

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.

+

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#)

+

Virtual Machine (VM)



Abbreviations / Acronyms / Synonyms:

[VM](#) show sources

+

Definitions:

A simulated environment created by virtualization.

Sources:

[NIST SP 800-125](#) under Virtual machine (VM)

[NIST SP 800-190](#) under Virtual machine from [NIST SP 800-125](#)

Software that allows a single host to run one or more guest operating systems.

Sources:

[NIST SP 1800-10B](#) under Virtual Machine from [NIST SP 800-115](#)

[NIST SP 1800-25B](#) under Virtual Machine from [NIST SP 800-115](#)

[NIST SP 1800-26B](#) under Virtual Machine from [NIST SP 800-115](#)

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.



```

File Actions Edit View Help
[kali㉿kali] ~
$ cd Downloads
[kali㉿kali] ~/Downloads
$ sudo openvpn starting_point_Damiano254(1).ovpn
[sudo] password for kali:
2024-01-24 21:22:18 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-01-24 21:22:18 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-01-24 21:22:18 OpenSSL 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL) [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-01-24 21:22:18 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-01-24 21:22:18 DCO version: N/A
2024-01-24 21:22:18 TCP/UDP: Preserving recently used remote address: [AF_INET]23.19.62.150:1337
2024-01-24 21:22:18 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-01-24 21:22:18 UDPv4 link local: (not bound)
2024-01-24 21:22:18 UDPv4 link remote: [AF_INET]23.19.62.150:1337
2024-01-24 21:22:18 TLS: Initial packet from [AF_INET]23.19.62.150:1337, sid=f3f478f5beb7a5
2024-01-24 21:22:21 VERIFY OK: depth=1, CN=HackTheBox
2024-01-24 21:22:21 VERIFY KU OK
2024-01-24 21:22:21 Validating certificate extended key usage
2024-01-24 21:22:21 + Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-01-24 21:22:21 VERIFY EKU OK
2024-01-24 21:22:21 VERIFY OK: depth=0, CN=htb
2024-01-24 21:22:21 Control Channel: TLSv1.3, cipher TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA256
2024-01-24 21:22:21 [htb] Peer Connection Initiated with [AF_INET]23.19.62.150:1337
2024-01-24 21:22:21 TLS: move_session: dest=<TM_ACTIVE> src=<TM_INITIAL> reinit_src=1
2024-01-24 21:22:21 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-01-24 21:22:22 SENT CONTROL [htb]: "PUSH_REQUEST" (status=1)
2024-01-24 21:22:22 PUSH: Received control message: "PUSH_REPLY", route 10.10.0.0 255.255.254.0, route 10.129.0.0 255.255.0.0, route-ipv6 dead:beef::/64, explicit-exit-no
2024-01-24 21:22:22 tun-ipv6, route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1038/64 dead:beef:2::1,ifconfig 10.10.14.58 255.255.254.0,peer-id 94,cipher AES-256-CBC"
2024-01-24 21:22:22 OPTIONS IMPORT: --ifconfig/up options modified
2024-01-24 21:22:22 OPTIONS IMPORT: route options modified
2024-01-24 21:22:22 OPTIONS IMPORT: route-related options modified
2024-01-24 21:22:22 net_route_v4_best_gw query: dst 0.0.0.0
2024-01-24 21:22:22 net_route_v4_best_gw result: via 192.168.142.225 dev eth0
2024-01-24 21:22:22 ROUTE_GATEWAY 192.168.142.225/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:df:55:da

```

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.




```

File Machine View Input Devices Help
File Actions Edit View Help
[kali㉿kali] ~
$ cd Downloads
[kali㉿kali] ~/Downloads
$ sudo openvpn starting_point_Damiano254(1).ovpn
[sudo] password for kali:
2024-01-24 21:22:18 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-01-24 21:22:18 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-01-24 21:22:18 OpenSSL 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL) [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-01-24 21:22:18 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-01-24 21:22:18 DCO version: N/A
2024-01-24 21:22:18 TCP/UDP: Preserving recently used remote address: [AF_INET]23.19.62.150:1337
2024-01-24 21:22:18 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-01-24 21:22:18 UDPv4 link local: (not bound)
2024-01-24 21:22:18 UDPv4 link remote: [AF_INET]23.19.62.150:1337
2024-01-24 21:22:18 TLS: Initial packet from [AF_INET]23.19.62.150:1337, sid=f3f478f5beb7a5
2024-01-24 21:22:21 VERIFY OK: depth=1, CN=HackTheBox
2024-01-24 21:22:21 VERIFY KU OK
2024-01-24 21:22:21 Validating certificate extended key usage
2024-01-24 21:22:21 + Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-01-24 21:22:21 VERIFY EKU OK
2024-01-24 21:22:21 VERIFY OK: depth=0, CN=htb
2024-01-24 21:22:21 Control Channel: TLSv1.3, cipher TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA256
2024-01-24 21:22:21 [htb] Peer Connection Initiated with [AF_INET]23.19.62.150:1337
2024-01-24 21:22:21 TLS: move_session: dest=<TM_ACTIVE> src=<TM_INITIAL> reinit_src=1
2024-01-24 21:22:21 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-01-24 21:22:22 SENT CONTROL [htb]: "PUSH_REQUEST" (status=1)
2024-01-24 21:22:22 PUSH: Received control message: "PUSH_REPLY", route 10.10.0.0 255.255.254.0, route 10.129.0.0 255.255.0.0, route-ipv6 dead:beef::/64, explicit-exit-no
2024-01-24 21:22:22 tun-ipv6, route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1038/64 dead:beef:2::1,ifconfig 10.10.14.58 255.255.254.0,peer-id 94,cipher AES-256-CBC"
2024-01-24 21:22:22 OPTIONS IMPORT: --ifconfig/up options modified
2024-01-24 21:22:22 OPTIONS IMPORT: route options modified
2024-01-24 21:22:22 OPTIONS IMPORT: route-related options modified
2024-01-24 21:22:22 net_route_v4_best_gw query: dst 0.0.0.0
2024-01-24 21:22:22 net_route_v4_best_gw result: via 192.168.142.225 dev eth0
2024-01-24 21:22:22 ROUTE_GATEWAY 192.168.142.225/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:df:55:da

```

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.

File Actions Edit View Help

kali@kali: ~/Downloads x kali@kali: ~ x

```
64 bytes from 10.129.130.40: icmp_seq=3 ttl=63 time=228 ms
64 bytes from 10.129.130.40: icmp_seq=4 ttl=63 time=233 ms
64 bytes from 10.129.130.40: icmp_seq=5 ttl=63 time=348 ms
64 bytes from 10.129.130.40: icmp_seq=6 ttl=63 time=305 ms
64 bytes from 10.129.130.40: icmp_seq=7 ttl=63 time=263 ms
64 bytes from 10.129.130.40: icmp_seq=8 ttl=63 time=237 ms
64 bytes from 10.129.130.40: icmp_seq=9 ttl=63 time=340 ms
64 bytes from 10.129.130.40: icmp_seq=10 ttl=63 time=218 ms
64 bytes from 10.129.130.40: icmp_seq=11 ttl=63 time=217 ms
64 bytes from 10.129.130.40: icmp_seq=12 ttl=63 time=2492 ms
64 bytes from 10.129.130.40: icmp_seq=13 ttl=63 time=1468 ms
64 bytes from 10.129.130.40: icmp_seq=14 ttl=63 time=440 ms
64 bytes from 10.129.130.40: icmp_seq=15 ttl=63 time=358 ms
64 bytes from 10.129.130.40: icmp_seq=16 ttl=63 time=235 ms
64 bytes from 10.129.130.40: icmp_seq=17 ttl=63 time=233 ms
^X64 bytes from 10.129.130.40: icmp_seq=18 ttl=63 time=231 ms
64 bytes from 10.129.130.40: icmp_seq=19 ttl=63 time=349 ms
^Z
zsh: suspended ping 10.129.130.40
```



```
(kali㉿kali)-[~]
$ ping 10.129.130.40
PING 10.129.130.40 (10.129.130.40) 56(84) bytes of data.
64 bytes from 10.129.130.40: icmp_seq=1 ttl=63 time=1603 ms
64 bytes from 10.129.130.40: icmp_seq=2 ttl=63 time=587 ms
64 bytes from 10.129.130.40: icmp_seq=3 ttl=63 time=227 ms
64 bytes from 10.129.130.40: icmp_seq=4 ttl=63 time=342 ms
^X64 bytes from 10.129.130.40: icmp_seq=5 ttl=63 time=742 ms
^C
--- 10.129.130.40 ping statistics ---
7 packets transmitted, 5 received, 28.5714% packet loss, time 6044ms
rtt min/avg/max/mdev = 227.277/700.283/1603.019/486.090 ms, pipe 2
```

```
(kali㉿kali)-[~]
$ HTB for Business
```

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.

kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Hack The Box :: Starting P × Top 5 Free Open Port Ch × +

https://www.upguard.com/blog/best-open-port-scanners

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

UpGuard

Products Solutions Pricing Resources Customers Login Contact sales Free trial →

1. Nmap

Contents

- What is Open Port Scanning?
- Should Ports Be Open or Closed?
- List of Common Network Port Numbers
- How Does Open Port Scanning Work?
- How Do Cybercriminals Use Port Scanning to Prepare Cyberattacks?



Nmap (short for Network Mapper) is one of the most popular free open-source port scanning tools available. It offers many different port scanning techniques including TCP half-open scans.

Key features:

- Multiple port scanning techniques

Author



Edward Kost

Operator from UpGuard • Just now
Hey there! 😊 Can I ask you a quick question?

K Sure! 😊 I'd like to speak to sales..
Join 27,000+ cyt I'm a current customer newsletter subsc

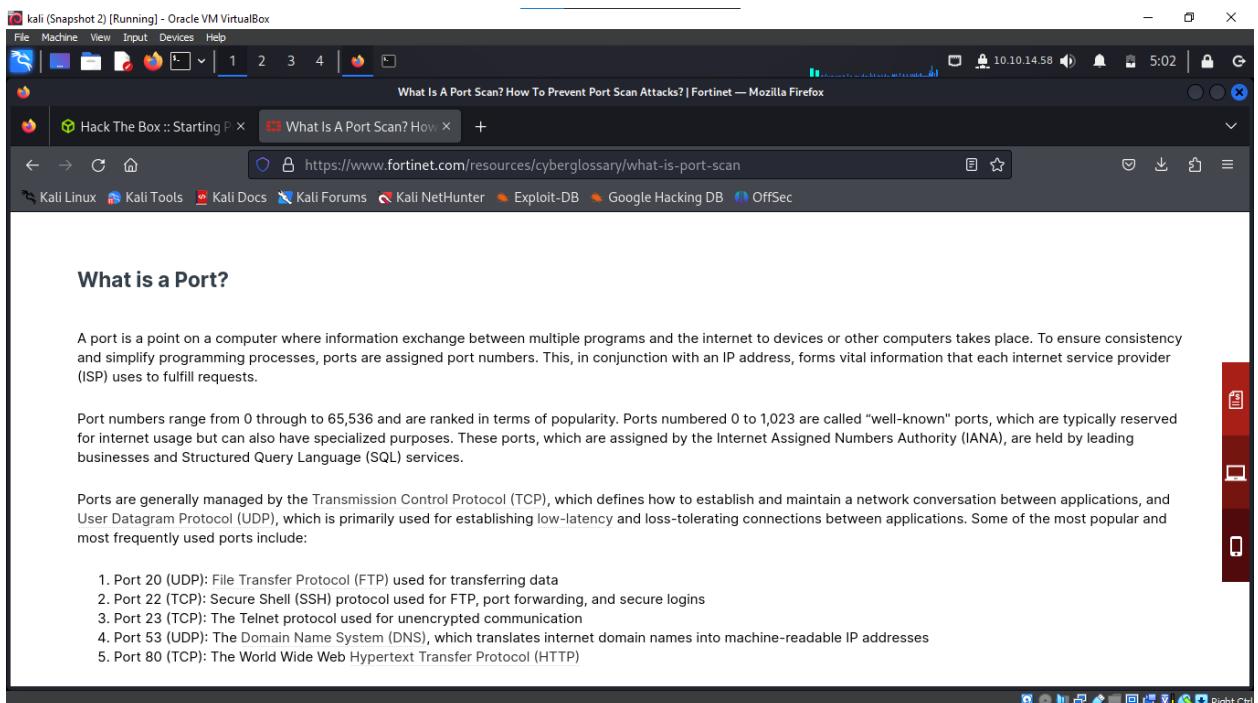
Email address*

1

```
[kali㉿kali)-[~] nmap 10.129.130.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 04:59 EAT
Nmap scan report for 10.129.130.40
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet
Nmap done: 1 IP address (1 host up) scanned in 93.52 seconds
```

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.



```
(kali㉿kali)-[~]
$ nmap 10.129.130.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 04:59 EAT
Nmap scan report for 10.129.130.40
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet
Nmap done: 1 IP address (1 host up) scanned in 93.52 seconds
```

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

File Machine View Input Devices Help

1 2 3 4

What Is "root" on Linux? — Mozilla Firefox

Hack The Box :: Starting Point | 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 superhero. 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

File Machine View Input Devices Help

1 2 3 4

What Is "root" on Linux? — Mozilla Firefox

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: Meow

Starting Point

Machines

Challenges

Sherlocks

Academy

HTB for Business

Telnet Frameworks Reconnaissance Weak Credentials

Tags Misconfiguration

ONLINE

TARGET MACHINE IP ADDRESS
10.129.130.40

Read the walkthrough provided, to get a detailed guide on how to pen this machine.

TASK 1
What does the acronym VM stand for?

Show Answer

Right Ctrl

kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 | 🔍

root@Meow: ~ - Mozilla Firefox

File Actions Edit View Help

kali@kali: ~/Downloads x root@Meow: ~ x

https://www.hackthebox.com/machines/point

Meow login: root

Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

* Documentation: <https://help.ubuntu.com>

* Management: <https://landscape.canonical.com>

* Support: <https://ubuntu.com/advantage>

System information as of Thu 25 Jan 2024 02:18:23 AM UTC

System load: 0.0

Usage of '/': 41.7% of 7.75GB

Memory usage: 4%

Swap usage: 0%

Processes: 136

Users logged in: 0

IPv4 address for eth0: 10.129.130.40

IPv6 address for eth0: dead:beef::250:56ff:fe96:4653

Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around. Read the walkthrough provided, to get a detailed guide on how to own this machine.

<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

TASKS

What does the acronym VM stand for?

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:~#

Task 8: Submit Flag

- **Flag:** b40abdfc23665f766f9c61ecba8a4c19
 - **Details:** Successfully retrieved the root flag, indicating full control over the target system.

kali (Snapshot2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

S D F M 1 2 3 4 |

root@Meow: ~

File Actions Edit View Help

kali:kali: ~/Downloads x root@Meow: ~ x

* Documentation: <https://help.ubuntu.com> <https://www.hackthebox.com/start-point>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

Kali NetHunter Exploit-DB Google Hacking DB OffSec

System information as of Thu 25 Jan 2024 02:18:23 AM UTC

System load: 0.0
Usage of /: 41.7% of 7.75GB
Memory usage: 4%
Swap usage: 0%
Processes: 136
Users logged in: 0
IPv4 address for eth0: 10.129.130.40
IPv6 address for eth0: dead:beef::250:56ff:fe96:4653

* Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around.

<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

b40abdfc23665f766f9c61ecba8a4c19

root@Meow:~# ^C

root@Meow:~#

Meow has been Pwned!

10.10.14.58 5:19

Damian... STARTING POINT

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.

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a Mozilla Firefox window displays the URL <https://www.fortinet.com/resources/cyberglossary/file-transfer-protocol-ftp-meaning>. The page content is about the definition of FTP (File Transfer Protocol). A red box highlights the section title "What is FTP (File Transfer Protocol)?". Another red box highlights the first paragraph of the text, which defines FTP as a standard network protocol for file transfer over TCP-based networks. The Kali Linux desktop interface includes a taskbar with icons for various tools like Kali Tools, Kali Docs, and OffSec, and a terminal window at the bottom.

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.

The screenshot shows a web browser displaying an article from TechTarget. The URL is <https://www.techtarget.com/searchnetworking/tip/Understanding-the-FTP-PORT-command>. The page title is "Understanding the FTP PORT command". The main content discusses the difference between the control channel (port 21) and the data channel (port 20). It also mentions the Service Name and Transport Protocol Port Number Registry and the Internet Assigned Numbers Authority website. Social sharing icons for Facebook, Twitter, LinkedIn, and Print are visible on the left. A sidebar on the right contains the text "pr 20 re" and a red button.

control channel, and port 20 is for the data channel. Learn how these two channels are used.

By [Terry Slattery](#), NetCraftsmen | [Laura Chappell](#), Chappell University Published: 16 Aug 2022

You may already know that, when FTP commands cross the wire, they use TCP port 21 by default. You may also know that port 20 is assigned to the FTP data channel by default. For further reference, see the *ftp-data* entry in the Service Name and Transport Protocol Port Number Registry on the Internet Assigned Numbers Authority, or IANA, [website](#).

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.

The screenshot shows a Mozilla Firefox browser window with multiple tabs open. The active tab is titled "SFTP vs. FTPS: What's the Best Protocol for Secure FTP? | GoAnywhere MFT — Mozilla Firefox" and displays an article from GoAnywhere MFT. The article compares SFTP and FTPS, noting that SFTP is the secure version of FTP. It highlights that SFTP uses SSH for secure file transfer. The browser interface includes a toolbar at the top, a navigation bar, and a sidebar on the right with links to "Securing FTP and SFTP Servers" and "Data Breach and Incident Response Plans | 2017 Templates & Resources". A tooltip in the bottom right corner asks if the user wants to stay on top of cybersecurity news.

SFTP vs. FTPS: What's the Best Protocol for Secure FTP? | GoAnywhere MFT — Mozilla Firefox

Hack The Box :: Starting | SFTP vs. FTPS: What's the Be | +

https://www.goanywhere.com/blog/sftp-vs-ftps-what-is-the-best-secure-ftp-protocol

FORTRA

GoAnywhere® Managed File Transfer

What is Secure FTP?

There are two mainstream protocols available for secure FTP:

1. SFTP (FTP over SSH)
2. FTPS (FTP over SSL)

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.

kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 |

Back The Box kali@kali: ~

File Actions Edit View Help

(kali㉿kali)-[~]

```
$ nmap 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 05:45 EAT
Nmap scan report for 10.129.1.14
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 89.13 seconds
```

(kali㉿kali)-[~]

```
$ ping 10.129.1.14
PING 10.129.1.14 (10.129.1.14) 56(84) bytes of data.
64 bytes from 10.129.1.14: icmp_seq=1 ttl=63 time=442 ms
64 bytes from 10.129.1.14: icmp_seq=2 ttl=63 time=329 ms
64 bytes from 10.129.1.14: icmp_seq=3 ttl=63 time=217 ms
64 bytes from 10.129.1.14: icmp_seq=4 ttl=63 time=244 ms
64 bytes from 10.129.1.14: icmp_seq=5 ttl=63 time=242 ms
64 bytes from 10.129.1.14: icmp_seq=6 ttl=63 time=230 ms
64 bytes from 10.129.1.14: icmp_seq=7 ttl=63 time=210 ms
64 bytes from 10.129.1.14: icmp_seq=8 ttl=63 time=237 ms
^C
--- 10.129.1.14 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7008ms
rtt min/avg/max/mdev = 210.291/268.951/442.473/73.894 ms
```

(kali㉿kali)-[~]

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.

```
[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 wfreemoterm
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

Service detection performed. Please report any incorrect results at https://nmap.org/report/
```

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.

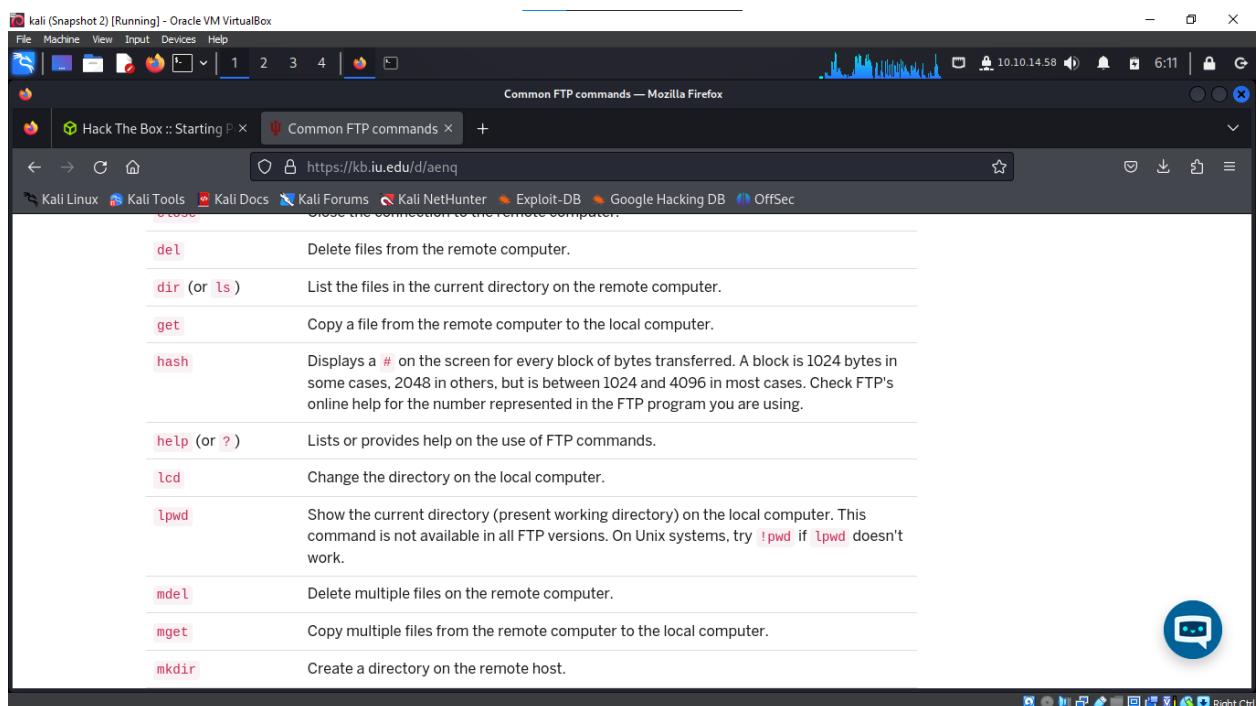
```
(kali㉿kali)-[~]
$ nmap -sV 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 05:51 EAT
Nmap scan report for 10.129.1.14
Host is up (0.44s latency).

Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp          vsftpd 3.0.3
1046/tcp  filtered wfreemoterm
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.

The screenshot shows a Firefox browser window with the URL <https://www.ibm.com/docs/en/i/7.4?topic=i-configuring-anonymous-ftp>. The page title is "Configuring anonymous File Transfer Protocol". A yellow banner at the top states, "A newer version of this product documentation is available. You are viewing an older version." Below this, the main content discusses Anonymous File Transfer Protocol (FTP) and its use for remote access without a password. It notes that Anonymous FTP enables unprotected access (no password required) to selected information about a remote system. The remote site determines what information is made available for general access. Such information is considered to be publicly accessible and can be read by anyone. It is the responsibility of the person who owns the information and the system to assure that only appropriate information is made available. The page also mentions that to access this information, a user logs on to the hosts using the user ID ANONYMOUS. The user ANONYMOUS has limited access rights to the files on the FTP server and has some operating restrictions. Typically, the following operations are only operations allowed.

Task 9: FTP Login Response Code

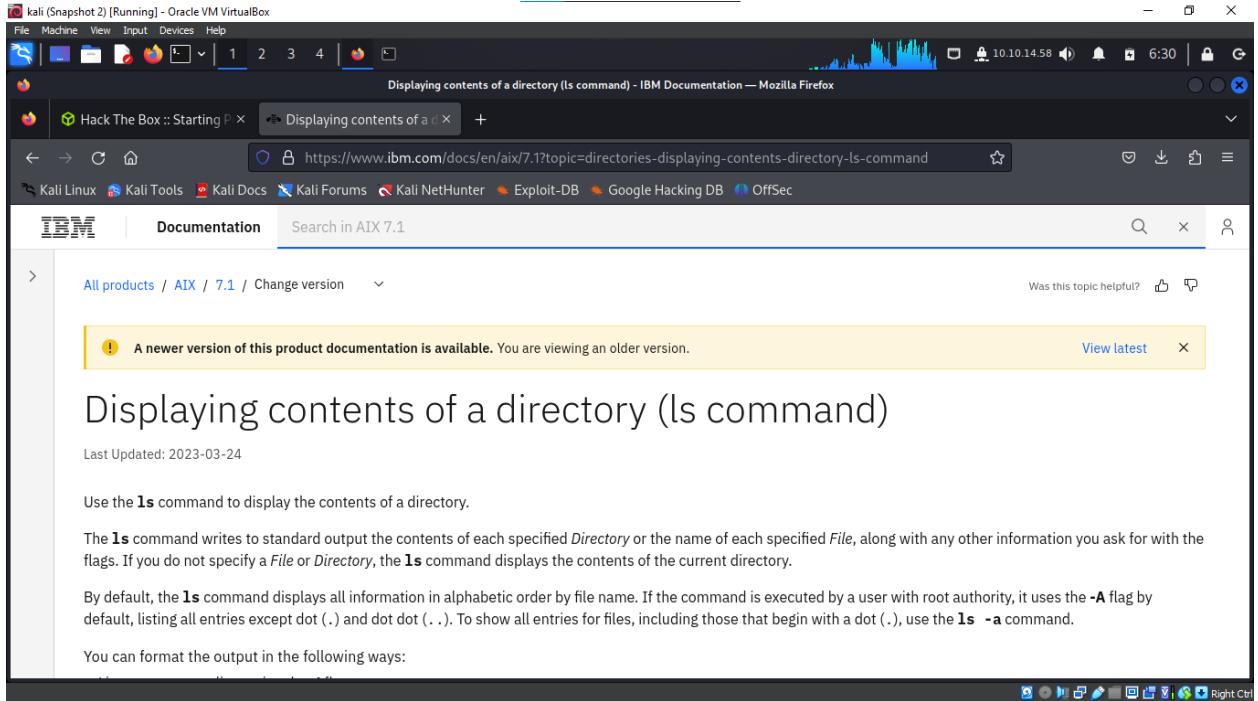
- **Question:** What is the response code for 'Login successful' in FTP?
- **Answer:** 230
- **Details:** The response code 230 indicates a successful login to the FTP server.

The screenshot shows a Firefox browser window with the URL <https://learn.microsoft.com/en-us/troubleshoot/developer/webapps/iis/ftp-service-svchost-inetinfo/ftp>. The page title is "The FTP status codes in IIS 7.0 and later versions - Internet Information Services | Microsoft Learn". The main content area displays a list of FTP status codes, starting with 200 and continuing through 234. To the right, there is a sidebar titled "Additional resources" with links to "Documentation", "FTP Log Files &LogFile>", "Changes in FTP 7.5 - Internet Information Services", "FTP Connections &connections>", and "Show 5 more".

Status Code	Description
200	Command okay.
202	Command not implemented, superfluous at this site.
211	System status, or system help reply.
212	Directory status.
213	File status.
214	Help message.
215	NAME system type, where NAME is an official system name from the list in the Assigned Numbers document.
220	Service ready for new user.
221	Service closing control connection. Logged out if appropriate.
225	Data connection open; no transfer in progress.
226	Closing data connection. Requested file action successful (for example, file transfer or file abort).
227	Entering Passive Mode (h1,h2,h3,h4,p1,p2).
229	Extended passive mode entered.
230	User logged in, proceed.
232	User logged in, authorized by security data exchange.
234	Security data exchange complete.

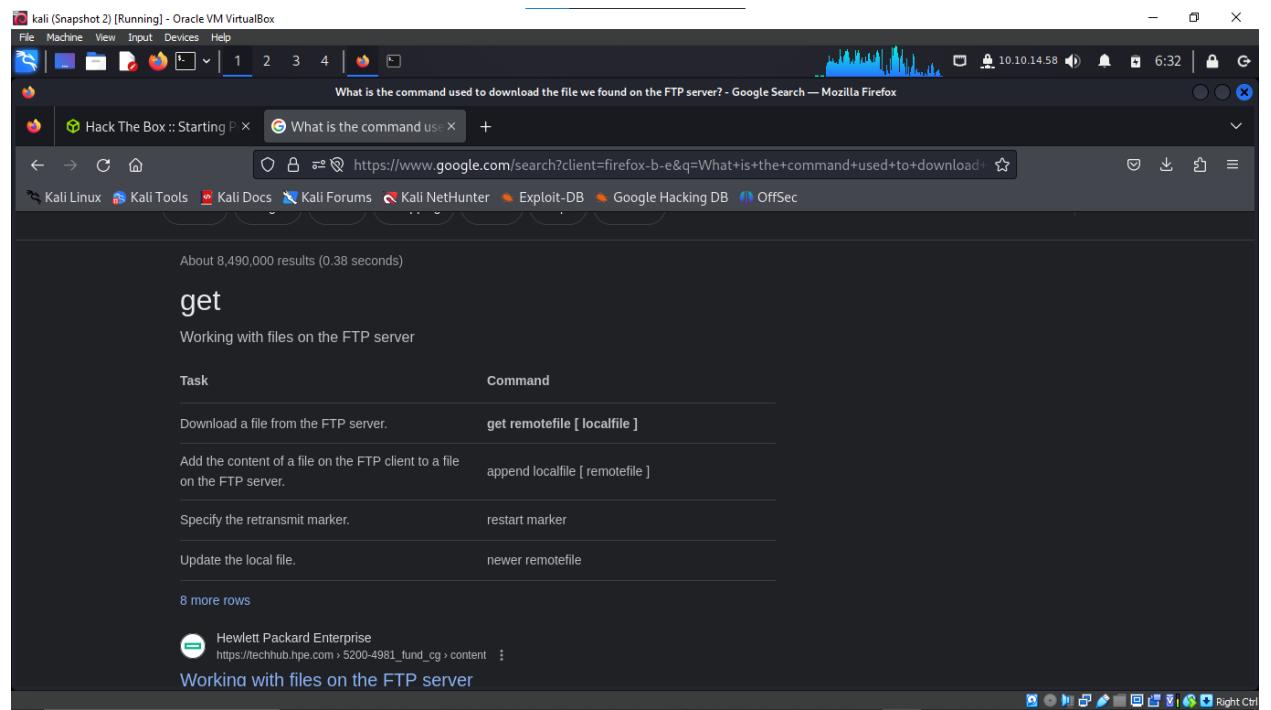
Task 10: Listing Files and Directories

- **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.



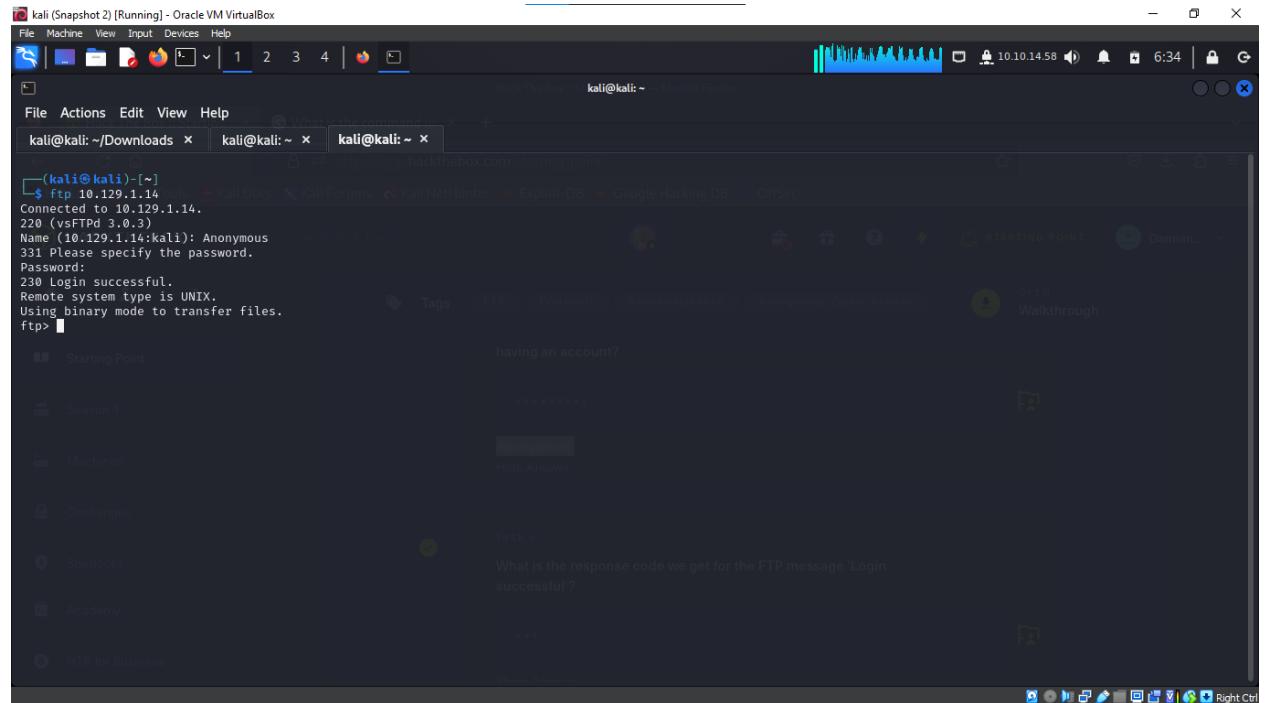
Task 11: Downloading Files via FTP

- **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.



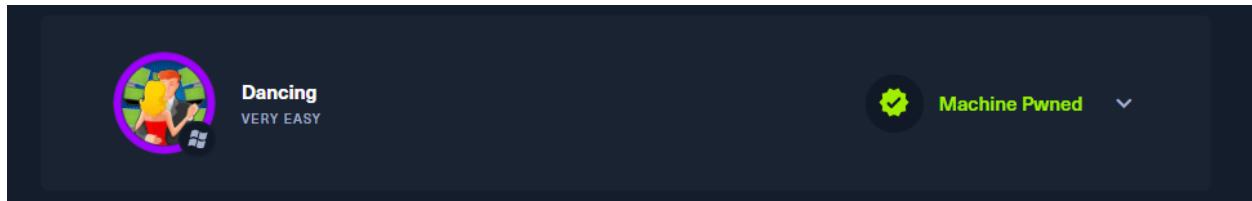
```
(kali㉿kali)-[~]
└─$ ftp 10.129.1.14
Connected to 10.129.1.14.
220 (vsFTPd 3.0.3)
Name (10.129.1.14:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /
ftp> ls
229 Entering Extended Passive Mode (|||62181|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> sudo su
?Invalid command.
ftp> cd /root
550 Failed to change directory.
ftp> cat flag.txt
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||35789|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% [*****] 32 15.16 KiB/s 00:00 ET
226 Transfer complete.
32 bytes received in 00:00 (0.09 KiB/s)
ftp> 
```

```
(kali㉿kali)-[~]
└─$ ls
Desktop  Downloads  hey.txt  nibbles_initial_scan.gnmap  nibbles_initial_scan.xml  Pictures  shell.php  text.txt  ty.txt
Documents  flag.txt  Music    nibbles_initial_scan.nmap  nishang                Public   Templates  text.txt-h  Videos
(kali㉿kali)-[~]
└─$ cat flag.txt
035db21c881520061c53e0536e44f815
(kali㉿kali)-[~]
```

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.

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** https://www.ibm.com/docs/en/aix/7.1?topic=management-smb-protocol
- Title Bar:** SMB protocol - IBM Documentation — Mozilla Firefox
- Content Area:** The page is titled "SMB protocol". It includes a sidebar with navigation links like "All products / AIX / 7.1 / Change version". The main content area describes the SMB protocol as a client-server communication protocol for shared access to files, directories, printers, serial ports, and other resources. It also mentions the Server Message Block file system and client file system.
- Bottom Bar:** Shows the Kali Linux desktop environment with various icons for tools like Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

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  isoipspgport-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

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]: Show Answer

      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 5

How many shares are there on Dancing?

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]: https://app.hackthebox.com/startng-point
KaliNetHunter Exploit-DB Google Hacking DB OffSec

      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
```

we are able to access
blank password?

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

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.

```
smbget is a simple utility with wget-like semantics, that can download files from SMB servers. You can specify the files you would like to download on the command-line. The files should be in the smb-URL standard, e.g. use smb://host/share/file for the UNC path \\HOST\\SHARE\\file.

S Samba
https://www.samba.org › docs › man-html › smbget.1.html ::

smbget - Samba.org
```

Submit Root Flag

Flag: 5f61c10dffbc77a704d76016a22f1664

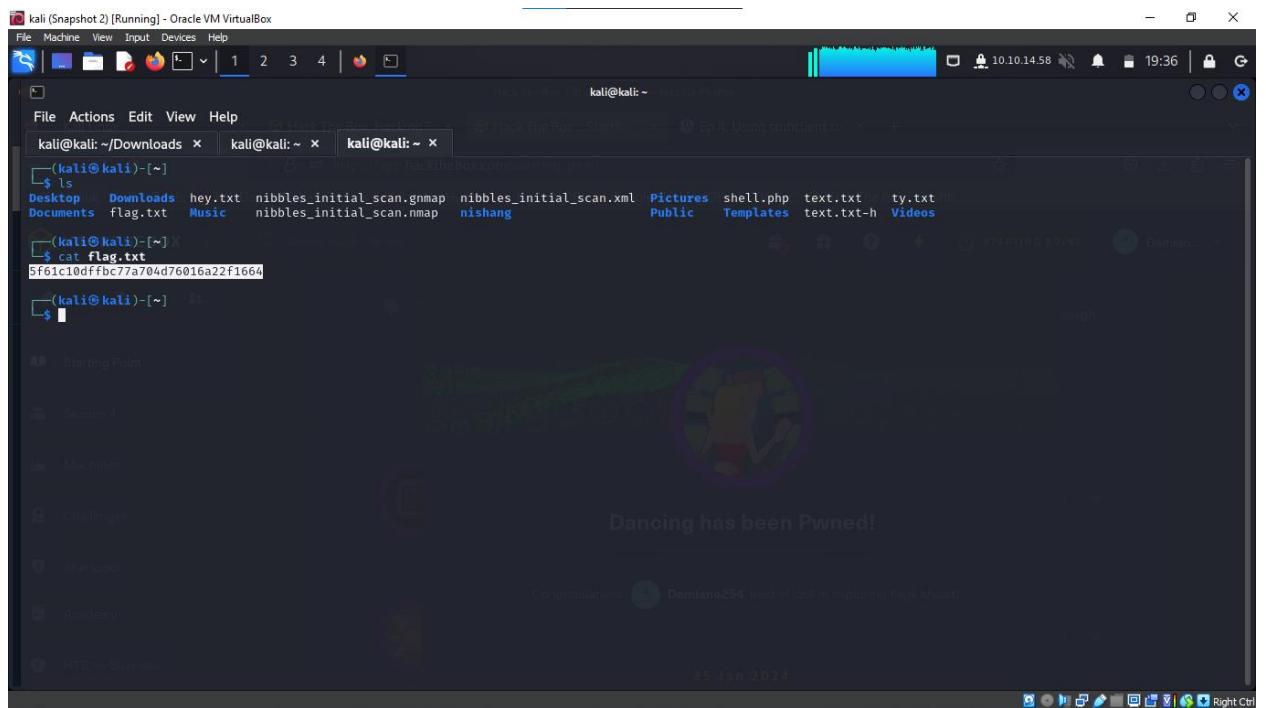
Details: Successfully retrieved the root flag from the target system.

```
Starting Point
└─(kali㉿kali)-[~]
$ smbclient //10.129.86.28/WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.
D      0 Mon Mar 29 11:22:01 2021
.. Machines
D      0 Mon Mar 29 11:22:01 2021
Amy.J
James.P
D      0 Mon Mar 29 12:08:24 2021
D      0 Thu Jun  3 11:38:03 2021

Challenge 5114111 blocks of size 4096. 1748753 blocks available
smb: \> cd James.P
smb: \James.P\> ls
.
Sherlock
..
flag.txt
D      0 Thu Jun  3 11:38:03 2021
D      0 Thu Jun  3 11:38:03 2021
A     32 Mon Mar 29 12:26:57 2021

Academy 5114111 blocks of size 4096. 1748753 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 Kilobytes/sec) (average 0.0 Kilobytes/sec)
smb: \James.P\> █

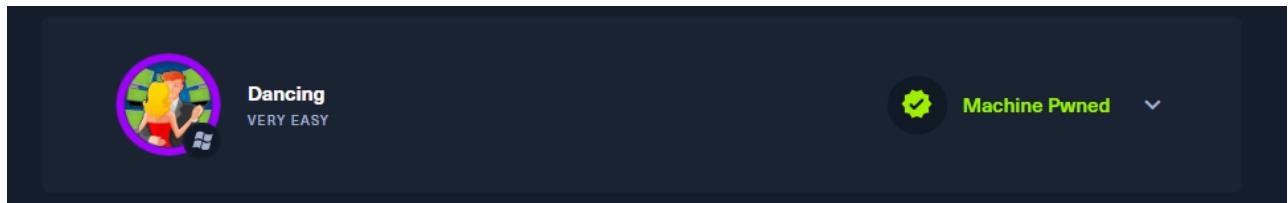
Dancing has been
Damiano254, best of
25 Jan 2024
```



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.

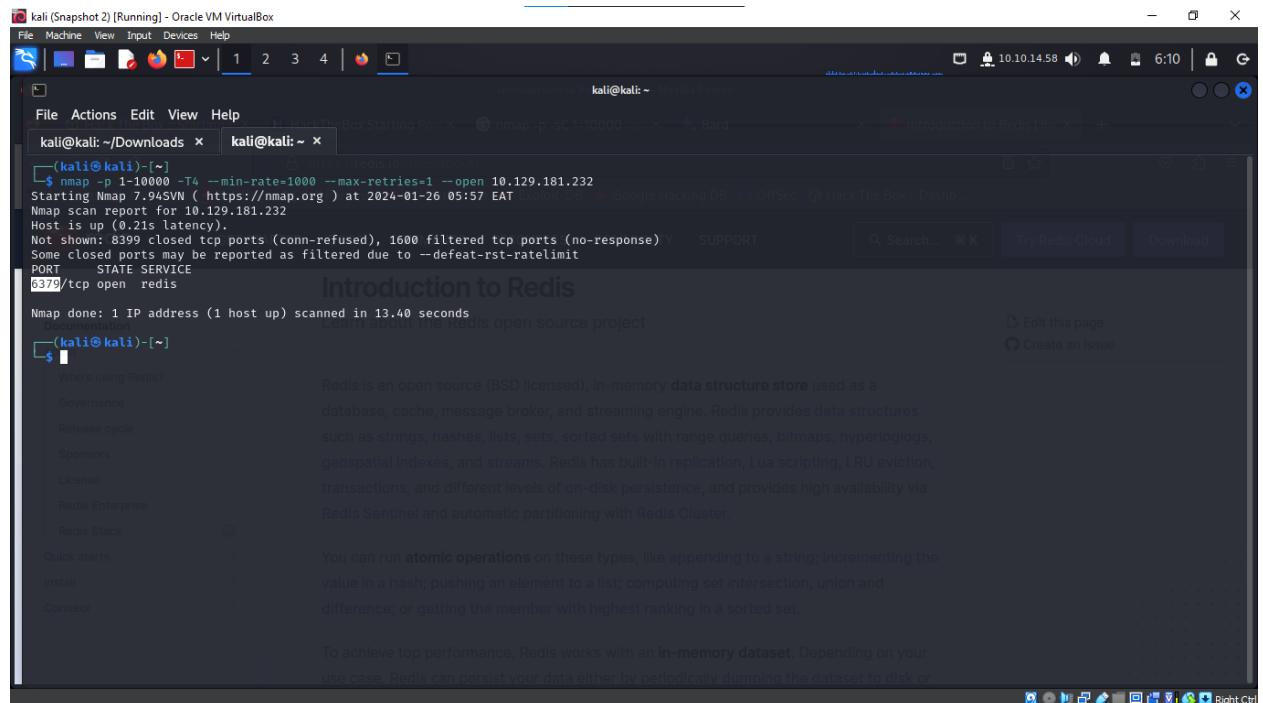
```
(kali㉿kali)-[~] $ nmap -p 1-10000 -T4 --min-rate=1000 --max-retries=1 --open 10.129.181.232
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 05:57 EAT (exploit-DB: Google Hacking DB, OffSec)
Nmap scan report for 10.129.181.232
Host is up (0.21s latency).
Not shown: 8399 closed tcp ports (conn-refused), 1600 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
6379/tcp  open  redis

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

The terminal window is part of a larger interface. Below it, there's a sidebar with links like "Who's using Redis?", "Governance", "Release cycle", "Sponsors", "License", "Redis Enterprise", "Redis Stack", "Quick starts", "Install", and "Connect". To the right of the terminal, there's a summary of Redis: "Redis is an open source (BSD licensed), in-memory data structure store used as a database, cache, message broker, and streaming engine. Redis provides data structures such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperloglogs, geospatial indexes, and streams. Redis has built-in replication, Lua scripting, LRU eviction, transactions, and different levels of on-disk persistence, and provides high availability via Redis Sentinel and automatic partitioning with Redis Cluster." There are also sections for atomic operations and performance optimization.

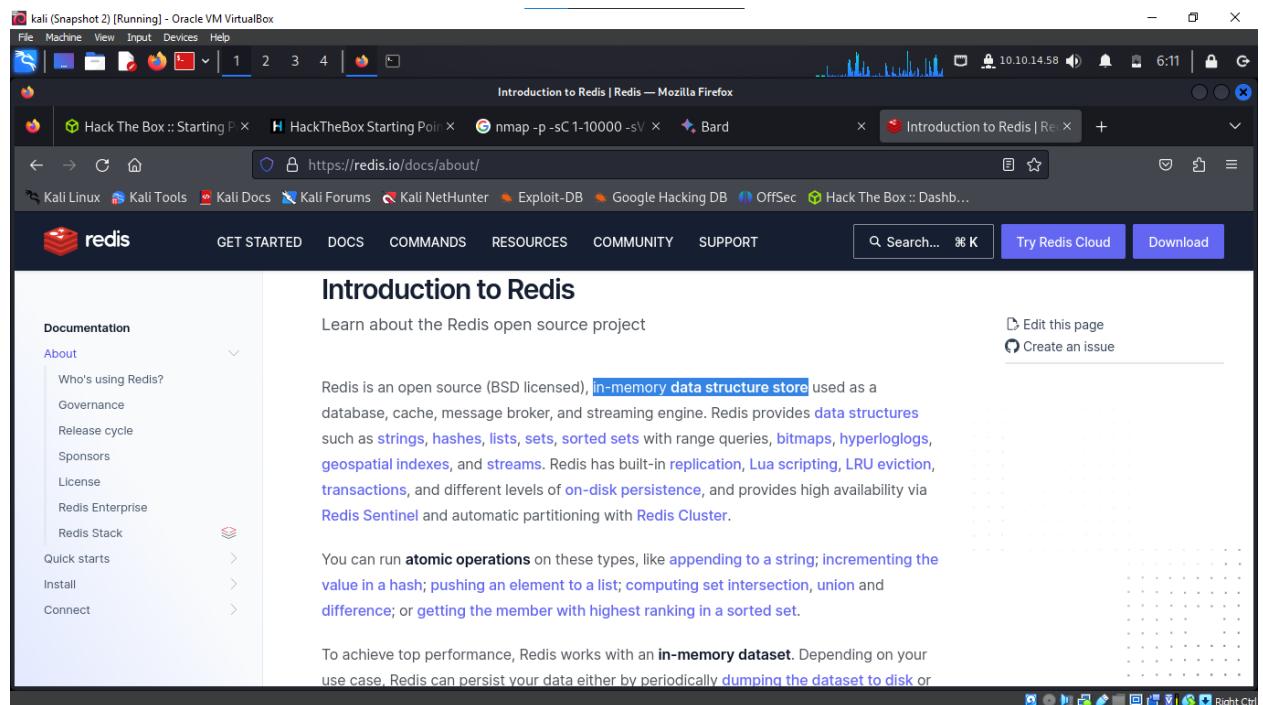
Task 2: Service on Open Port

- 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.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'redis-cli | Redis Documentation Center — Mozilla Firefox' at <https://docs.redis.com/latest/rs/references/cli-utilities/redis-cli/>. The page content is about the Redis command-line interface (redis-cli). The left sidebar has a 'Redis Enterprise Software' section with a 'Command-line utilities' link under 'Reference'. The right sidebar shows a 'Contents' menu with various Redis documentation links.

Task 5: Specifying Hostname in Redis

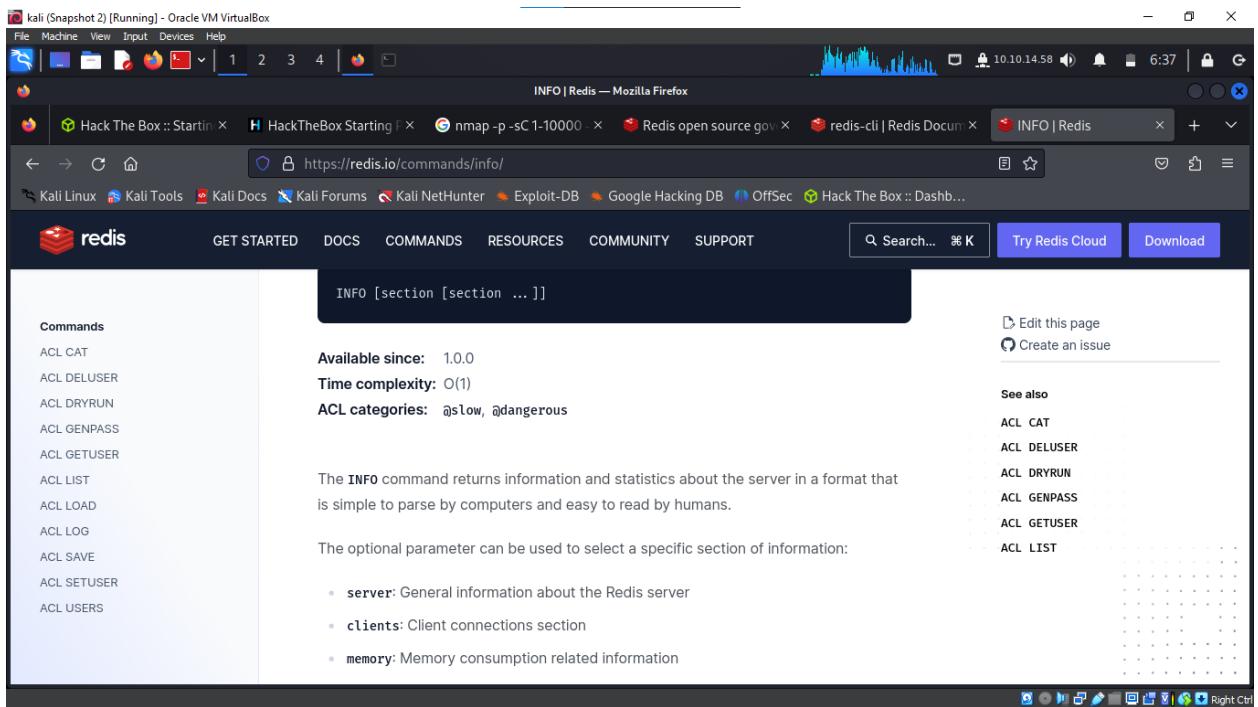
- **Question:** Which flag is used with Redis-cli to specify the hostname?
- **Answer:** -h
- **Details:** The '-h' flag is used to specify the target hostname in Redis-cli.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'redis-cli | Redis Documentation Center — Mozilla Firefox' at <https://docs.redis.com/latest/rs/references/cli-utilities/redis-cli/>. The page content is about the Redis command-line interface (redis-cli) configuration. The left sidebar has a 'Redis Enterprise Software' section with a 'Command-line utilities' link under 'Reference'. The right sidebar shows a 'Contents' menu with various Redis documentation links.

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.

```

kali@kali: ~$ redis
Command 'redis' not found, did you mean:
  command 'redir' from deb redir
  command 'pedis' from deb pep
  command 'iredis' from deb iredis
Try: sudo apt install <deb name>
kali@kali: ~$ redis-cli
Could not connect to Redis at 127.0.0.1:6379: Connection refused
not connected> 
Could not connect to Redis at 127.0.0.1:6379: Connection refused
not connected> 
kali@kali: ~$ redis-cli -h 10.129.181.232
10.129.181.232:6379> ls
(error) ERR unknown command 'ls', with args beginning with:
10.129.181.232:6379> clear
10.129.181.232:6379> 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

```

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.

The screenshot shows the Redis documentation for the `SELECT` command. The page has a header with links to GET STARTED, DOCS, COMMANDS, RESOURCES, COMMUNITY, SUPPORT, a search bar, and buttons for Try Redis Cloud and Download. The main content area is titled `SELECT` and contains the following information:

- Syntax:** `SELECT index`
- Available since:** 1.0.0
- Time complexity:** $O(1)$
- ACL categories:** `@fast, @connection`
- Description:** Select the Redis logical database having the specified zero-based numeric index. New connections always use the database 0.
- Note:** Selectable Redis databases are a form of namespacing: all databases are still persisted in the same RDB / AOF file. However different databases can have keys with the same name.
- See also:** AUTH, CLIENT CACHING, CLIENT GETNAME, CLIENT GETREDIR, CLIENT ID, CLIENT INFO, and a list of other Redis commands.

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.

The screenshot shows a terminal window on a Kali Linux VM. The user is running the Redis command-line interface (`redis-cli`). The session shows the following Redis commands and their responses:

```

role:master
connected_slaves:0
master_replid:da7e5ba859309f7516269c2cf20748c74314b39
master_replid2:0000000000000000000000000000000000000000
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:5.755107
used_cpu_user:6.307956
used_cpu_sys_children:0.000000
used_cpu_user_children:0.003666

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(11.62s)
10.129.181.232:6379> version
(error) ERR unknown command `version`, with args beginning with:
(2.38s)
10.129.181.232:6379> select 0
OK
(1.97s)
10.129.181.232:6379> keys *
1) "temp"
2) "flag"
3) "stor"
4) "numb"
10.129.181.232:6379>

```

Below the terminal, there is a challenge interface with the following text:

TASK 9
How many keys are present inside the database with index 0?

SUBMIT ANSWER **HINT**

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

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.

The screenshot shows a terminal window titled 'kali (Snapshot 2) [Running] - Oracle VM VirtualBox'. The terminal is running on a Kali Linux system. The user has performed several Redis commands:

```

role:master
connected_slaves:0
master_replid:dac7e5ba859309f7516269c2cf20748c74314b39
master_replid2:0000000000000000000000000000000000000000000000000000000000000000
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:5.755107
used_cpu_user:6.307956
used_cpu_sys_children:0.000000
used_cpu_user_children:0.003666

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(11.62s)
10.129.181.232:6379> version
(error) ERR unknown command `version` , with args beginning with:
(2.38s)
10.129.181.232:6379> select 0
OK
(1.97s)
10.129.181.232:6379> keys *
1) "temp"
2) "flag"
3) "stor"
4) "numb"
10.129.181.232:6379>

```

A task card is visible in the background with the title 'TASK 8' and the question 'How many keys are present inside the database with index 0?'. Below the terminal, a message asks 'Which command is used to obtain all the keys in a database?' with options: 1) 'keys *', 2) 'KEYS', 3) 'KEY', 4) 'KEYS*'.

Submit Root Flag

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

The screenshot shows a terminal window titled 'kali (Snapshot 2) [Running] - Oracle VM VirtualBox'. The terminal is running on a Kali Linux system. The user has performed several Redis commands:

```

role:master
connected_slaves:0
master_replid:dac7e5ba859309f7516269c2cf20748c74314b39
master_replid2:0000000000000000000000000000000000000000000000000000000000000000
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:5.755107
used_cpu_user:6.307956
used_cpu_sys_children:0.000000
used_cpu_user_children:0.003666

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(11.62s)
10.129.181.232:6379> version
(error) ERR unknown command `version` , with args beginning with:
(2.38s)
10.129.181.232:6379> select 0
OK
(1.97s)
10.129.181.232:6379> keys *
1) "temp"
2) "flag"
3) "stor"
4) "numb"
10.129.181.232:6379>

```

A task card is visible in the background with the title 'TASK 10' and the question 'Which command is used to obtain all the keys in a database?' with options: 1) 'keys *', 2) 'KEYS', 3) 'KEY', 4) 'KEYS*'.

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.

