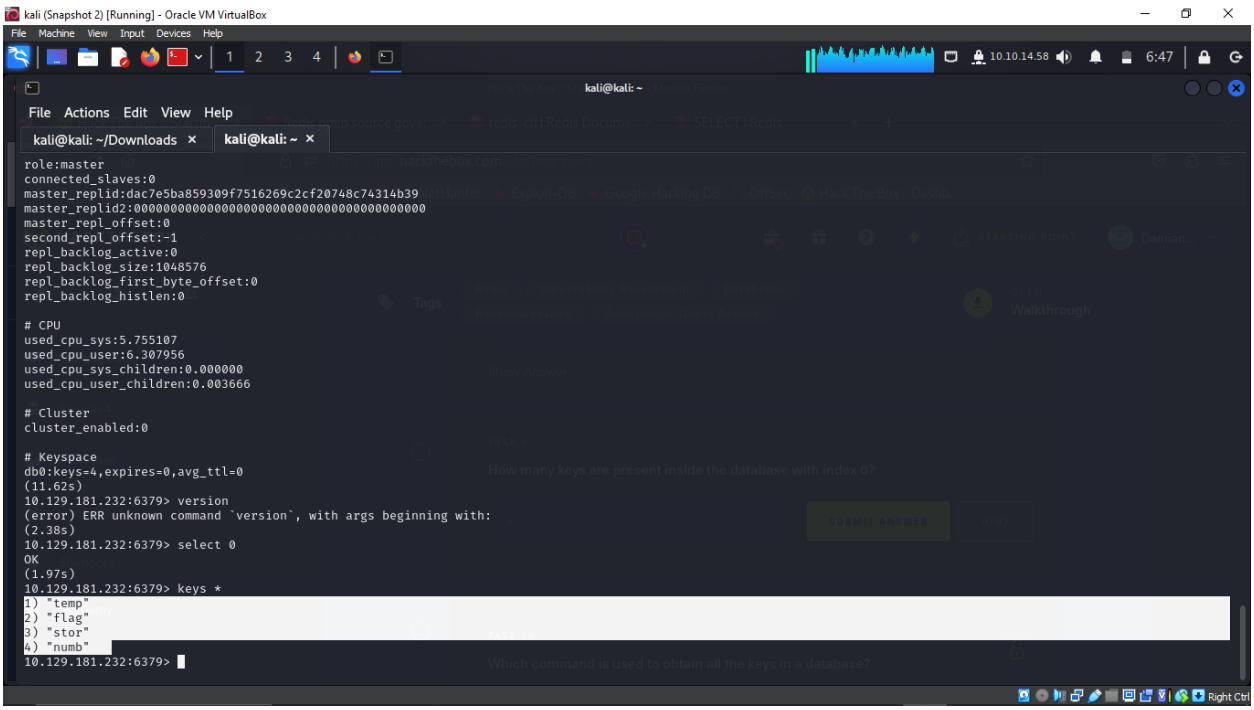
Task 7: Redis Server Version

- **Question:** What is the version of the Redis server on the target?
- **Answer:** 5.0.7
- **Details:** The target is running Redis server version 5.0.7.
- 

Task 8: Selecting Database in Redis

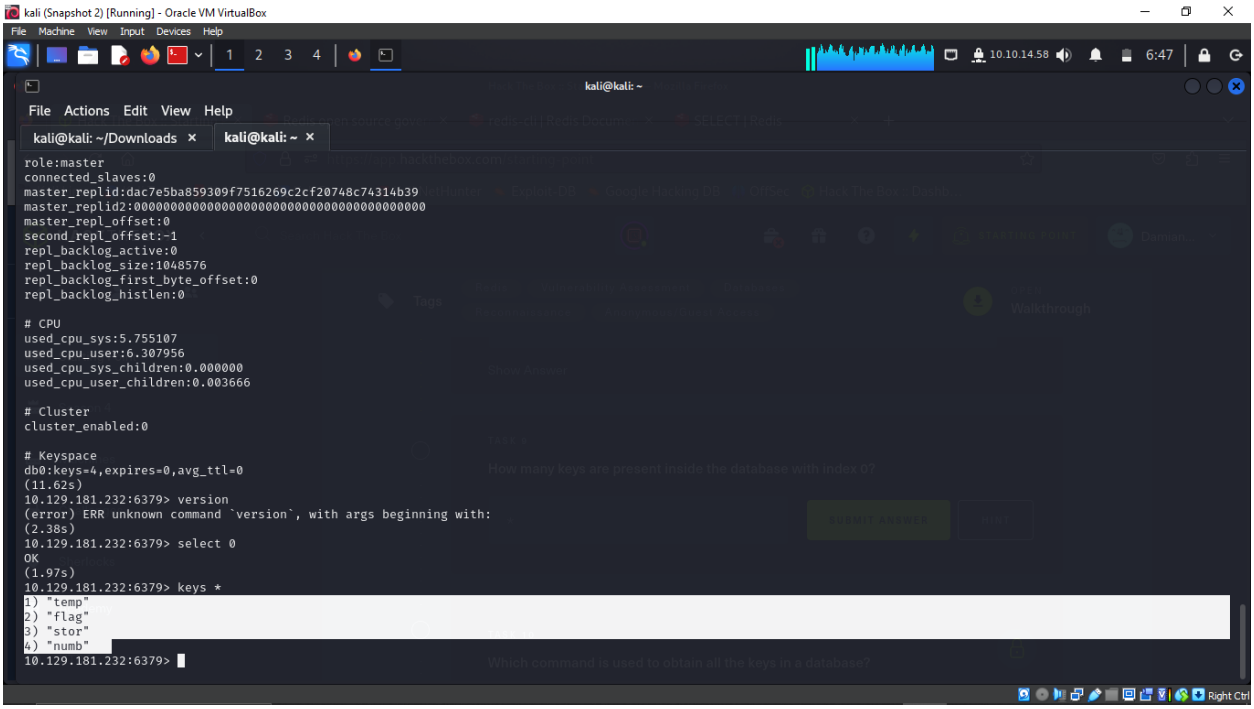
- **Question:** Command to select a database in Redis?
- **Answer:** select
- **Details:** The 'select' command is used to choose the desired database in Redis.
- 

Task 9: Number of Keys in Database

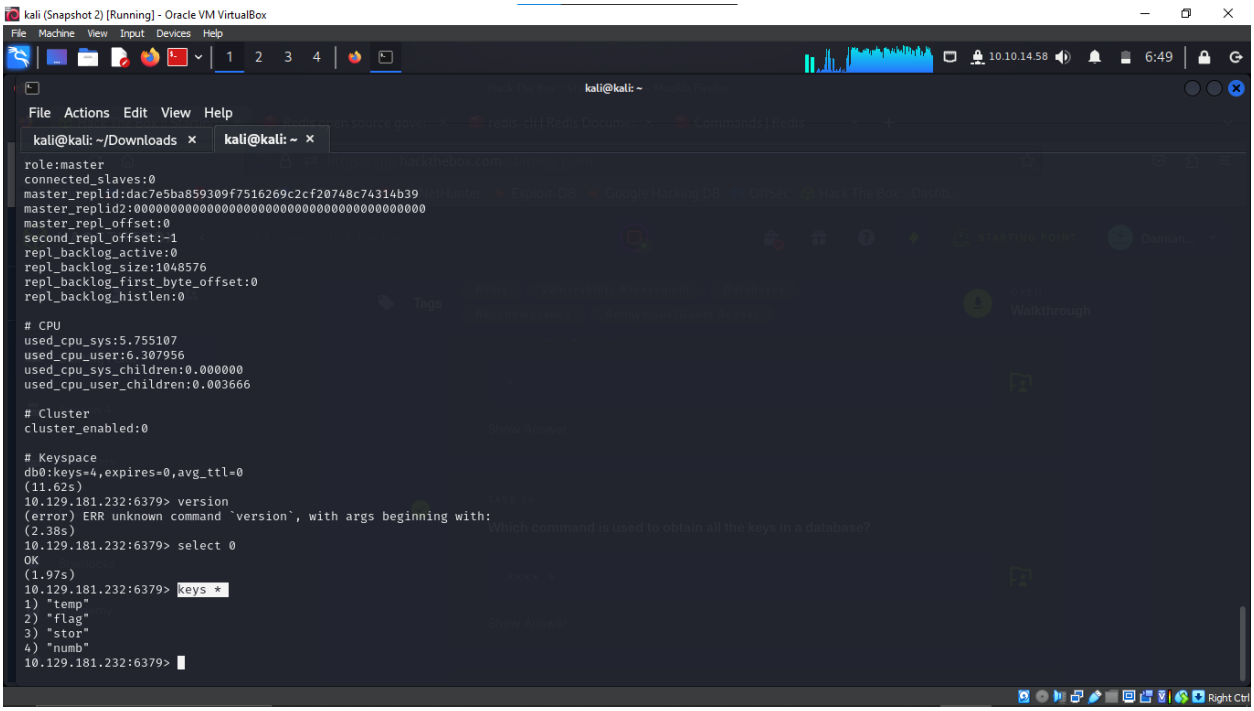
- **Question:** How many keys in the database with index 0?
- **Answer:** 4
- **Details:** There are 4 keys in the database with index 0 on the Redis server.
- 

Task 10: Listing All Keys in Database

- **Question:** Command to list all keys in a database?
- **Answer:** keys *

- **Details:** The 'keys *' command lists all keys in the current Redis database.
- 

Submit Root Flag

- **Flag:** 03e1d2b376c37ab3f5319922053953eb
- **Details:** Successfully retrieved the root flag, indicating successful data retrieval from the Redis server.
- 

Conclusion

This lab provided practical experience with Redis, focusing on enumeration, interaction, and data retrieval from an in-memory database. The tasks highlighted

the importance of understanding different types of databases and their operational specifics.