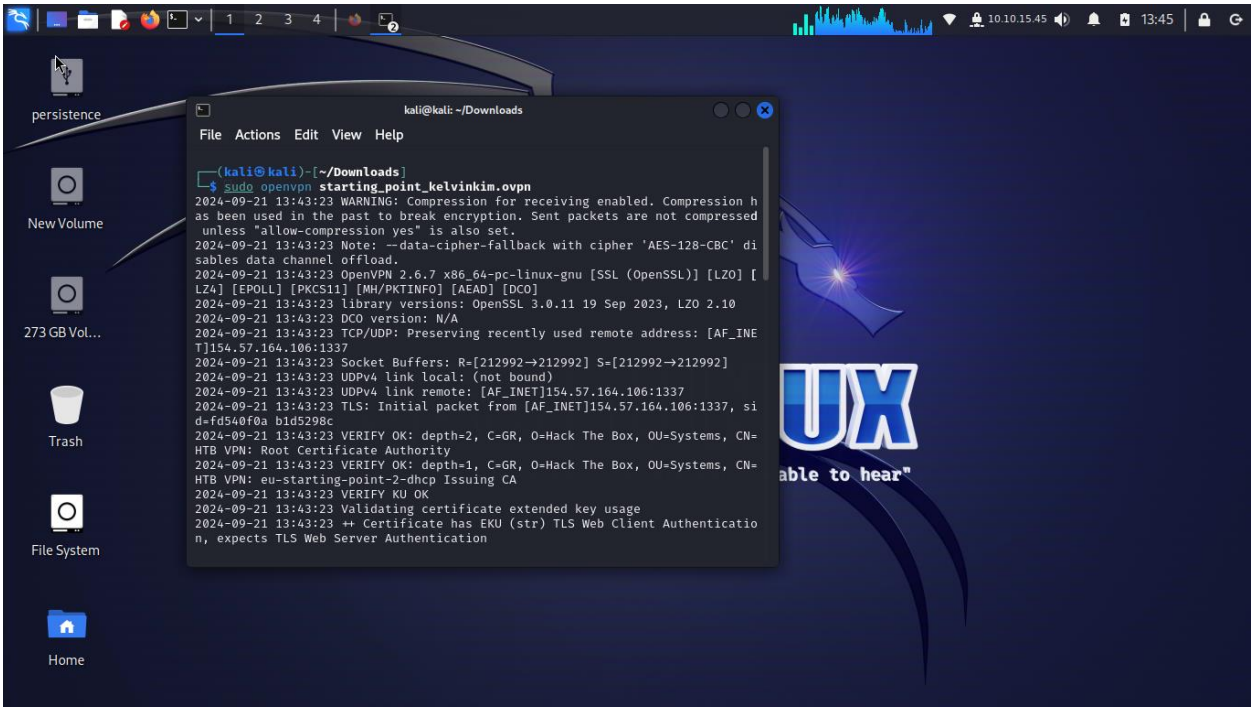
NAME: Kelvin Kimotho

LinkedIn: kelvin kimotho

GETTING STARTED ON HACK THE BOX TIER 0

Meow

- First, I learnt how to connect to the hackthebox vpn using the following command. "sudo openvpn vpn_file"



- Then to test connectivity i just need to ping the target IP using this command. "ping IP"
- The first step in penetration testing is enumeration which involves documenting the state of the target machine by gaining information about it.
- We start by scanning for open ports on the system to see what services are running and which can we exploit. We use nmap a tool.
- " nmap -sV IP" is the command format, where V flag gives us the version of the services running and also the operating system information.
- For telnet services that usually run on port 23, we can use the telnet tool and try connect.

" telnet Target_IP" is the command. We can use username "root" to login without a password.

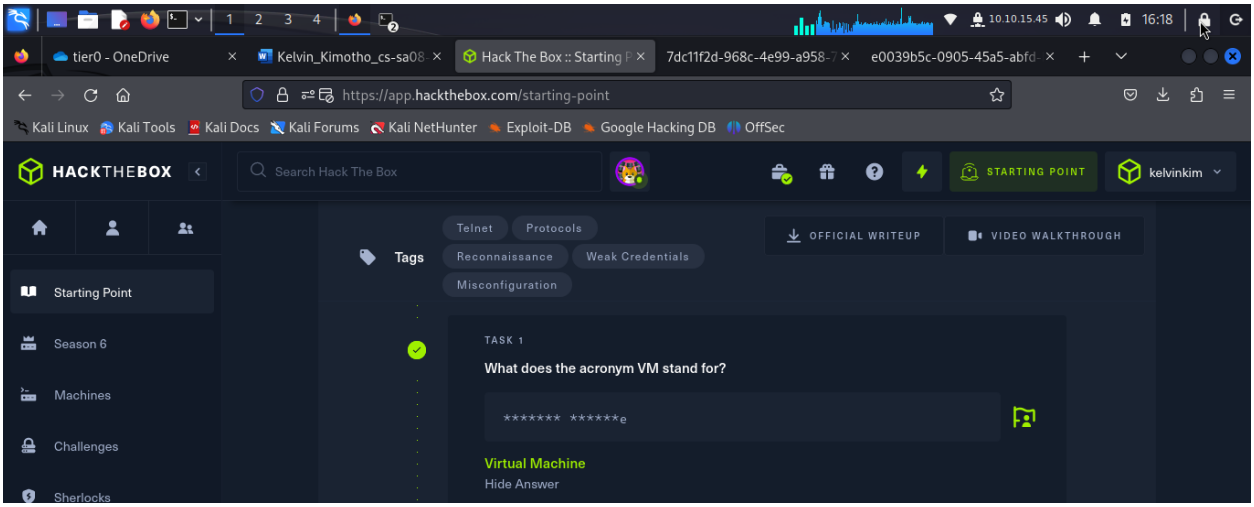
- After a successful login, we can use ls command to list contents.
- Cat command to read contents of a file.

Then i went ahead and answered the questions that followed.

Task 1

Question: What does the acronym VM stand for?

Answer: Virtual Machine



Task 2

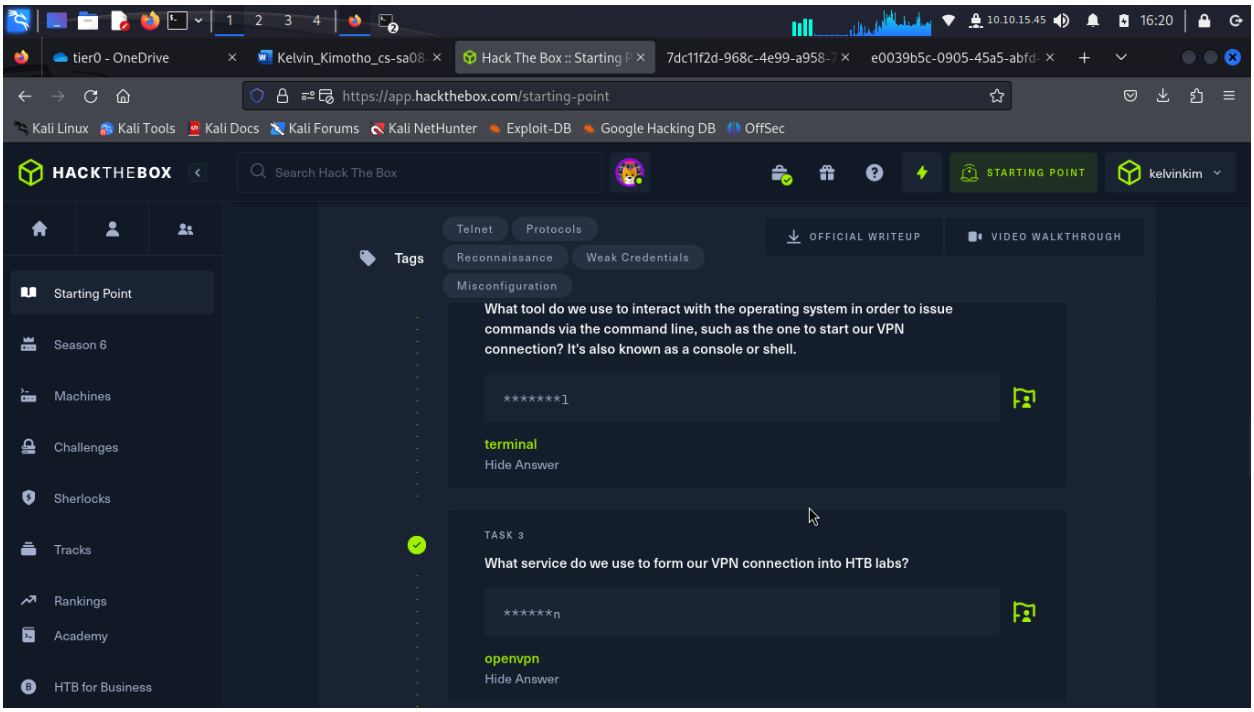
Question: What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.

Answer: Terminal

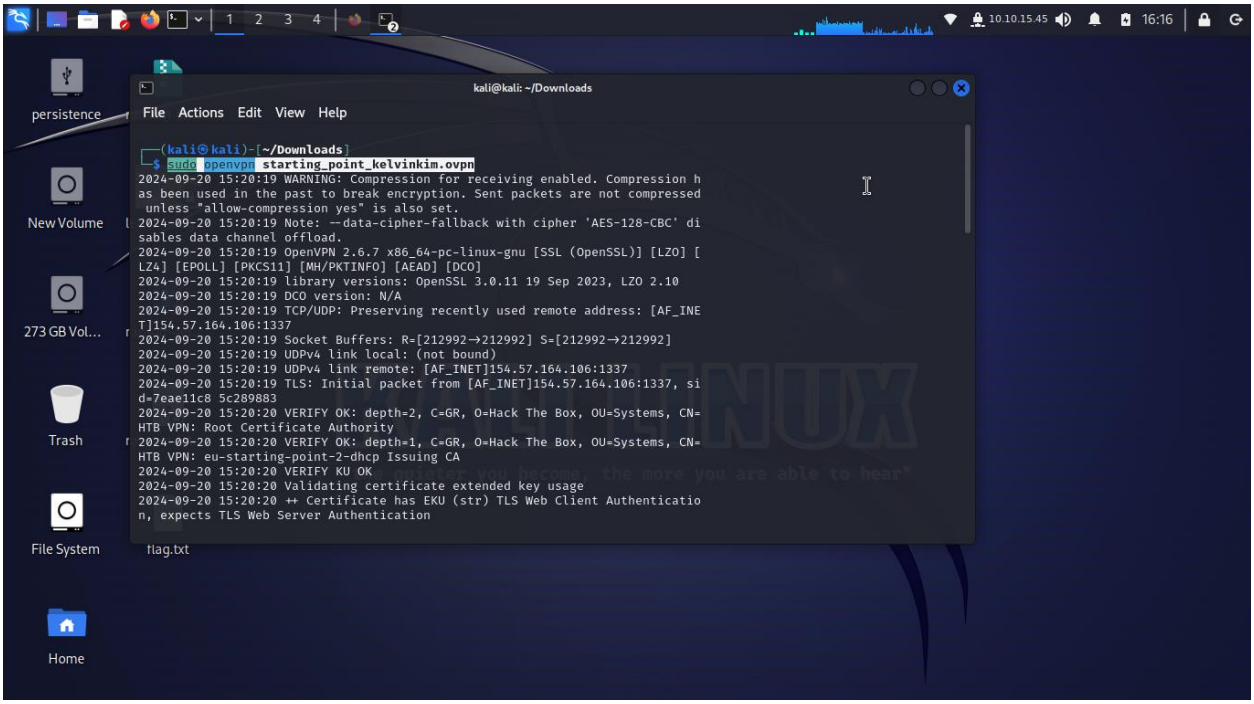
Task 3

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

Answer: Openvpn



I connected to hackthebox vpn via my linux machine terminal.



Task 4

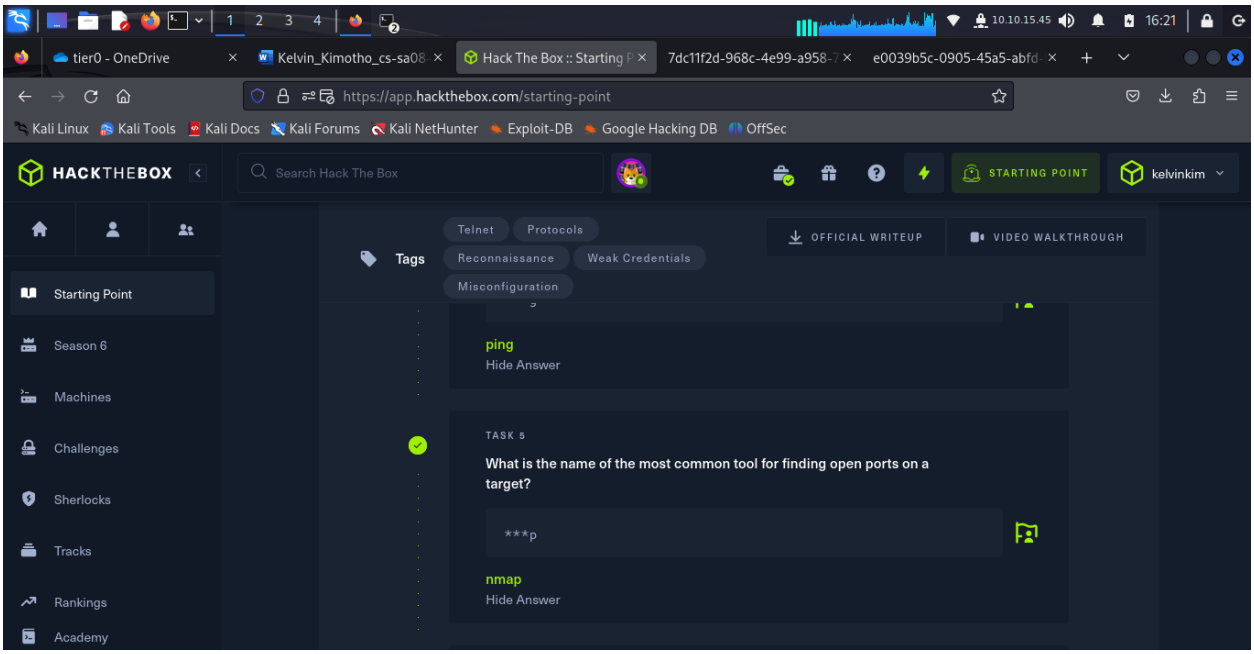
Question: What tool do we use to test our connection to the target with an ICMP echo request?

Answer: ping

Task 5

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

Answer: Nmap



Task 6

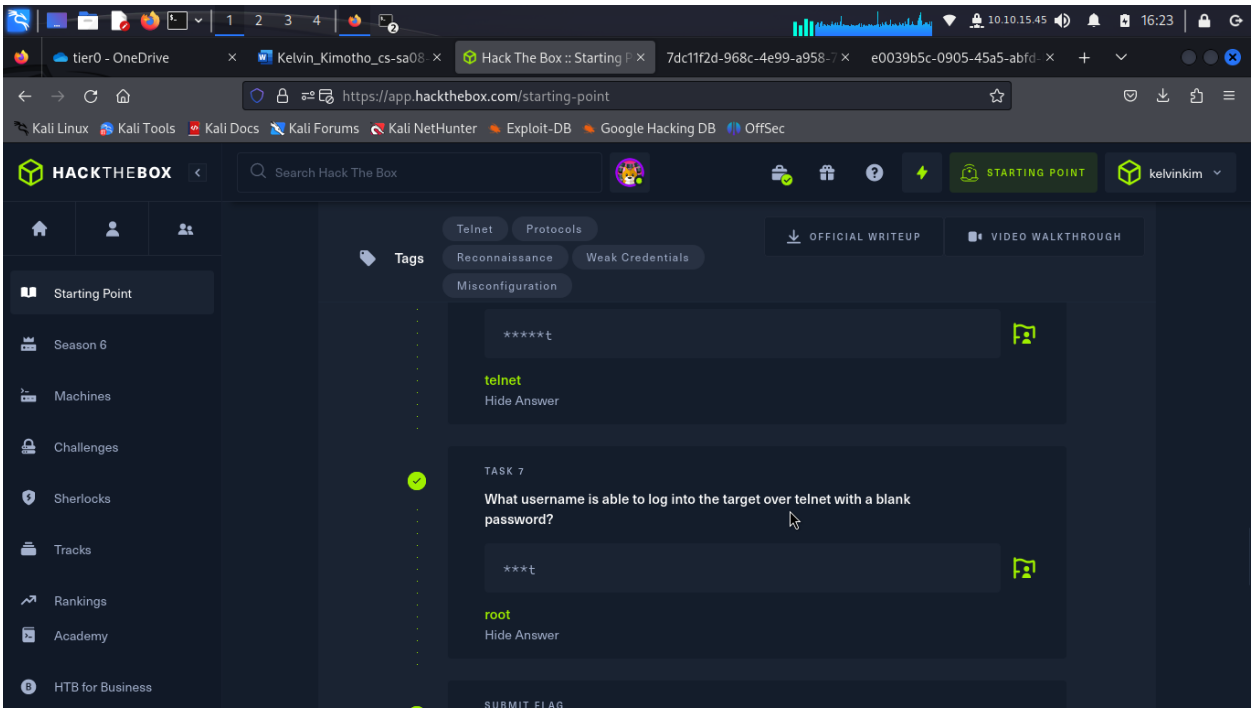
Question: What service do we identify on port 23/tcp during our scans?

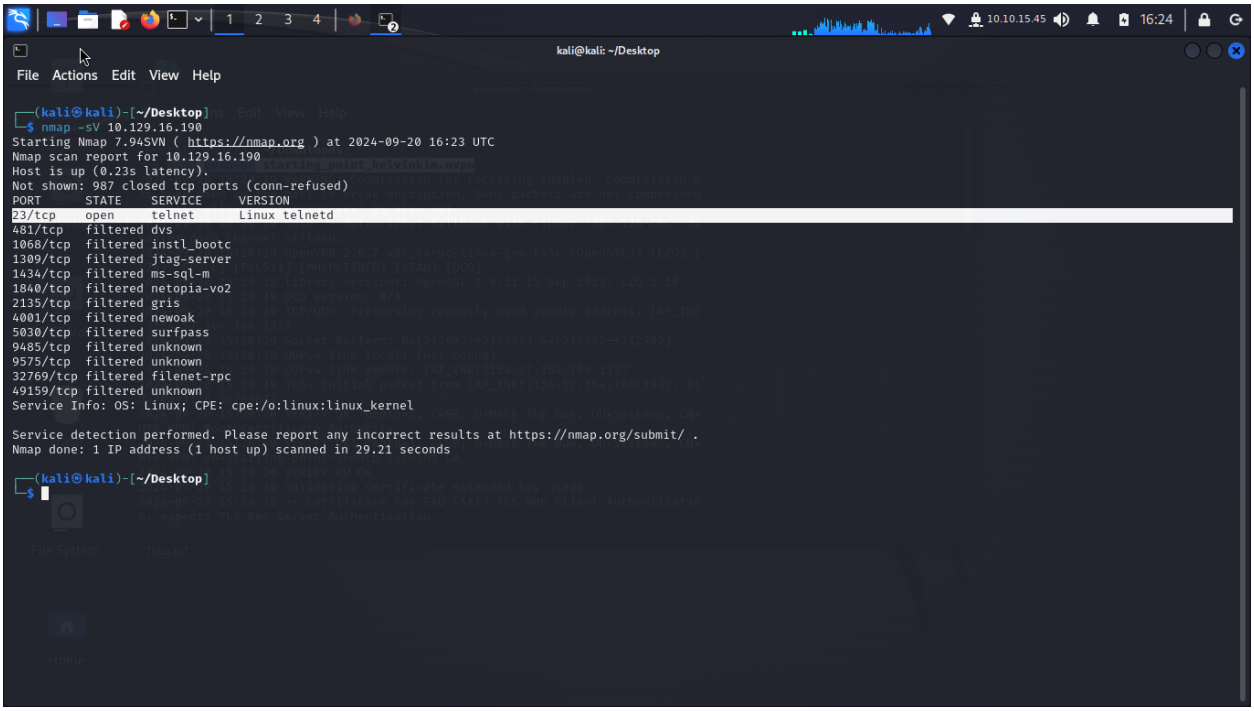
Answer: Telne

Task 7

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

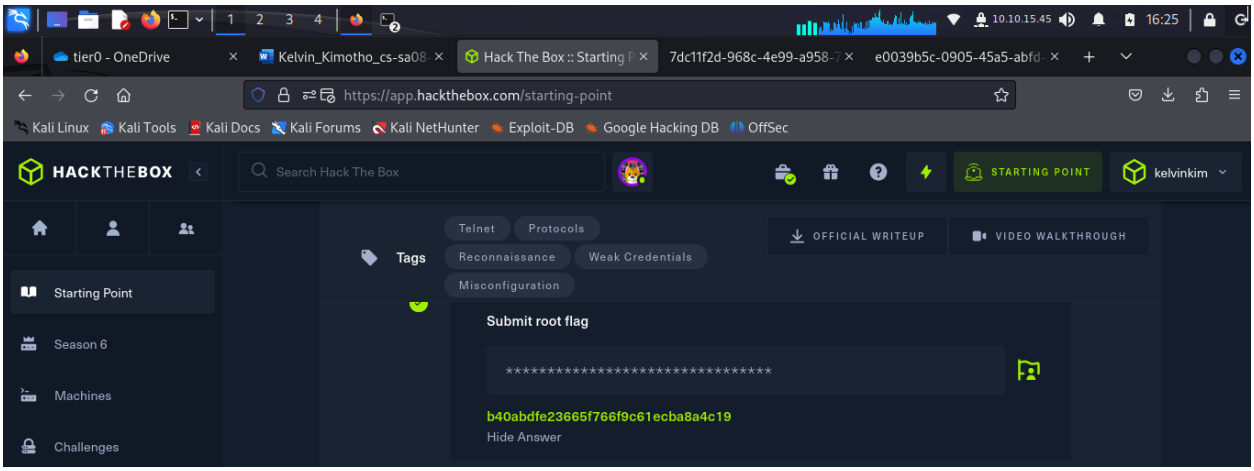
Answer: root

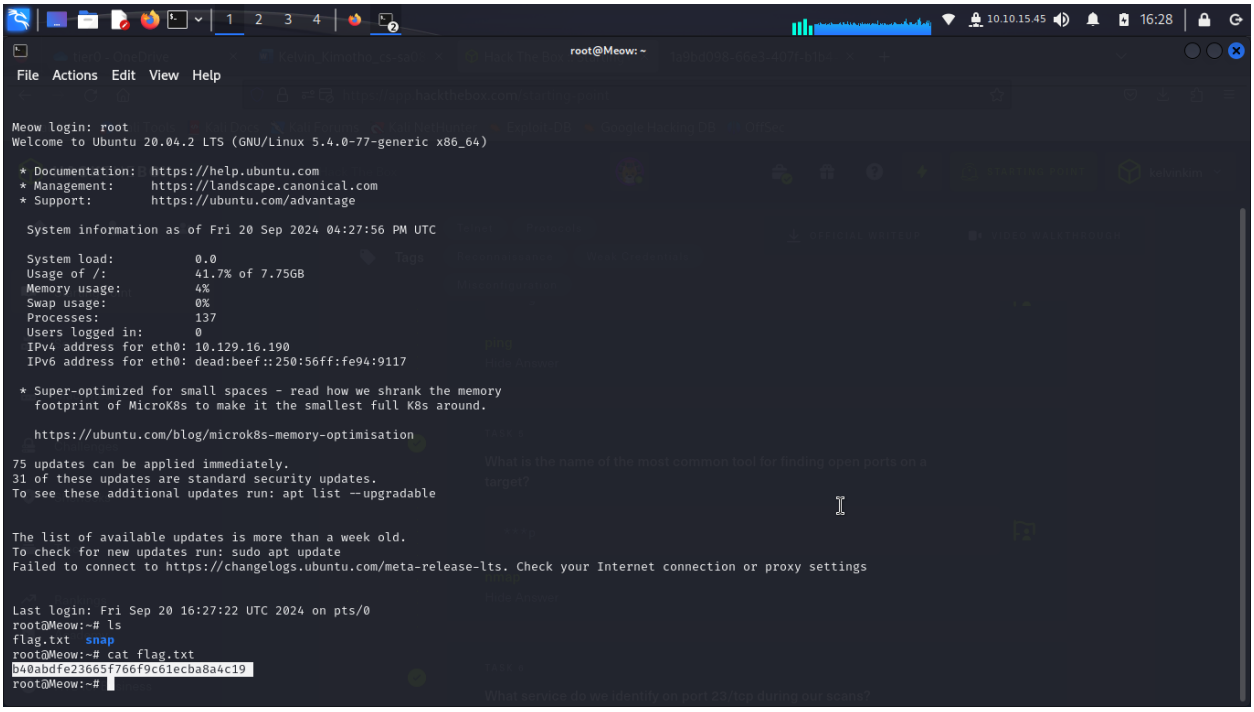




Question: Submit root flag

Answer: b40abdfe23665f766f9c61ecba8a4c19





Fawn

- This is where I learnt About FTP (file transfer protocol) used for simple file transfer tasks.
- It is used to transfer files from a server to a client within the same network.
- FTP may allow authentication using passwords and usernames in plain text.
- One can connect to an ftp server using username "anonymous" if the server allows it.
- We can secure FTP with SSL or use SSH (ssh file transfer protocol) SFTP.

- Traffic via FTP can be intercepted during man in the middle attack. The contents of the files can be read since they are in plain text.
- FTP runs on port 21.
- SSH on port 22
- webservers run on port 80.
- For enumeration we first ping the target IP. "ping Target_IP"
- Then use Nmap to see the open ports. "Nmap Target_IP"
- Adding -sV flag reveals more information including the Version of the server and the os information.

To gain foothold.

- We type ftp -? command to see more on how to use it.
- Then use "ftp Target_IP" to connect to the target.
- We can use anonymous username followed by any password to login if the server is misconfigured to allow this.
- Once in, we can type, help, --help to see the commands available for us users.
- We can use man command to see more on how to use a given tool available for us. e.g. "man get"
- We use ls to list contents.
- We use get command to download files from the server to our local machine.

I answered the questions that followed.

Task 1

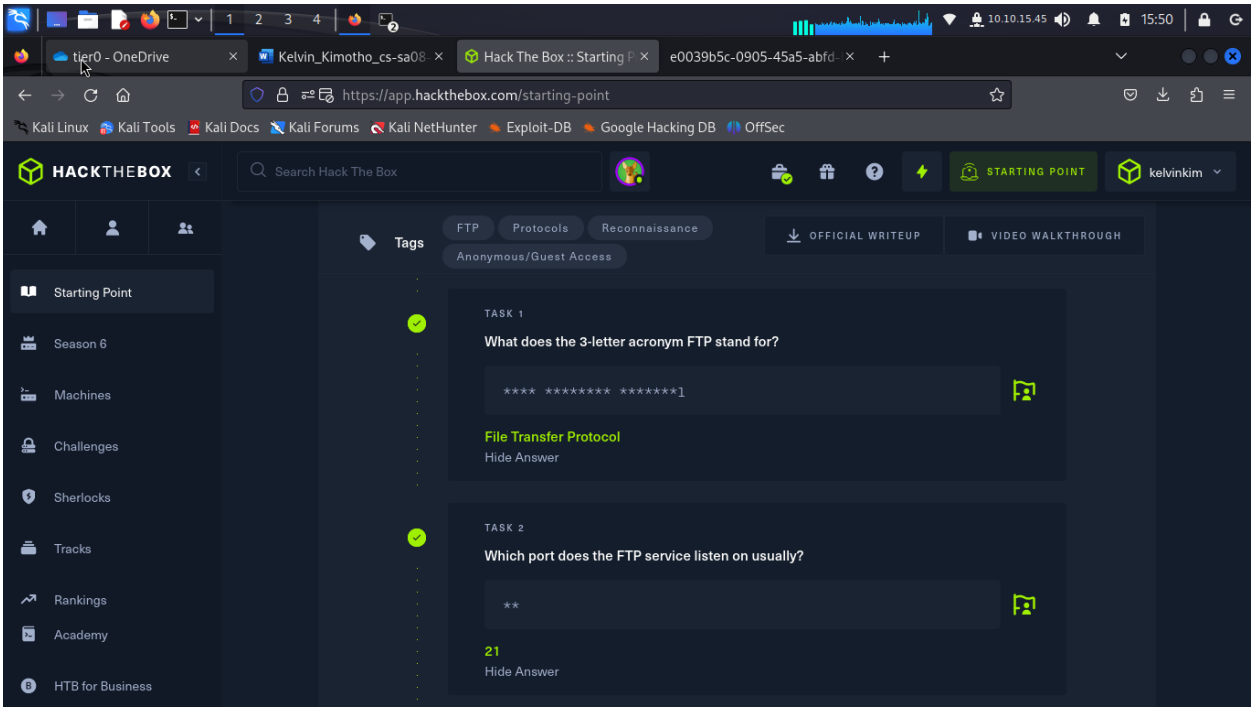
Question: What does the 3-letter acronym FTP stand for?

ANswer: File Transfer Protocol

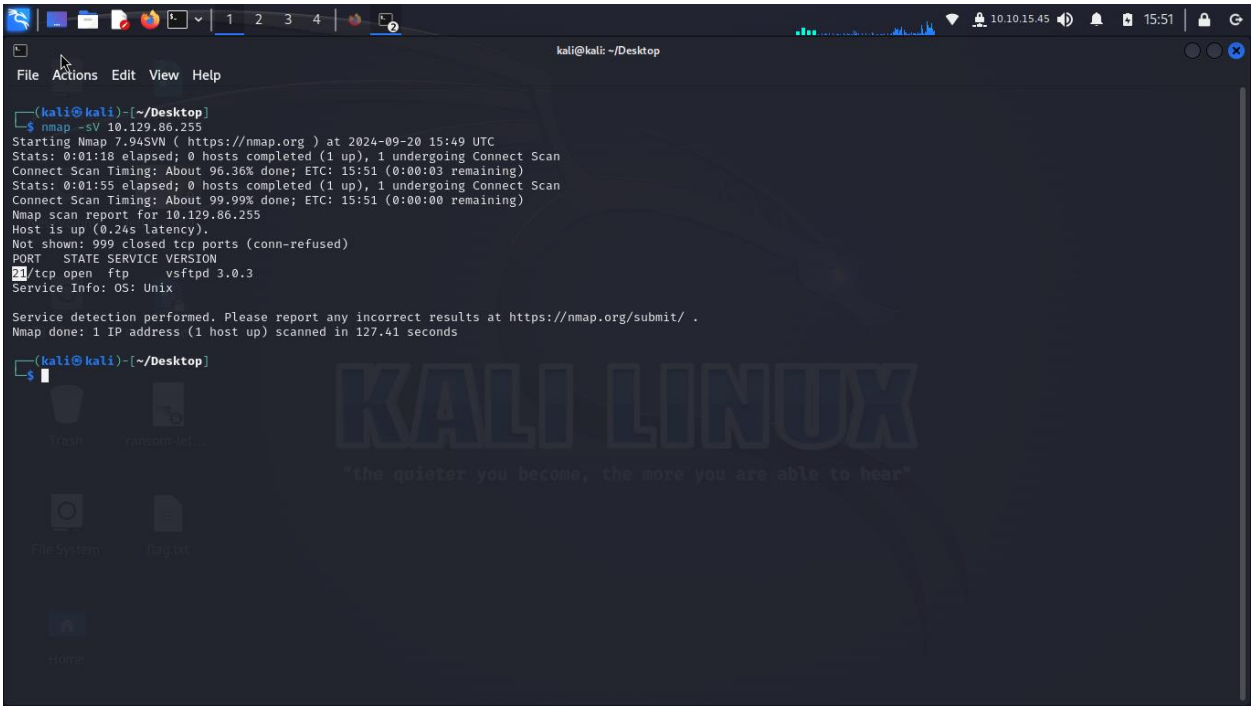
Task 2

Question: Which port does the FTP service listen on usually?

Answer: 21



I confirmed the port where the ftp service was running from on the spawned machine.



Task 3

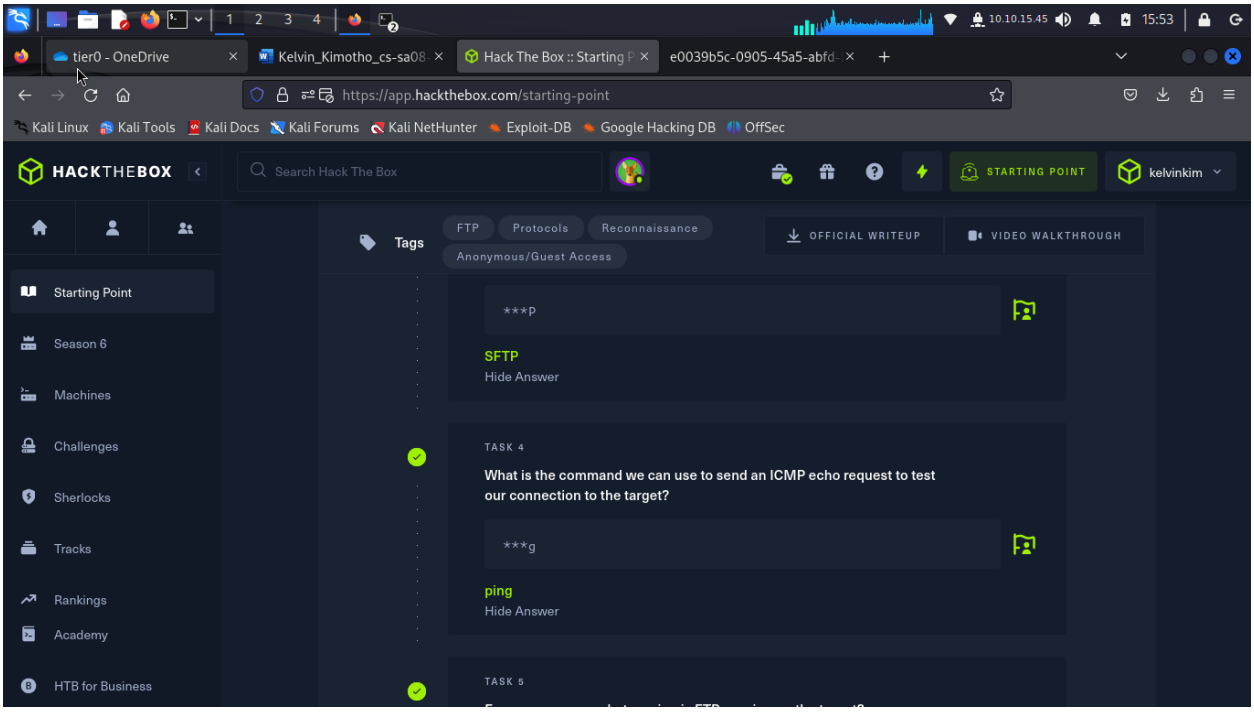
Question: FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

Answer: SFTP

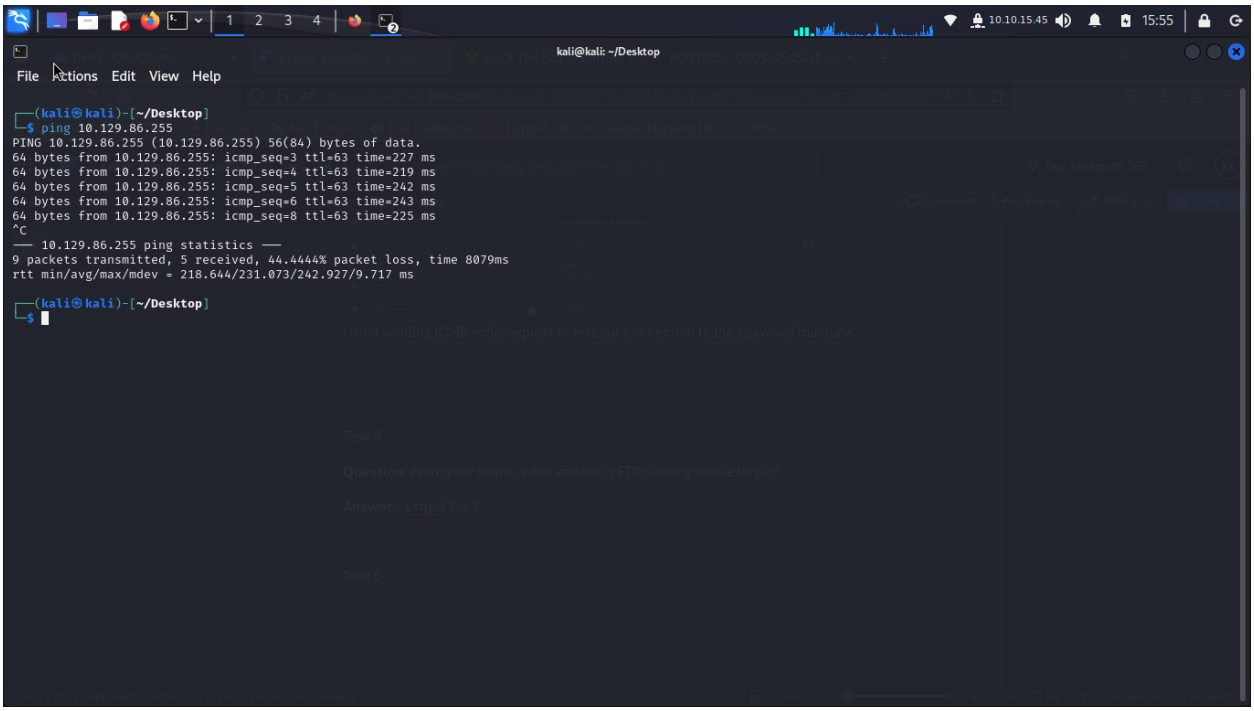
Task 4

Question: What is the command we can use to send an ICMP echo request to test our connection to the target?

Answer: ping



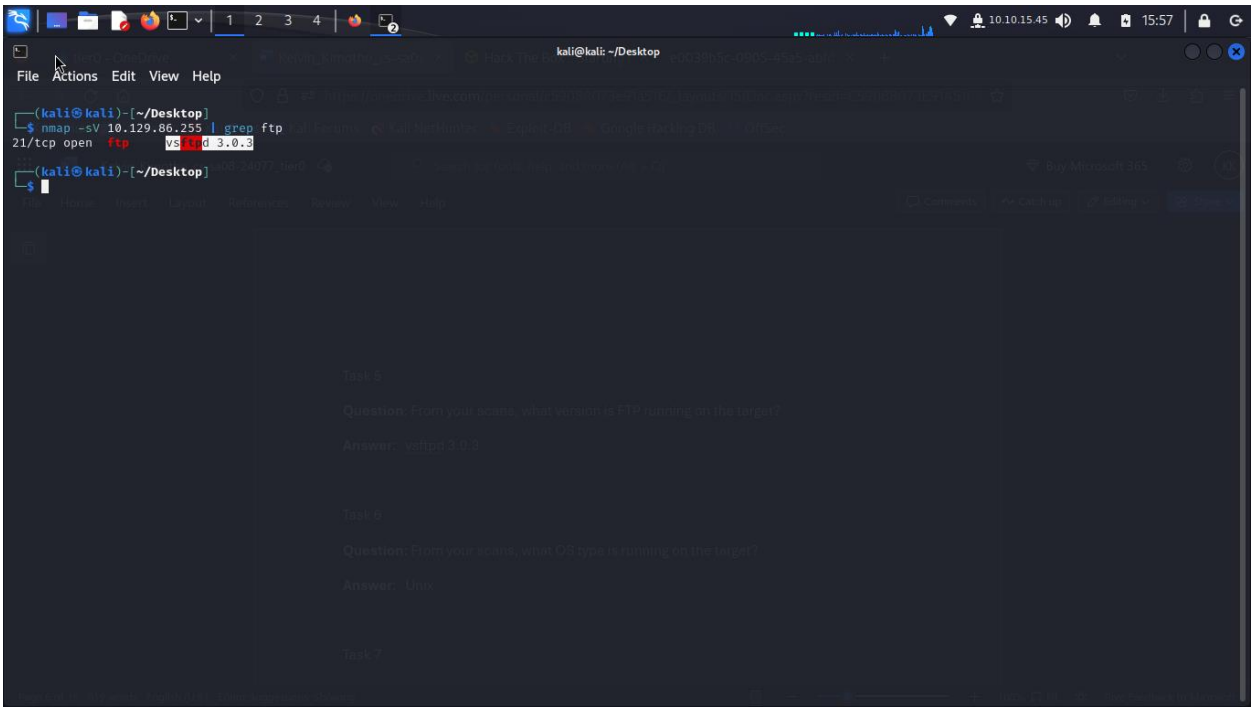
I tried sending ICMP echo request to test our connection to the spawned machine.



Task 5

Question: From your scans, what version is FTP running on the target?

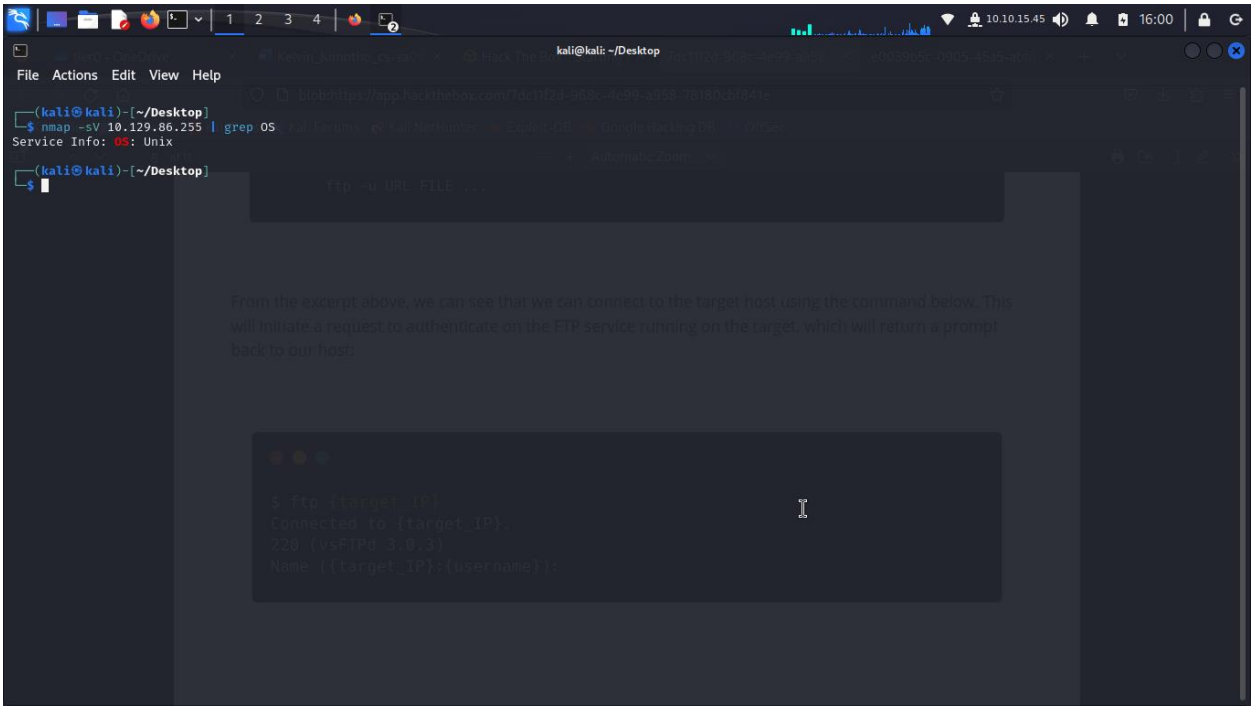
Answer: vsftpd 3.0.3



Task 6

Question: From your scans, what OS type is running on the target?

Answer: Unix



Task 7

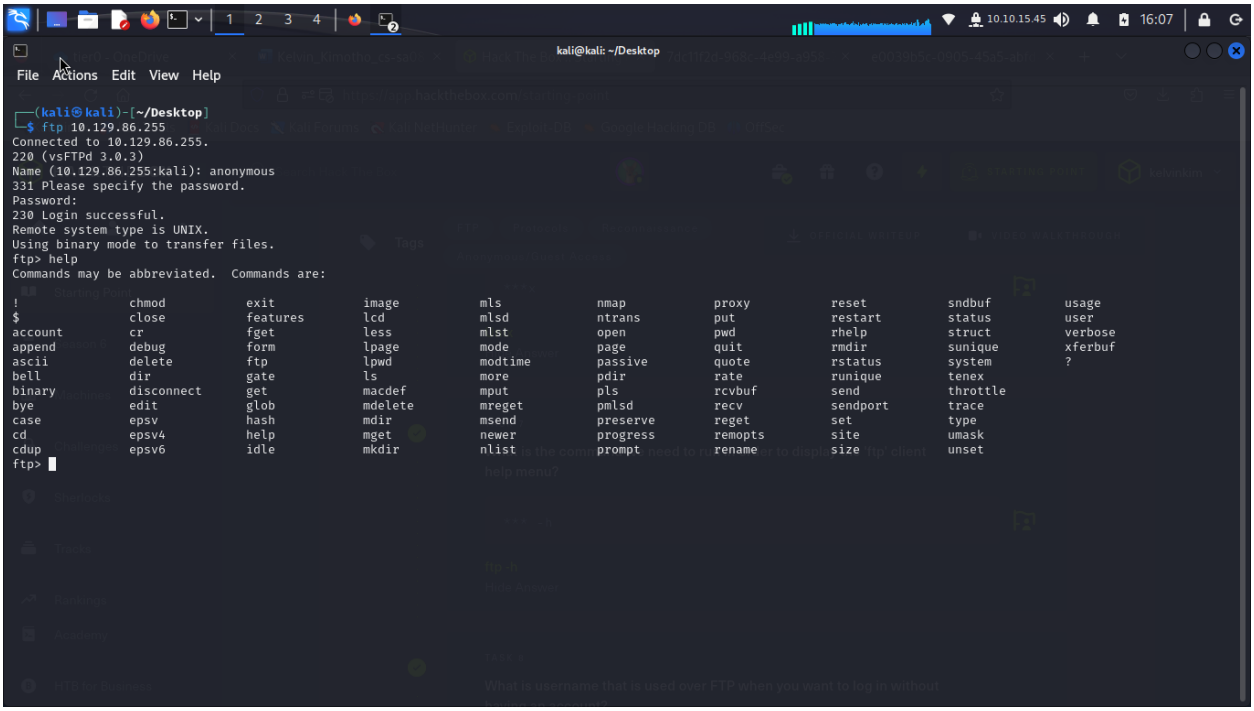
Question: What is the command we need to run in order to display the 'ftp' client help menu?

Answer: ftp –h

Task 8

Question: What is username that is used over FTP when you want to log in without having an account?

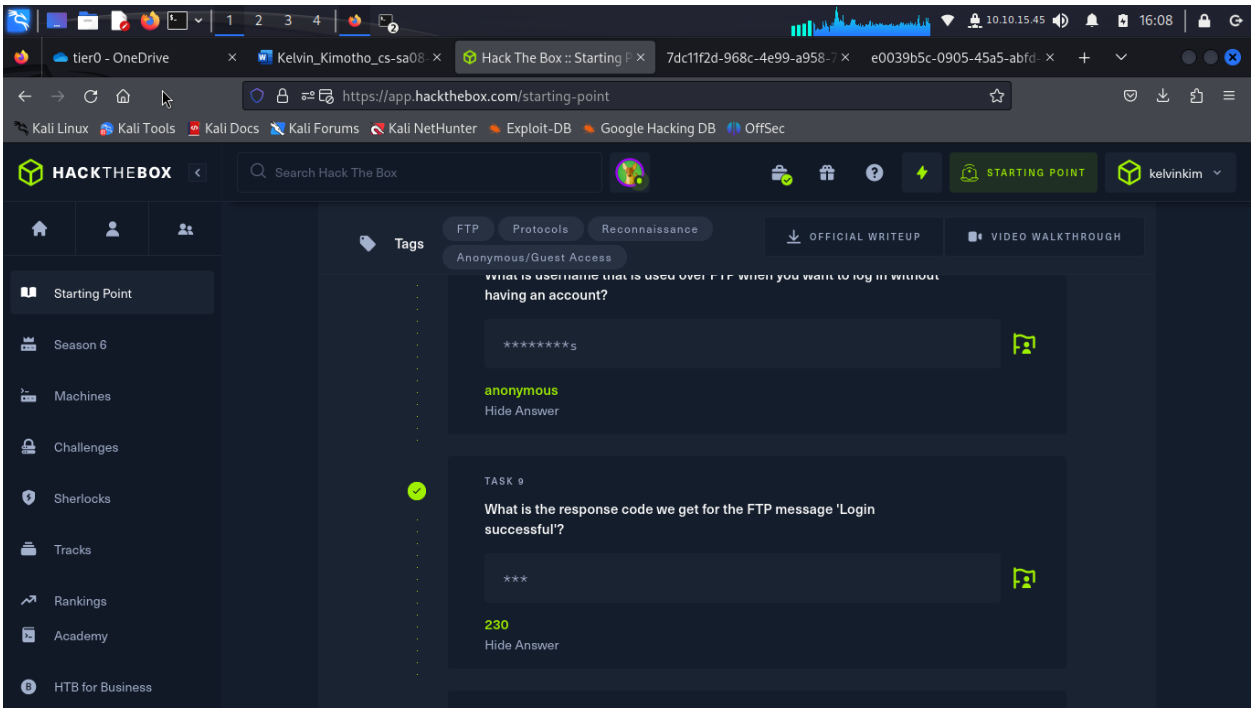
Answer: Anonymous



Task 9

Question: What is the response code we get for the FTP message 'Login successful'?

Answer: 230



Task 10

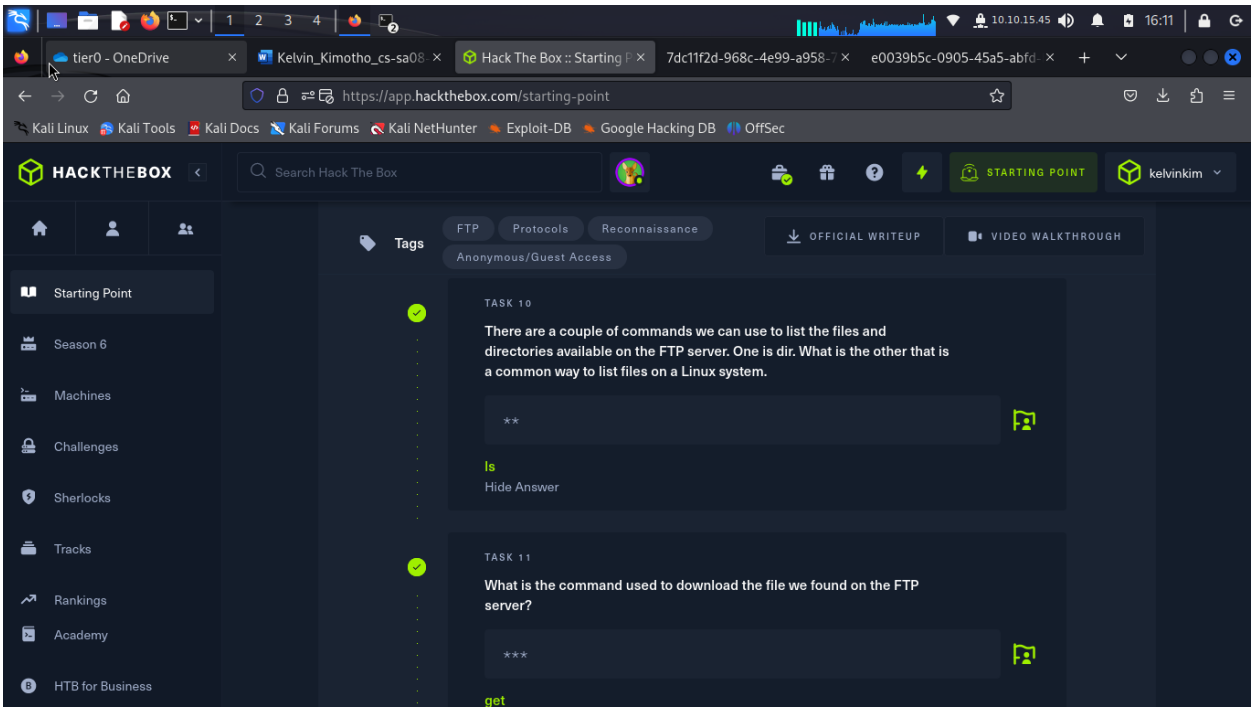
Question: There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.

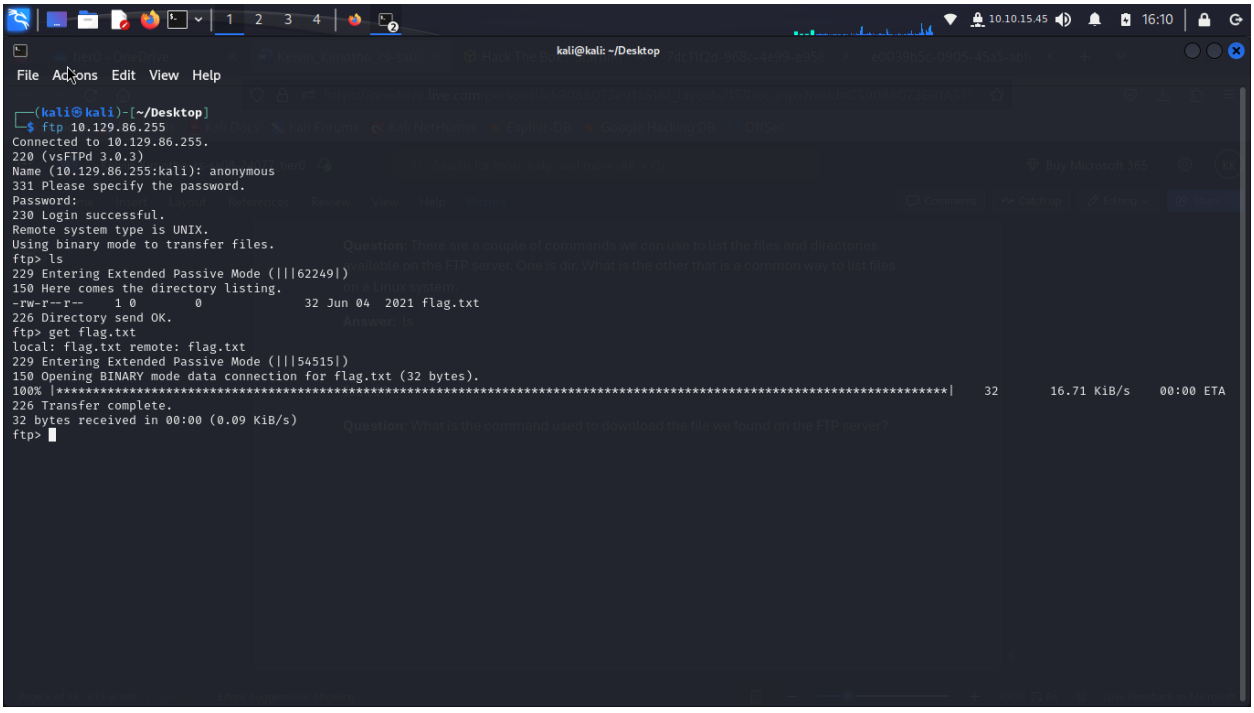
Answer: ls

Task 11

Question: What is the command used to download the file we found on the FTP server?

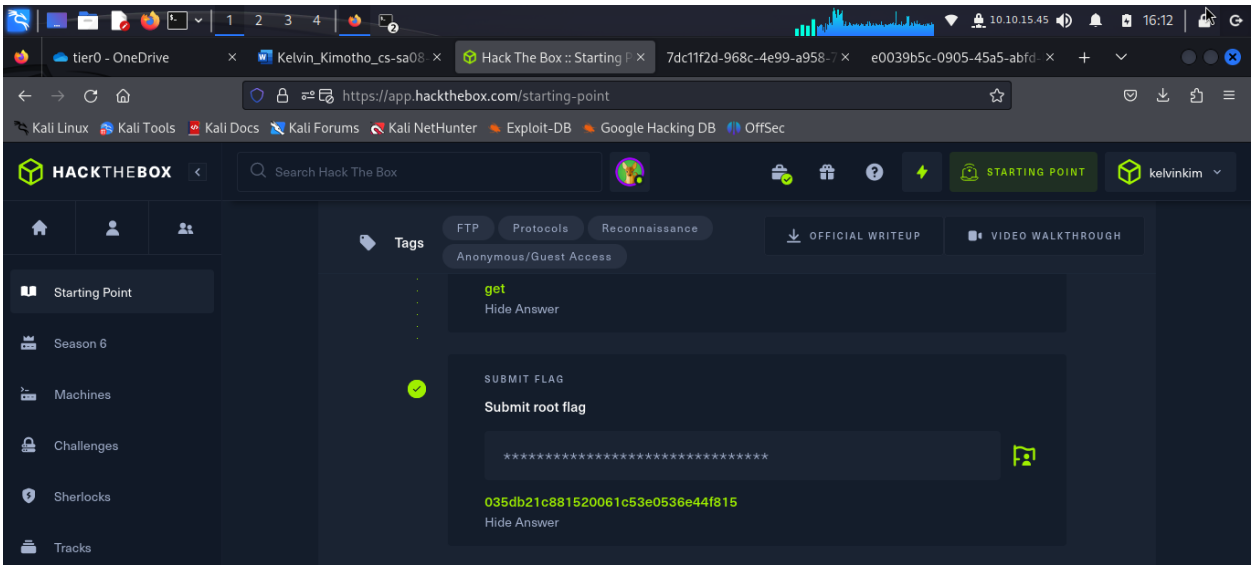
Answer: get

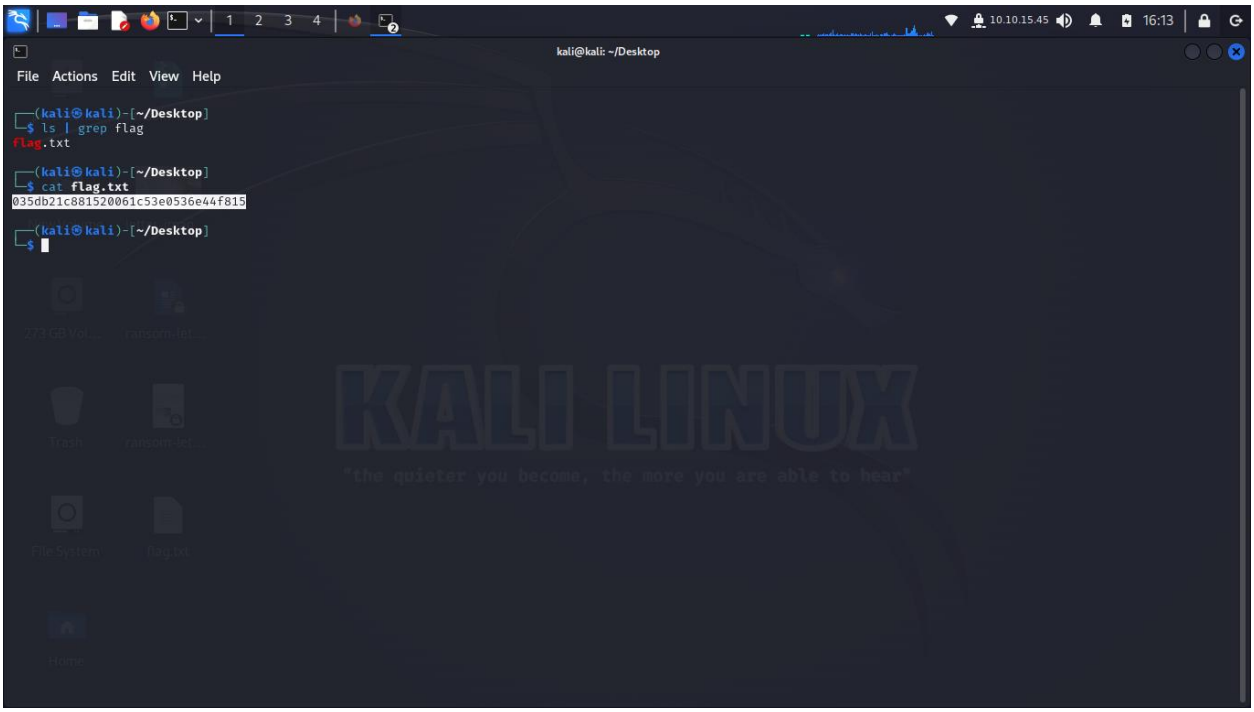




Submit root flag

Answer: 035db21c881520061c53e0536e44f815





Dancing

- Here, I learnt on how to transfer files between computers on the same network.
- SMB (server message block) for example is a protocol mostly in windows machines used share files and other resources between end points in a network.

- SMB protocol runs on port 445.
- SMB runs on the application layer as per the OSI model.
- Microsoft SMB Protocol is often used with is NetBIOS over TCP/IP.
- A share is an SMB-enabled storage on the network.
- A share can be accessed by any client with an address to the server and the correct username and password.
- We can use guest account or even make anonymous logins incase the network admin misconfigured.

For Enumeration,

- We will use Nmap to scan for open ports and services running there. -sV flag will allow us get both the service and the version running.

  "nmap -sV Target_IP"

- We can access the shares in the target machine from our Linux attacking machine using "smbclient" tool.
- To install it we run " apt-get install smbclient"
- And to run it, this is the format. "smbclient -L Target_IP", where the -L helps us Select the targeted host for the connection request.
- Without the correct login creds, we can login as quest or anonymous users.

Shares present in our target may include,

- ADMIN$ share which is a hidden share that allows system administrators to have remote access to every disk volume on a network connected system.
- IPCS$ share is used for inter process communication via named pipes.
- c$ is an administrative share where the operating system resides.

To gain access to a share we use smbclient.

- We use the following command format "smbclient \\\\Target_IP\\share"
- We need to have the correct credentials to access the share, otherwise we will always get an error "NT_STATUS_ACCESS_DENIED"

Human made shares are prone to attacks, we should always focus on those.

- After a successful login, we use "help" command to see what we can do in the shell.
- we have commands like, cd to navigate through directories, ls for file listing, get for downloading contents/files, exit for exiting the smb shell,etc.

Then I answered the questions that followed.

Task 1

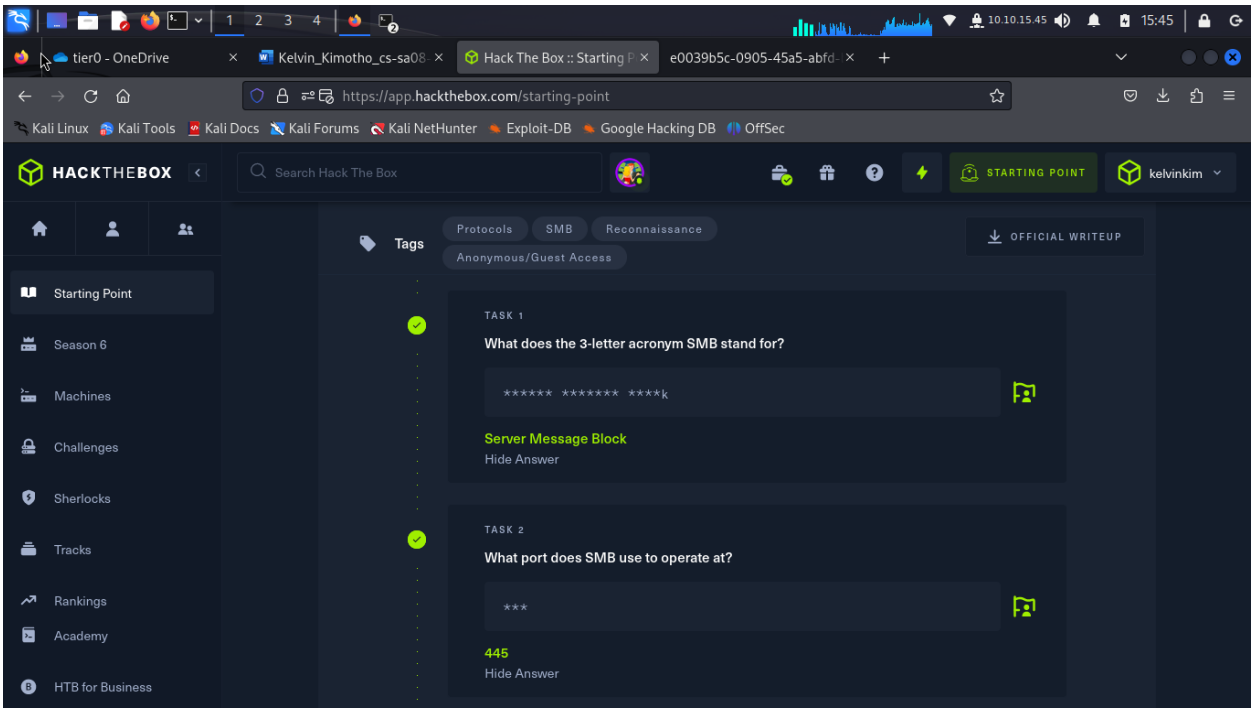
Question: What does the 3-letter acronym SMB stand for?

Answer: server message block

Task 2

Question: What port does SMB use to operate at?

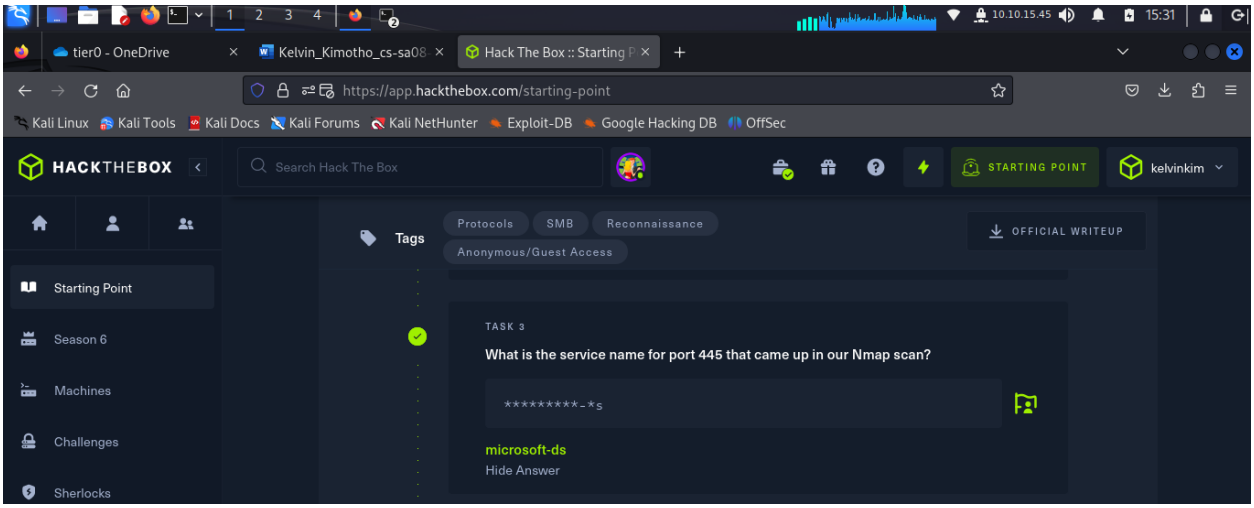
Answer: 445

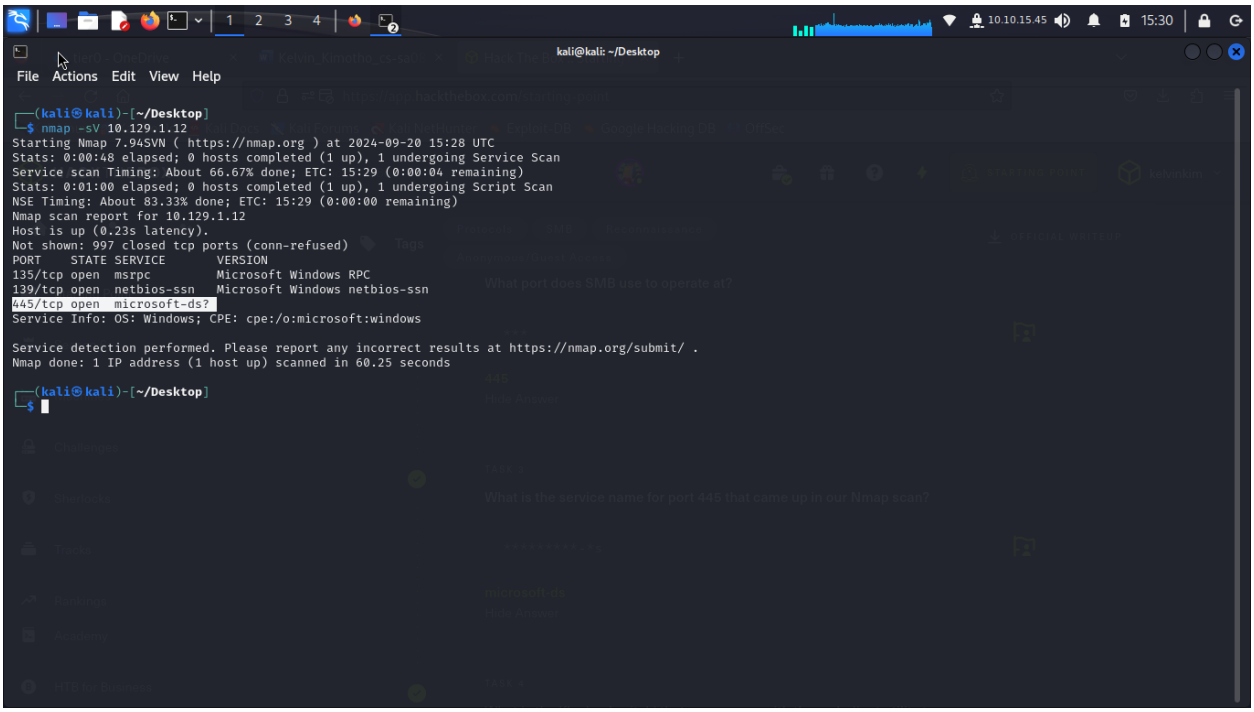


Task 3

Question: What is the service name for port 445 that came up in our Nmap scan?

Answer: microsoft-ds





Task 4

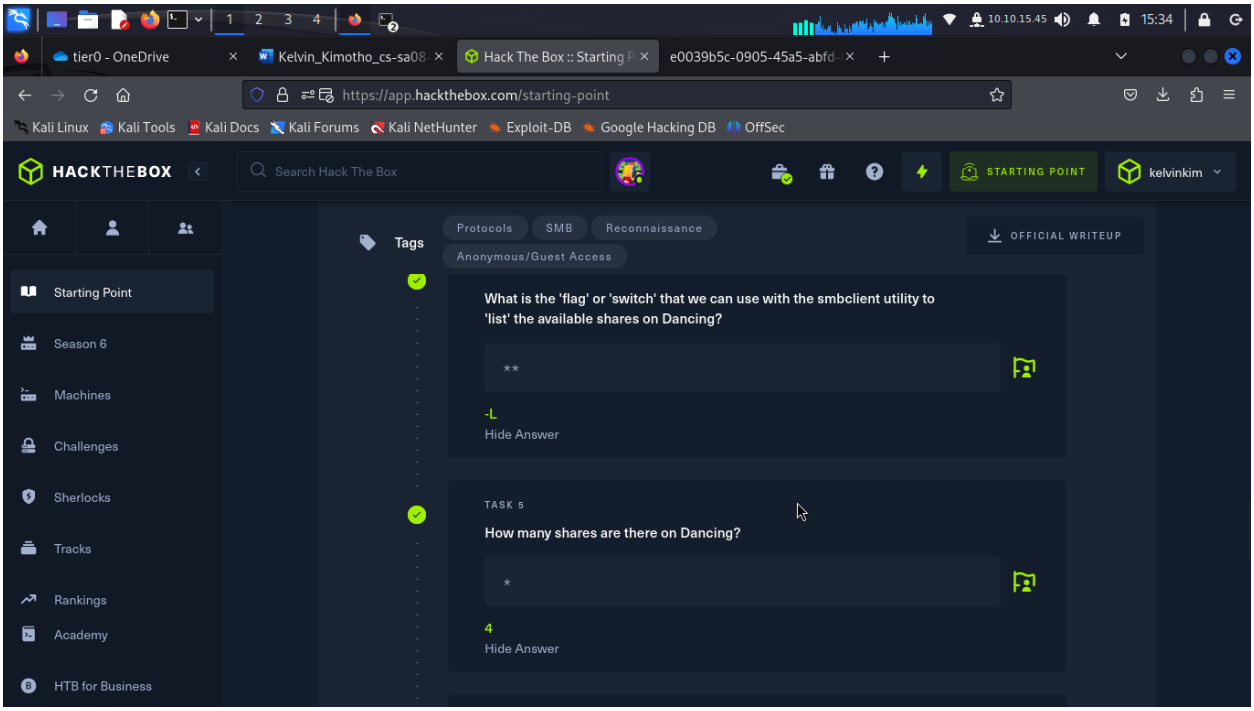
Question: What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

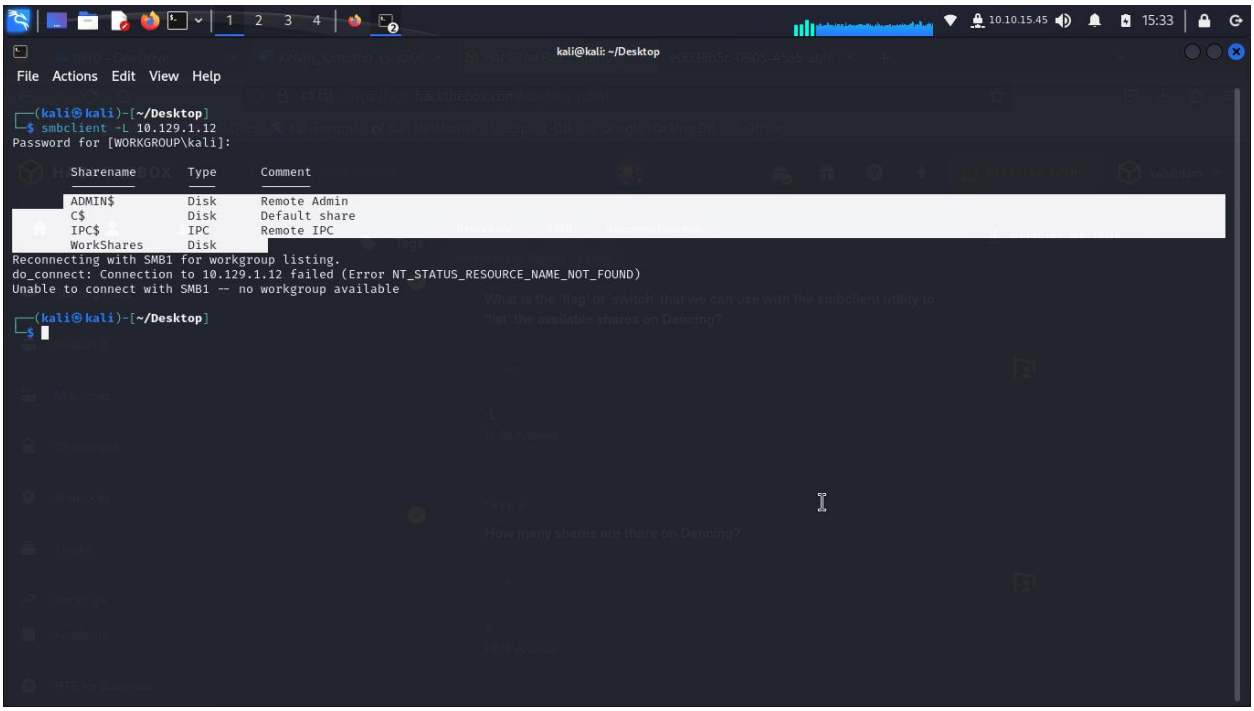
Answer: -L

Task 5

Question: How many shares are there on Dancing?

Answer: 4

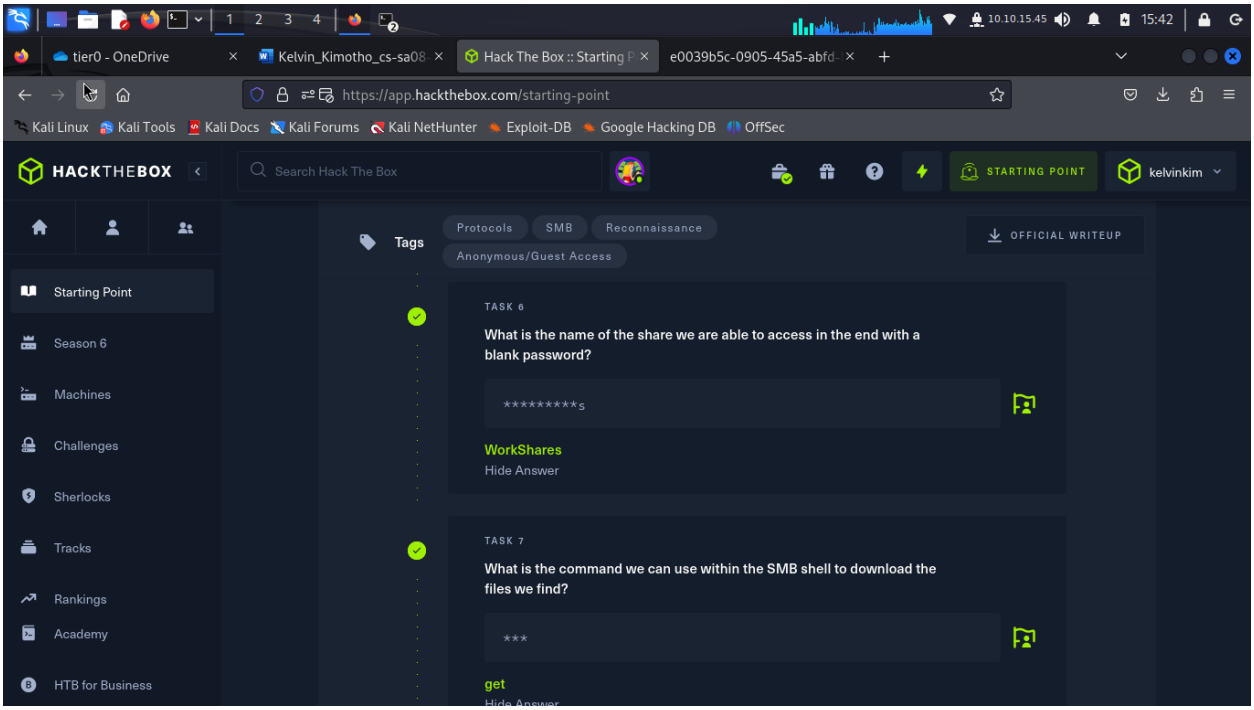




Task 6

Question: What is the name of the share we are able to access in the end with a blank password?

Answer: workshares

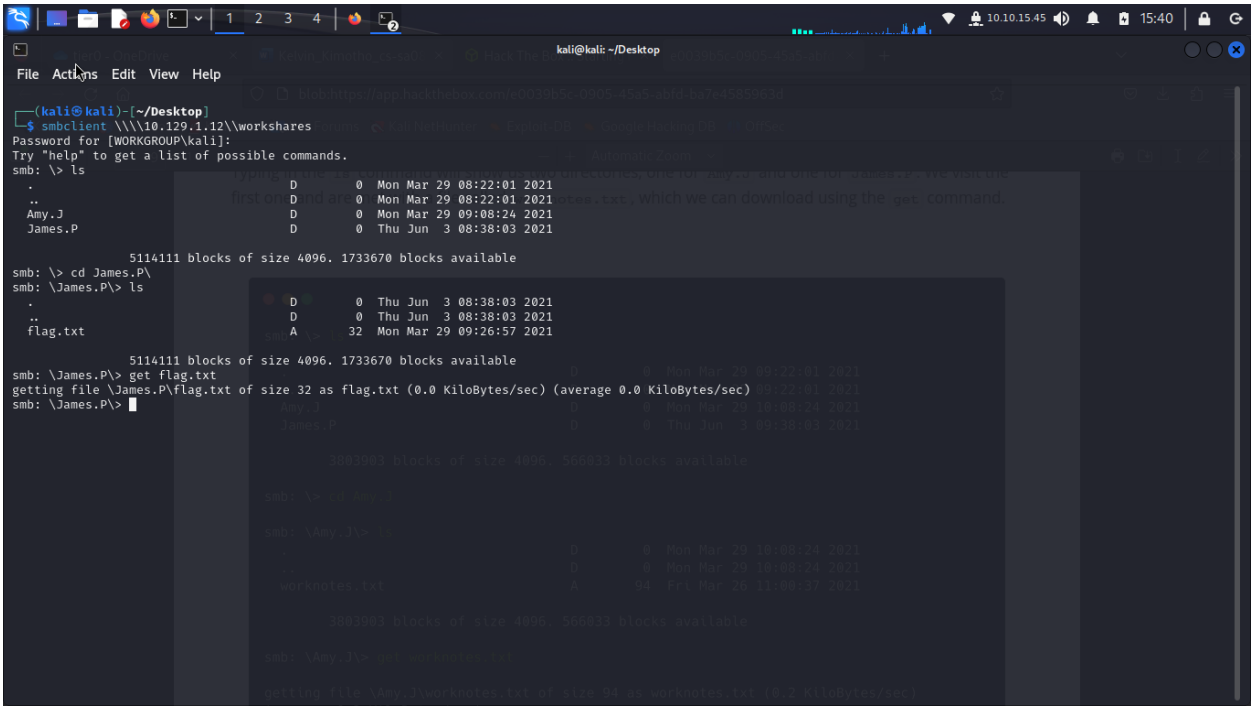


Task 7

Question: What is the command we can use within the SMB shell to download the files we find?

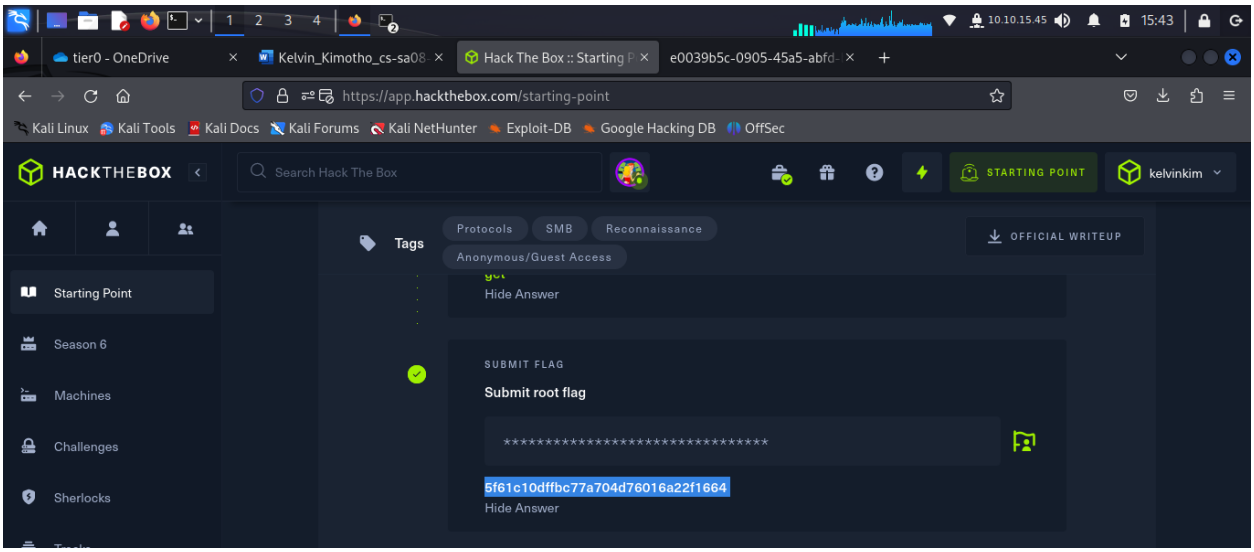
Answer: get

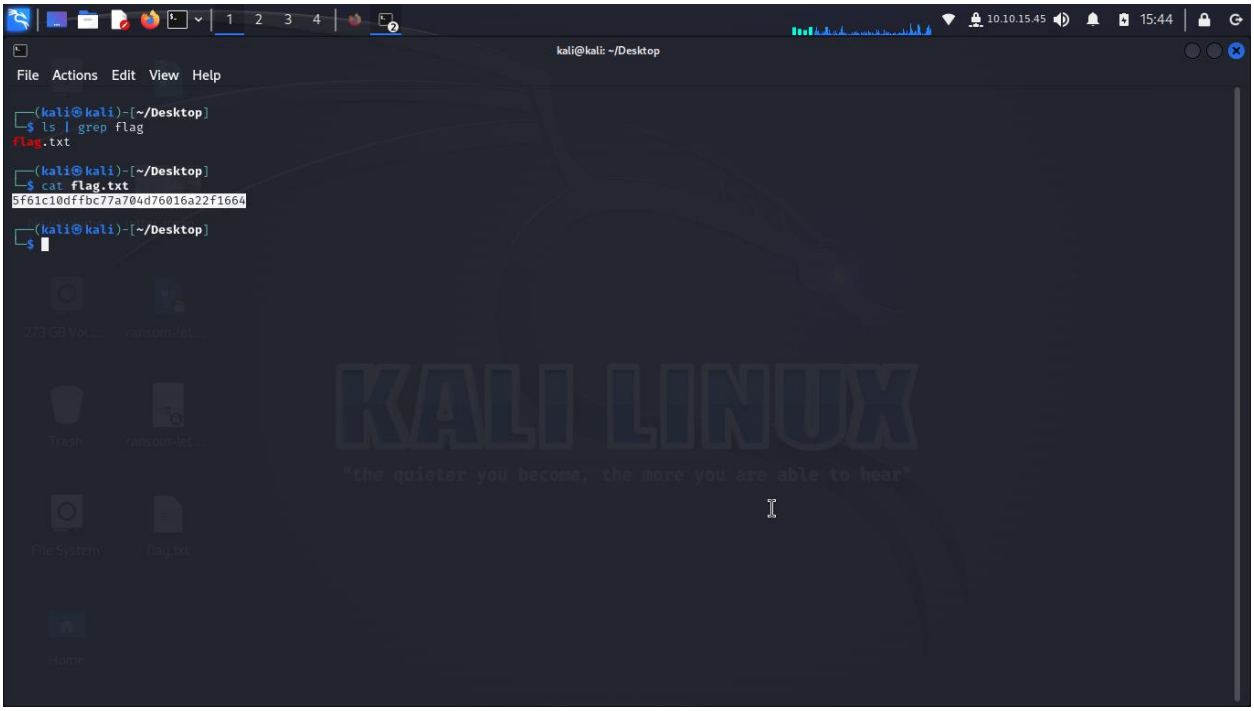
I used get command to retrieve a flag.txt file from a user folder that was in the workshare.



Submit root flag

Answer: 5f61c10dffbc77a704d76016a22f1664





Redeemer

The following is what i learnt under this section.

- A database is a collection of organized information that we can update, manage,etc.
- In-memory databases are those that managed in the RAM system. Like, they rely on primary memory for data storage. An example is Redis.

- Since primary memory is faster than secondary memory, Redis offers efficient and minimal response time.

During the enumeration phase,

- We first ping the target IP to test our connectivity.
- Then we can do a nmap scan to see what ports are running on the target machine.

"nmap -p- -sV IP", where -sV determines both the service and its version

- Redis (Remote dictionary server) is an advanced NoSQL database used as a cache, database and also a message broker.
- Data is stored in dictionary format (in key value pairs).
- CLI (command line interface) is a tool we can use to gain access to Redis's data and also its functionalities.
- The database is stored in the server ram for fast data access.
- To install Redis we can use the following command. "sudo apt install redis-tools"
- we can use "redis-cli --help" gives us switches we can use.
- To specify the host, we are targeting we use the -h flag. An example include, "redis-cls -h Target_IP"
- After a successful connection, we see a prompt in terminal. "Info " command will give use information about the server.
- We then select the target database using it index. " Select INDEX". We will get an ok message if the selection succeeded.
- we can list all the keys present in the database using the command. "keys *"
- we can view the values stored for a corresponding key using the get command followed by the keynote. "get KEY".

I went ahead and answered the questions that followed.

Task 1

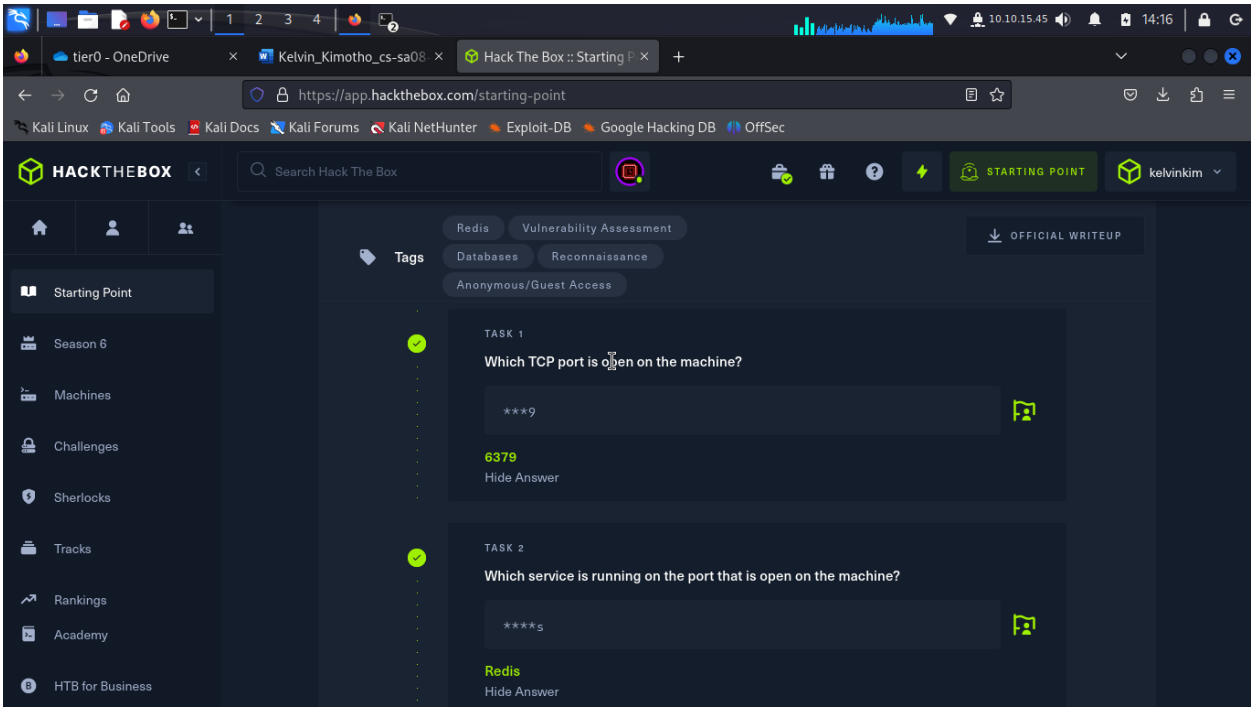
Question: Which TCP port is open on the machine?

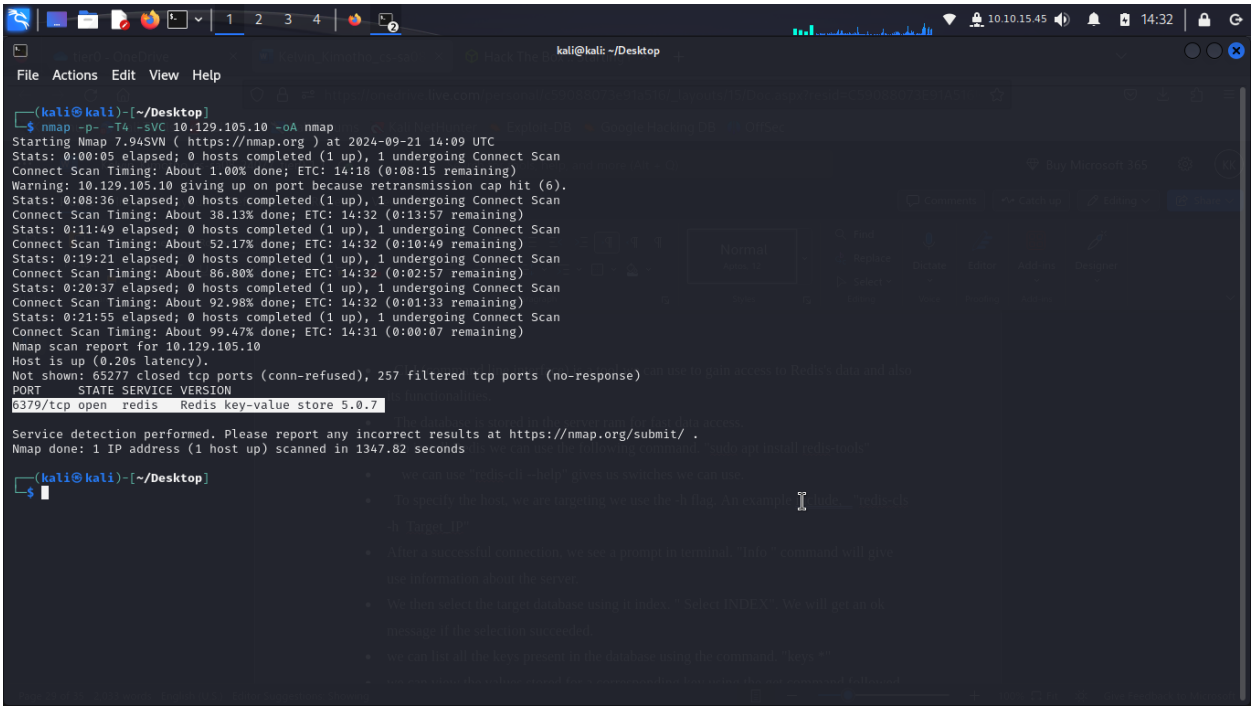
Answer: 6379

Task 2

Question: Which service is running on the port that is open on the machine?

Answer: Redis





Task 3

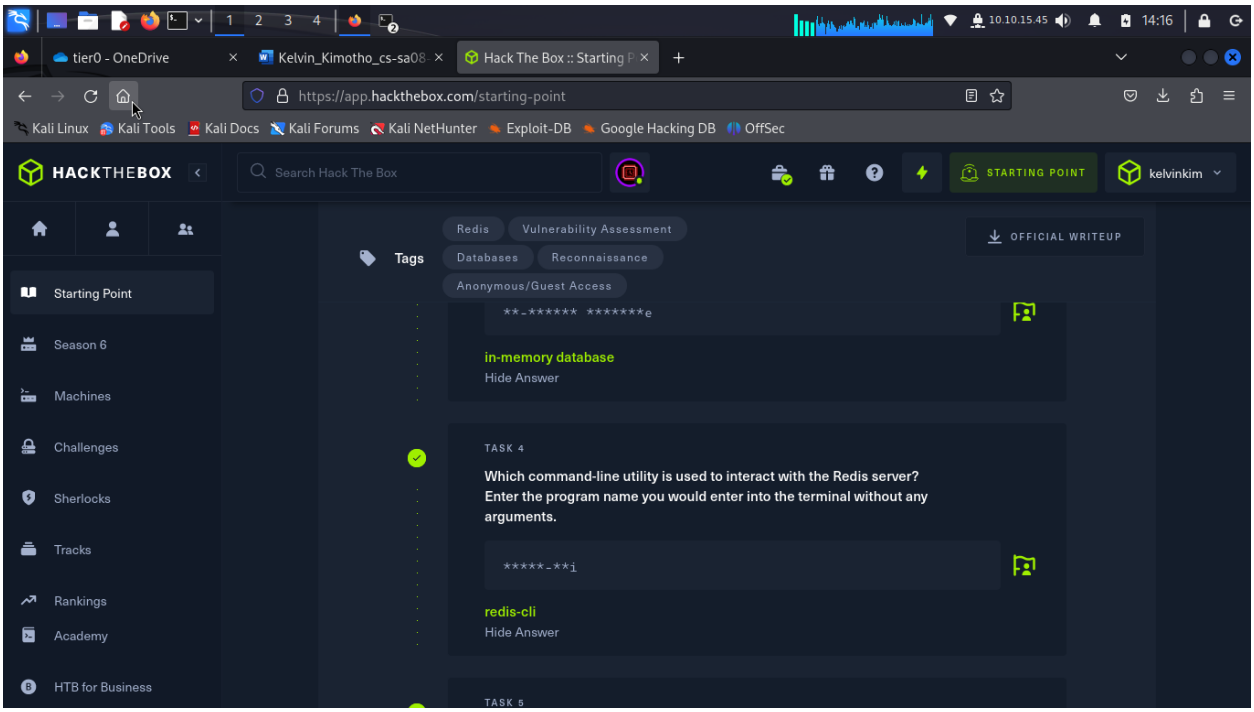
Question: What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

Answer: in-memory database

Task 4

Question: Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.

Answer: redis-cli



Task 5

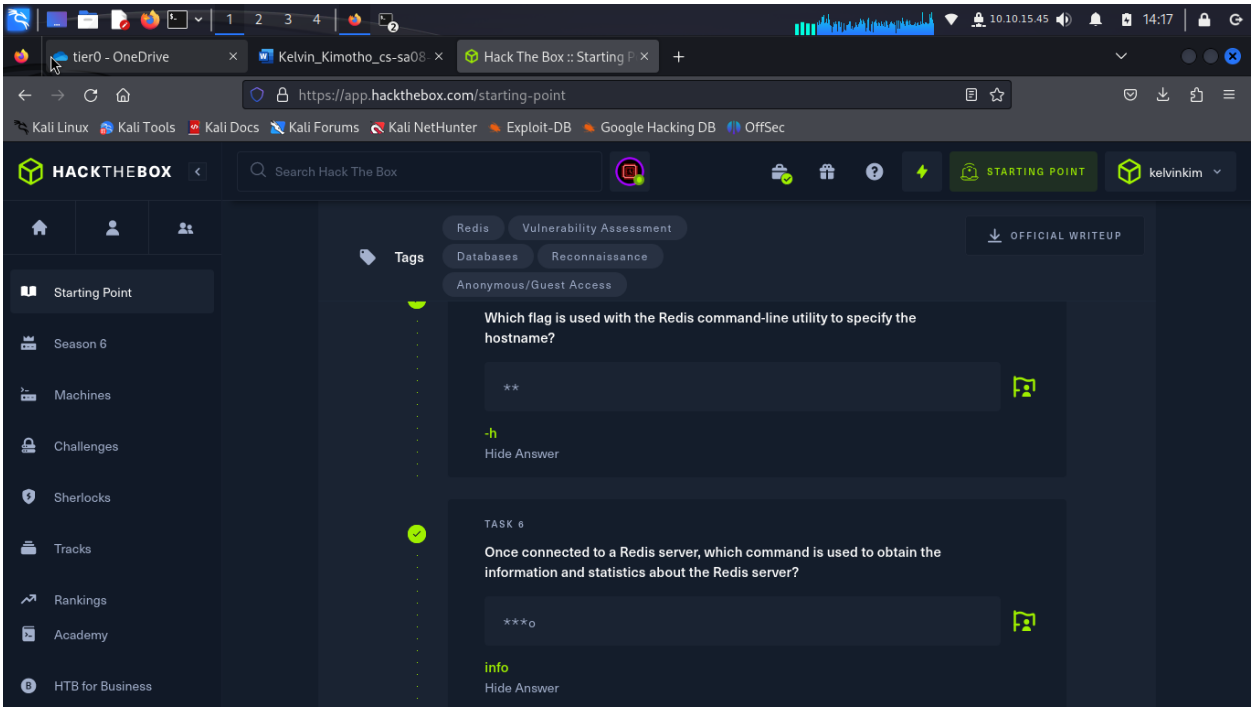
Question: Which flag is used with the Redis command-line utility to specify the hostname?

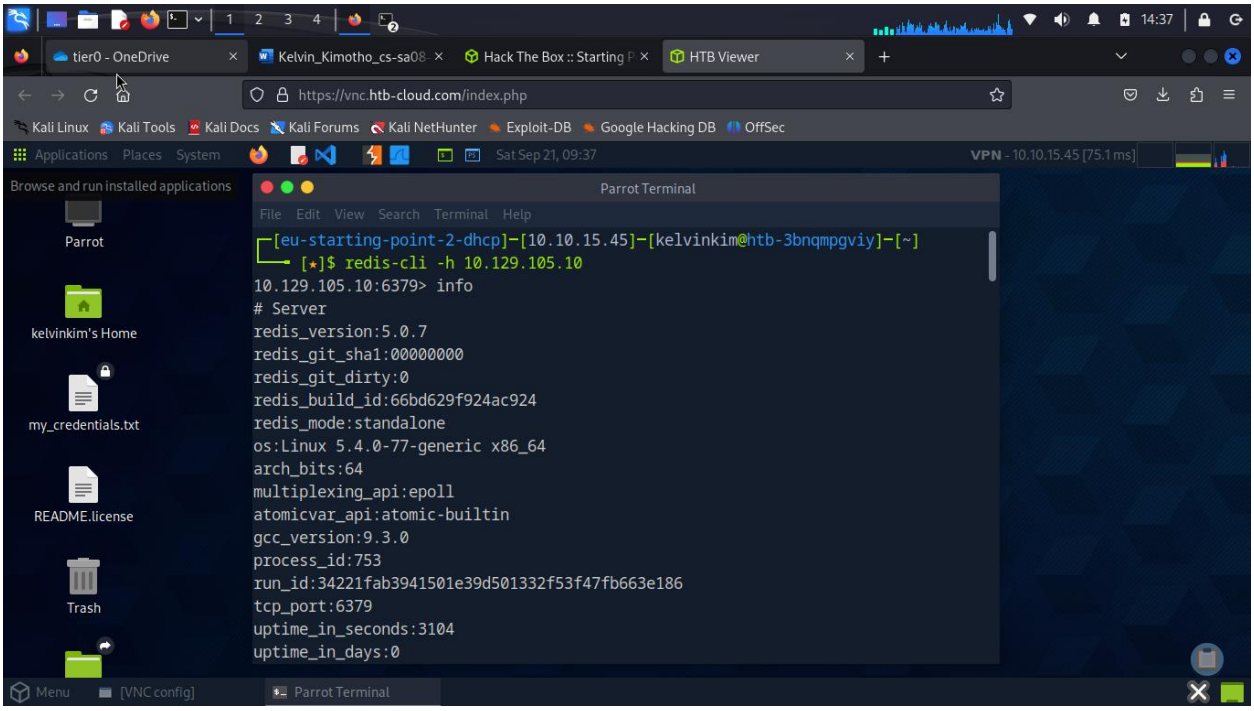
Answer: -h

Task 6

Question: Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?

Answer: info

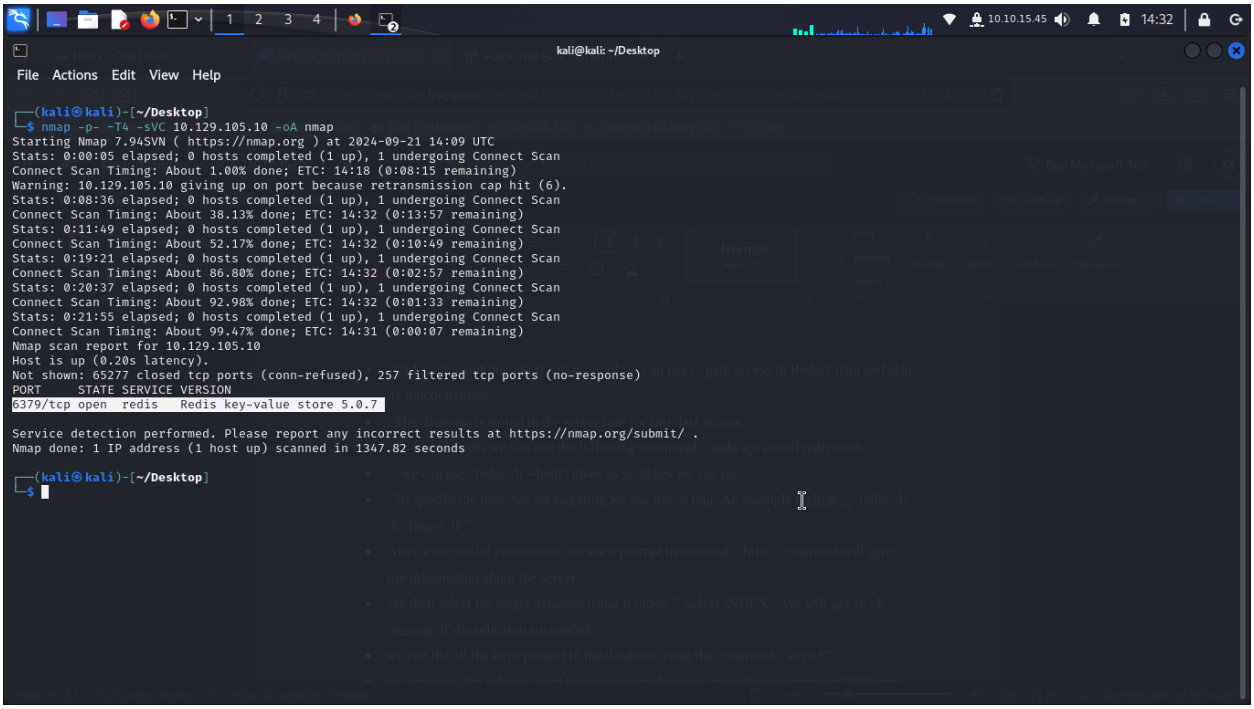




Task 7

Question: What is the version of the Redis server being used on the target machine?

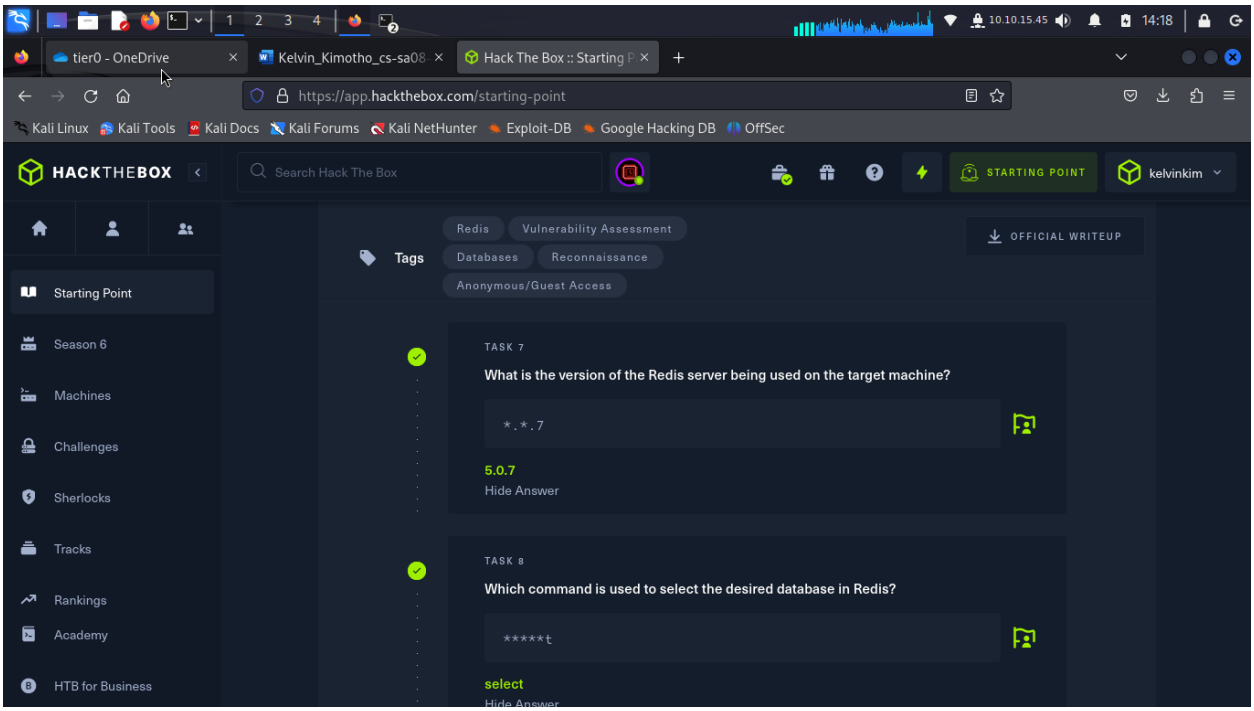
Answer: 5.0.7

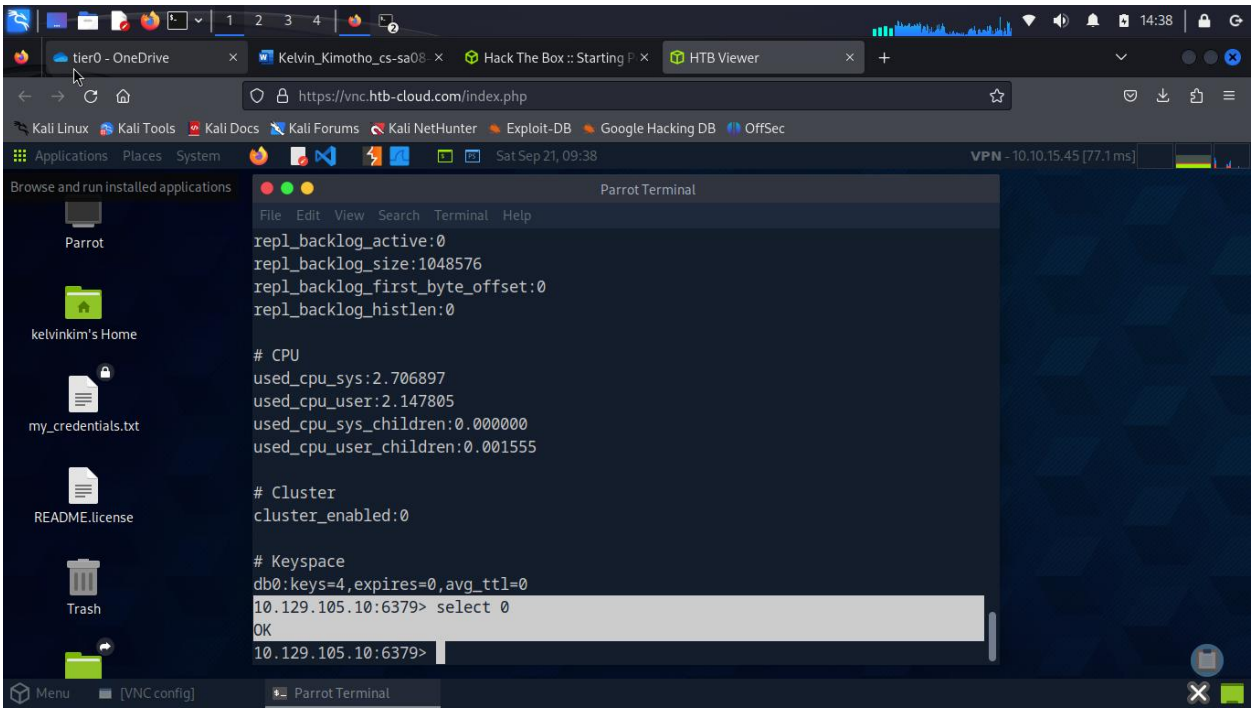


Task 8

Question: Which command is used to select the desired database in Redis?

Answer: select





Task 9

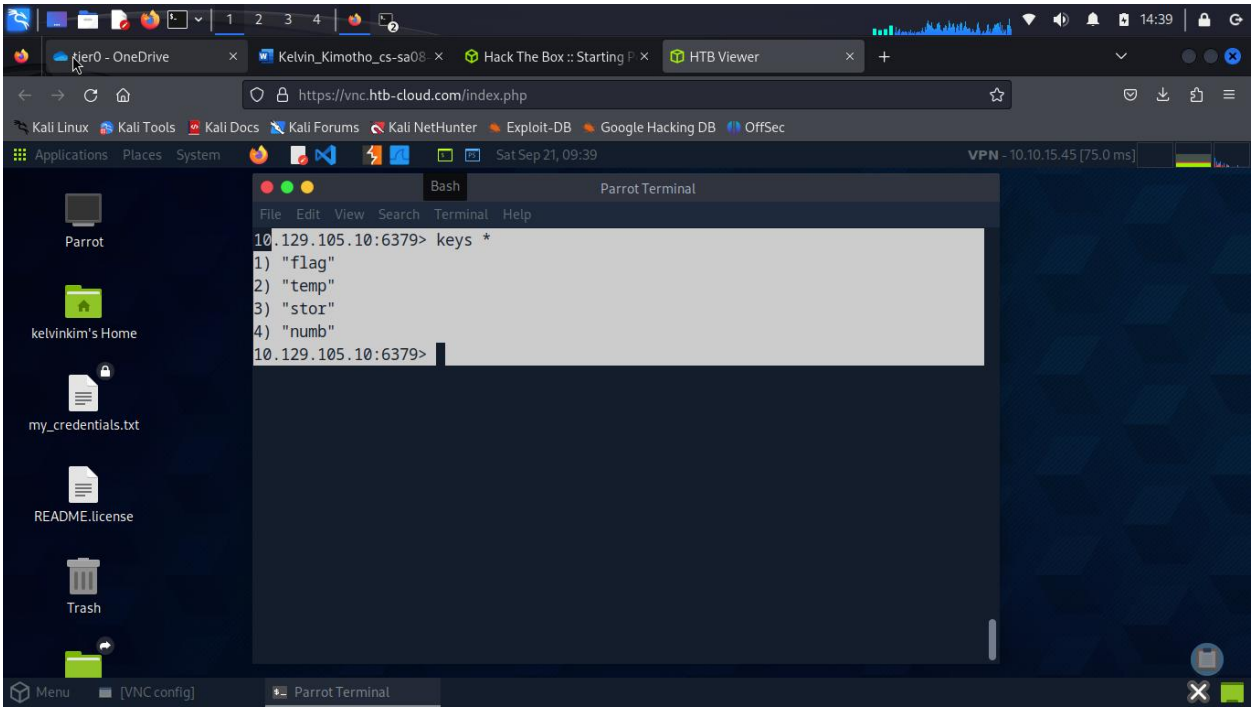
Question: How many keys are present inside the database with index 0?

ANswer: 4

Task 10

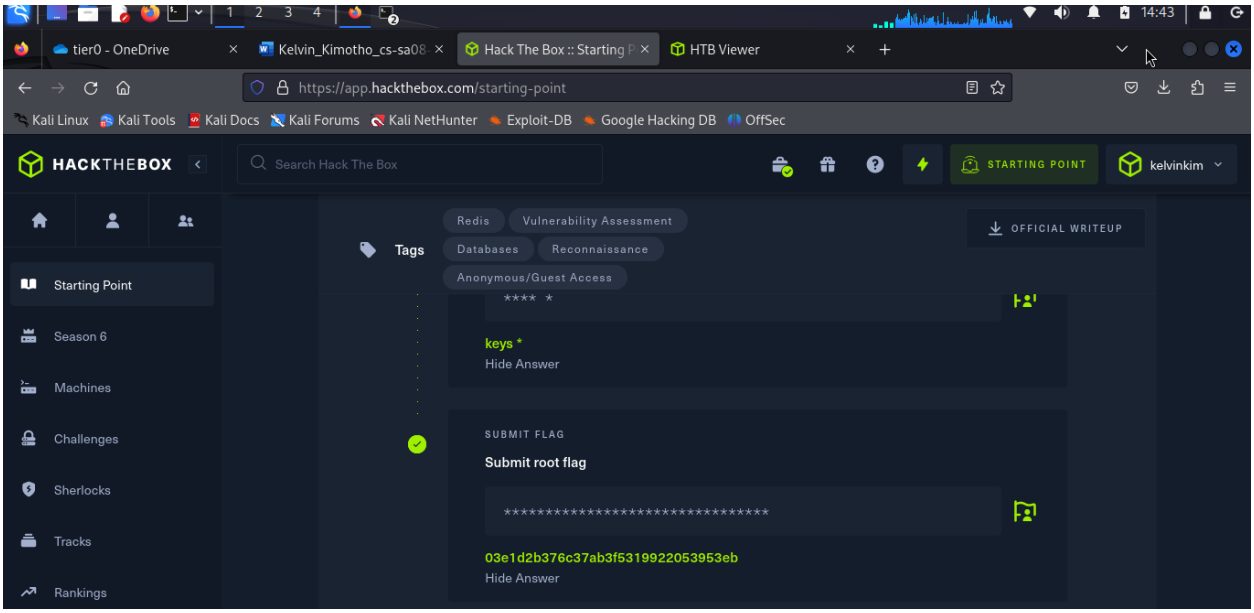
Question: Which command is used to obtain all the keys in a database?

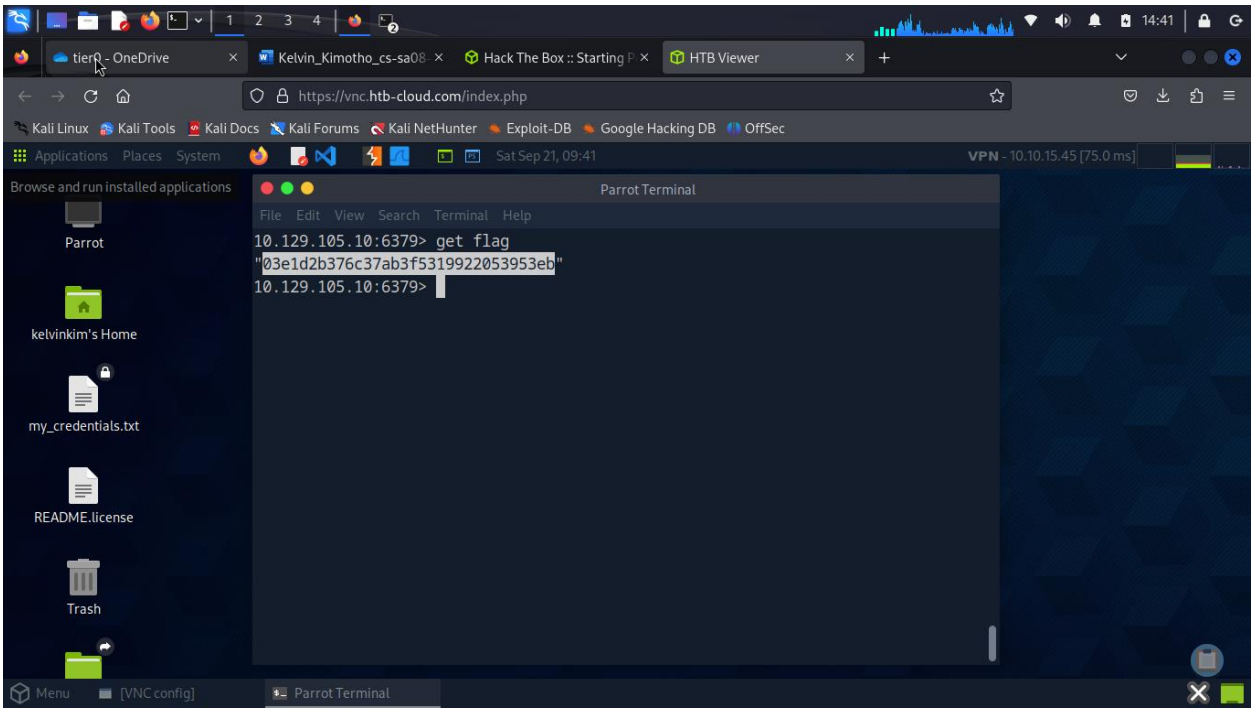
Answer: keys *



Submit root flag

Answer: 03e1d2b376c37ab3f5319922053953eb


14:43
tier0 - OneDrive
Kelvin_Kimotho_cs-sa08
Hack The Box :: Starting P
HTB Viewer
https://app.hackthebox.com/starting-point
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HACKTHEBOX
Search Hack The Box
STARTING POINT
kelvinkim
Starting Point
Season 6
Machines
Challenges
Sherlocks
Tracks
Rankings
Tags
Redis
Vulnerability Assessment
Databases
Reconnaissance
Anonymous/Guest Access
OFFICIAL WRITEUP
**** *
keys *
Hide Answer
SUBMIT FLAG
Submit root flag
****
03e1d2b376c37ab3f5319922053953eb
Hide Answer


14:41
tier0 - OneDrive
Kelvin_Kimotho_cs-sa08
Hack The Box :: Starting P
HTB Viewer
https://vnc.htb-cloud.com/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Applications
Places
System
Sat Sep 21, 09:41
VPN - 10.10.15.45 [75.0 ms]
Browse and run installed applications
Parrot
kelvinkim's Home
my_credentials.txt
README.license
Trash
Parrot Terminal
File Edit View Search Terminal Help
10.129.105.10:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
10.129.105.10:6379>
Menu
[VNC config]
Parrot Terminal

Conclusion

After completing this tier, I have gained the practical knowledge on how to connect to a vpn from may machines terminal. I gained insight on various tools and techniques used in the entire penetration testing. How to use Nmap to perform port scans on our target machines, how to gather information about the services running on the machine and how to exploit vulnerabilities associated with the services we find running. I also learnt about databases, In-memory databases for this case and how to exploit or access them. Also gained insight on the server message block protocol for windows systems and how i can access shares from my kali machine using smbclient tool even without the access rights. By exploiting vulnerabilities mostly on human created shares.