SECTION 1: LINUX BASICS

1. **What is Linux, and how does it differ from other operating systems like Windows and macOS?**

System Name	Definition and cost	Source type	Distribution type	Security	User interface	Uses
Linux	An open-source operating system widely used in server environments and critical infrastructure **Cost:** Generally free	Open source, allowing specialists to inspect and modify the source code	Includes distributions tailored for cybersecurity, such as Kali Linux and Parrot Security OS.	Considered more secure due to frequent updates, high customizability, and its use in server environments.	Highly customizable, can be configured to meet cybersecurity requirements	Popular among cybersecurity experts due to specialized distributions and open-source tools like Metasploit and Wireshark
Windows	A closed-source operating system developed by Microsoft, popular on personal computers and in enterprises **Cost:** Requires a purchase license	Closed source, with some security tools provided by Microsoft	No specific distributions, but various security tools can be Installed	Provides strong security tools like Windows Defender, but is a common target for malware.	Familiar and user-friendly interface with integrated security tools	Widely used in corporate environments with security tools like Sysinternals Suite and Microsoft Security Essentials
macOS	A closed-source operating system developed by Apple, designed exclusively for Apple devices **Cost:** Comes free with Apple devices	Closed source, offering built-in security tools	No specific distributions, relies on built-in tools and third-party	Known for high security due to its closed ecosystem and regular updates.	Fixed and user-friendly interface with high security integration	Used In creative and corporate environments, with built-in security tools and support for third-party applications like Little Snitch and KnockKnock

2. **Name three popular Linux distributions and briefly describe one of them.**

- **Kali Linux**
- **Ubuntu**
- **Fedora**

Kali Linux:

A Linux distribution based on Debian, specifically designed for information security and penetration testing. It is developed and maintained by Offensive Security.

Key Features:

Extensive Security Tools: Includes over 600 tools specialized in cybersecurity.

Regular Updates: Frequent updates to the distribution and tools to ensure compatibility with the latest Threats

Ease of Use: Provides an integrated environment for penetration testing and digital forensics.

Common Uses: Penetration testing, digital forensics, and network analysis

3. **What is the root directory in Linux, and what is its significance?**

root directory:(denoted as `/`) Is the top-level directory in the file system hierarchy

Importance:

a. **Starting Point:** The root directory is the starting point for all other paths in the file system. All files and directories are organized under it

b. **File Organization:** It contains essential directories such as `/home` (for user files), `/etc` (for system configurations), `/var` (for variable files like logs), and `/bin` (for essential executables).

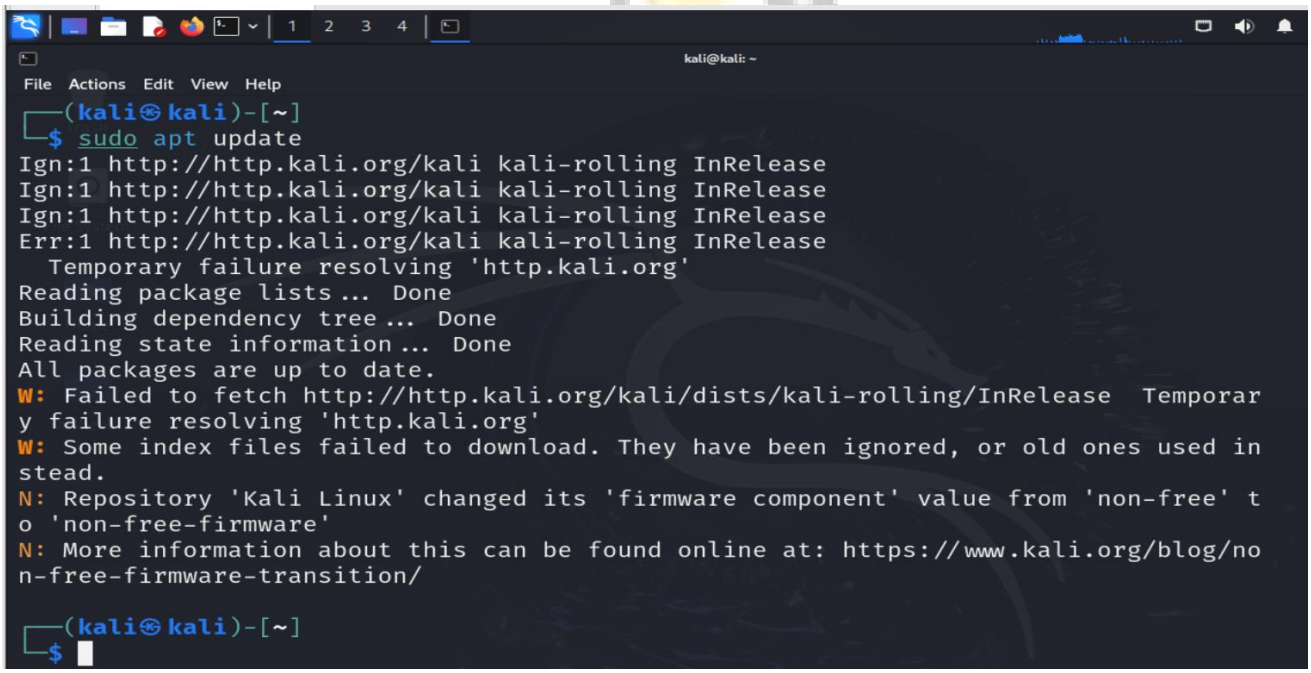
c. **Permission Management:** Accessing and modifying the root directory typically requires root (superuser) privileges to ensure system security and stability

d. **File System Structure:** The root directory forms the foundation of the file system structure in Linux, reflecting the overall organization of the system

4. **Explain the difference between an absolute path and a relative path in Linux.**

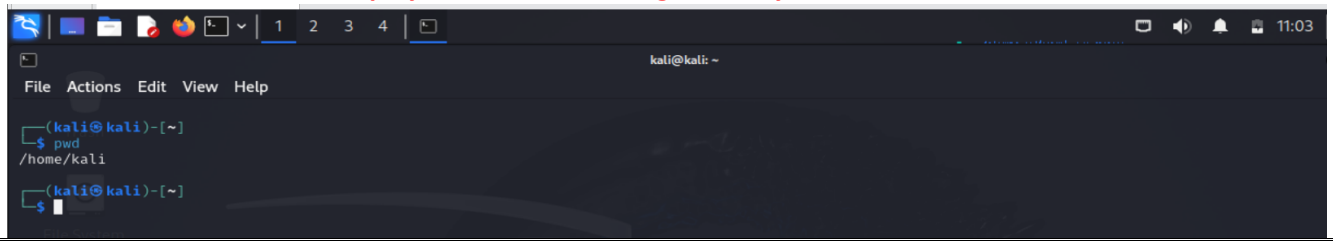
Path Name	Definition	Structure	Ex	Features
Absolute Path	The full path from the root directory	Starts with `/` and follows the complete file system hierarchy	`/home/user/Documents/file.txt`	-Independent of the current location. -Accurate and accessible from anywhere in the system
Relative Path	The path specified relative to the current location	Starts from the current directory and uses references like '.'	`Documents/file.txt` If you are in `/home/user	-Dependent on the current location. -Shorter and easier to use within the current context

5. **What command would you use to update the package list on a Debian-based system?**



SECTION 2: BASIC COMMANDS AND NAVIGATION

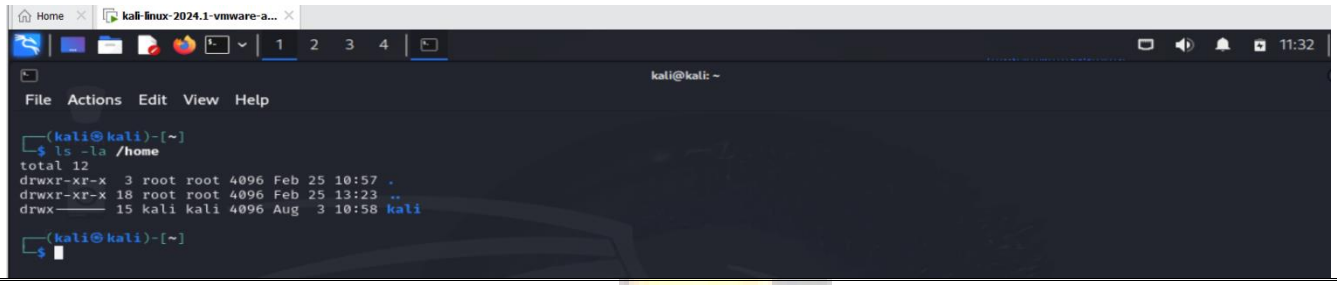
6. **Write the command to display the current working directory.**



7. **How do you change to the `/etc` directory from your current location?**

Some Command	Cd directory_name	Cd /path/to/directory	.. Cd	~ Cd
Use	To move to a subdirectory within the current directory	To move to a directory located at a specific path	To move to the parent directory (one level up):	To move to the home directory of the current user

8. **List the contents of the `/home` directory, including hidden files, in a detailed list format.**



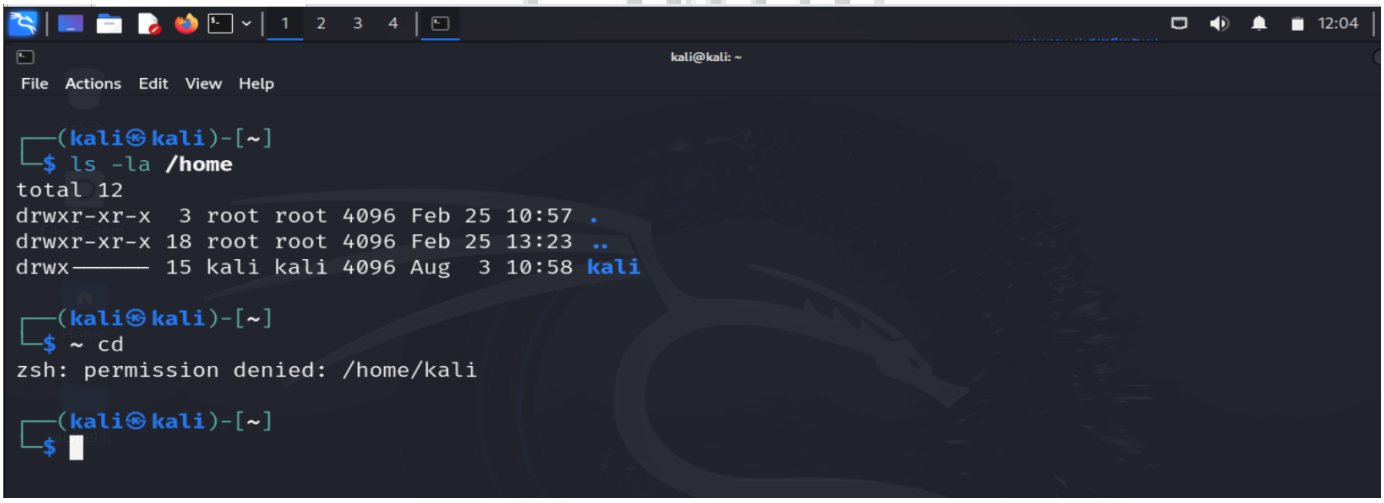
9. **Explain the purpose of the `ls -l` command and what information it provides.**

The `ls -l` command in Linux is used to list the contents of a directory in a detailed format.

When you use this command, it provides the following information about each file or directory in the directory:

Permissions: Shows the permissions granted to the file or directory for the user, group, and others.
Number of Links: Indicates the number of links pointing to the file or directory.
Owner Name: Shows who owns the file or directory
Group Name: Indicates the group the file or directory belongs to
Size: Displays the size of the file or directory In bytes
Date and Time: Shows the last modification date and time of the file or directory

10. **What command can be used to return to your home directory from any location in the file system?**



SECTION 3: FILE MANAGEMENT

11. **Write the command to create an empty file named `testfile.txt`.**

```
┌──(kali㉿kali)-[~]
└─$ touch estfile.txt

┌──(kali㉿kali)-[~]
└─$ ls -i estfile.txt
786495 estfile.txt

┌──(kali㉿kali)-[~]
└─$
```

12. **How do you create a directory named `testdir`?**

```
┌──(kali㉿kali)-[~]
└─$ mkdir testdir

┌──(kali㉿kali)-[~]
└─$ ls -d testdir
testdir

┌──(kali㉿kali)-[~]
└─$
```

13. **Write the command to copy `testfile.txt` to `backup_testfile.txt`.**

```
┌──(kali㉿kali)-[~]
└─$ touch testfile.txt

┌──(kali㉿kali)-[~]
└─$ cp testfile.txt backup_testfile.txt

┌──(kali㉿kali)-[~]
└─$ ls -i backup_testfile.txt
786539 backup_testfile.txt

┌──(kali㉿kali)-[~]
└─$
```

14. **What command would you use to move (rename) `testfile.txt` to `newfile.txt`?**

```
┌──(kali㉿kali)-[~]
└─$ mv testfile.txt newfile.txt

┌──(kali㉿kali)-[~]
└─$ ls -i newfile.txt
786524 newfile.txt

┌──(kali㉿kali)-[~]
└─$
```

15. **Write the command to remove the directory `testdir` and its contents.**

```
┌──(kali㉿kali)-[~]
└─$ rm -r testdir

┌──(kali㉿kali)-[~]
└─$ ls -i
786539 backup_testfile.txt  786473 Downloads    786524 newfile.txt  786474 Templates
786472 Desktop              786495 estfile.txt  786478 Pictures     786479 Videos
786476 Documents            786477 Music        786475 Public

┌──(kali㉿kali)-[~]
└─$
```

SECTION 4: USER AND GROUP MANAGEMENT

16. **How can you list all existing users on the system?**

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
[sudo] password for kali:
root:*:19778:0:99999:7:::
daemon:*:19778:0:99999:7:::
bin:*:19778:0:99999:7:::
sys:*:19778:0:99999:7:::
sync:*:19778:0:99999:7:::
games:*:19778:0:99999:7:::
man:*:19778:0:99999:7:::
lp:*:19778:0:99999:7:::
mail:*:19778:0:99999:7:::
news:*:19778:0:99999:7:::
uucp:*:19778:0:99999:7:::
proxy:*:19778:0:99999:7:::
www-data:*:19778:0:99999:7:::
backup:*:19778:0:99999:7:::
list:*:19778:0:99999:7:::
irc:*:19778:0:99999:7:::
_apt:*:19778:0:99999:7:::
nobody:*:19778:0:99999:7:::
systemd-network:!*:19778::::::
systemd-timesync:!*:19778::::::
messagebus:!:19778::::::
```

17. **Write the command to create a new user with the username `alshebli`.**

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd alshebli

┌──(kali㉿kali)-[~]
└─$ sudo passwd alshebli
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$
```

18. **How do you create a new group named `alsheblirоup`?**

```
┌──(kali㉿kali)-[~]
└─$ sudo groupadd alshebligroup
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ getent group alshebligroup
alshebligroup:x:1002:

┌──(kali㉿kali)-[~]
└─$
```

19. **Write the command to add the user `alshebli` to the group `alshebligroup`.**

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG alshebligroup alshebli

┌──(kali㉿kali)-[~]
└─$ id alshebli
uid=1001(alshebli) gid=1001(alshebli) groups=1001(alshebli),1002(alshebligroup)

┌──(kali㉿kali)-[~]
└─$
```

20. **What command would you use to change the password for the user `alshebli`?**

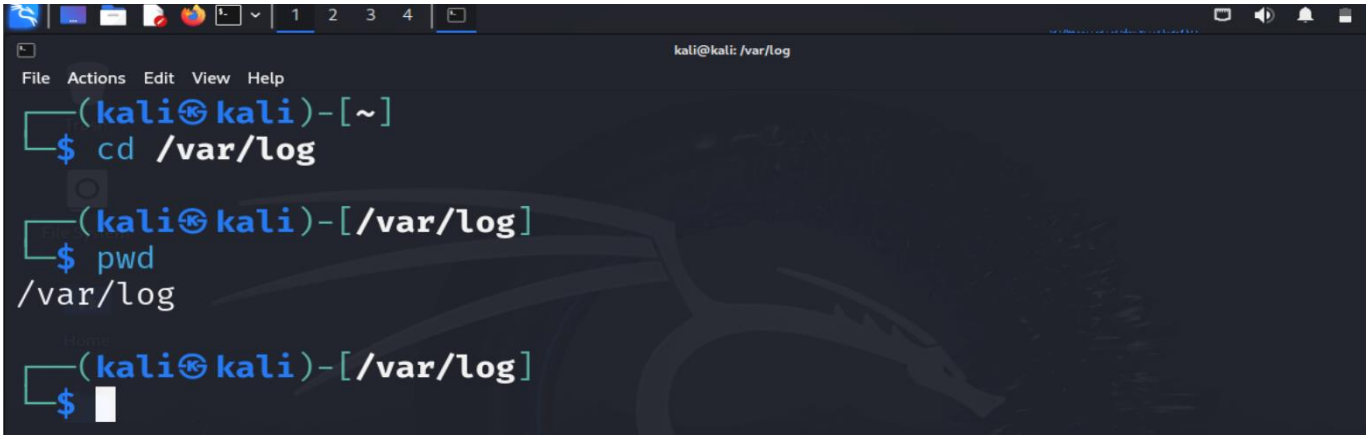
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd alshebli
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo passwd -S alshebli
alshebli P 2024-08-03 0 99999 7 -1

┌──(kali㉿kali)-[~]
└─$
```

SECTION 5: PRACTICAL APPLICATION

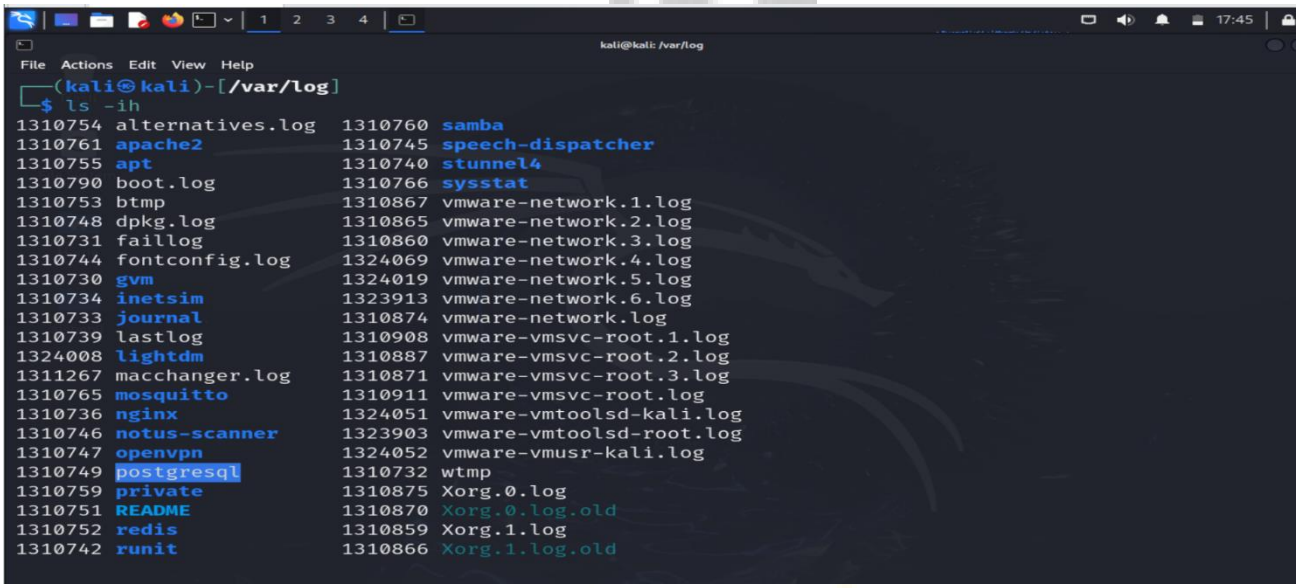
21. **Describe the steps you would take to install a Linux distribution on a virtual machine.**
To install a Linux distribution on a virtual machine, follow these steps:

- **Install Virtual Machine Software:** Such as VirtualBox or VMware.
- **Download the ISO Image:** From the desired Linux distribution's website.
- **Create a Virtual Machine:** Using the virtual machine software.
- **Configure Resources:** Allocate memory and disk size.
- **Attach the ISO Image:** As the boot medium.
- **Start the Virtual Machine:** And install the distribution from the ISO.
- **Follow Installation Instructions:** To set up the distribution and configure user accounts.

22. **If you are in the `/home/user` directory, what command would you use to navigate to `/var/log`?**



23. **How do you display the contents of the current directory in a human-readable format?**



24. **Explain what the following command does: `cp -r /home/user/docs /home/user/docs_backup`.**

command	Explaining
cp	This Is the command for copying files and directories
-r	This option stands for "recursive," which means it will copy directories and their contents
/home/user/docs	This Is the path to the source directory you want to copy
/home/user/docs_backup	This is the path to the destination where the directory will be copied

25. **What is the difference between the `rm` and `rm -r` commands?**

command	difference
rm	This command is used to delete files only. It will fail with an error if you try to delete a directory with it
rm -r	This command is used to delete files and directories recursively. The `-r` option stands for "recursive," allowing it to delete directories and all their contents, including subdirectories and files.

26. **Explain the significance of the `/etc` directory in Linux.**

the `/etc` directory contains essential configuration files for the system and applications, such as network settings, user information, and service configurations. It is crucial for system management and customization.

تم بحمد الله

Prepared By Eng.	**Alshebli Fisal Ahmeb Al-Shebli**
Subject	**Cyber Security**
Subject teacher	**Eng. Abdulrazzaq Al-Samawi**