

الامن السيبراني

عمل الطالب / اصيل حفيظ

Information Transfer

Subsystem Organization

Modular Assembly

Technology Level Increase

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Technological Simplicity

Security Report
GEN-07:18:13pm

Security Report
GEN-07:18:13pm

Security Report
GEN-07:18:13pm

Security Report
GEN-07:18:13pm

Security Report
GEN-07:18:13pm

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

Feature	Linux	Windows	macOS
Source	Open source; code can be modified and distributed freely.	Closed source; proprietary to Microsoft.	Closed source; proprietary to Apple.
Cost	Generally free; no licensing fees.	Requires purchasing a license; can be costly.	Included in the price of Apple devices; no additional fees.
Customization	Highly customizable with multiple desktop environments.	Limited customization; mainly themes and settings.	Limited customization; focuses on a unified experience.
Security	Known for high security and quick vulnerability patches.	More susceptible to malware; receives regular updates.	Secure, but can still be targeted; regular updates provided.
Software	Supports open-source software; may lack compatibility with some proprietary software.	Extensive library of proprietary software and games.	Compatible with creative software like Adobe; smaller game library.
User Interface	Varied interfaces depending on the distribution; can have a learning curve.	Consistent and user-friendly interface.	Polished and intuitive interface.
Use Cases	Popular in servers, cloud computing, and embedded systems.	Widely used in business, gaming, and personal computing.	Preferred for creative work and within the Apple ecosystem.

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

1. **Ubuntu**
2. **Fedora**
3. **Debian**

Brief Description of Ubuntu

Ubuntu is one of the most popular and user-friendly Linux distributions. It is based on Debian and is developed by Canonical Ltd. Ubuntu is known for its ease of use, making it a great choice for beginners and those transitioning from other operating systems like Windows or macOS. It provides a polished and cohesive user experience with a wide range of pre-installed applications and a robust software center for installing additional software.

Key Features of Ubuntu:

- **User-Friendly Interface:** Ubuntu features a clean and intuitive interface, with the GNOME desktop environment being the default in the latest versions. It also offers other desktop environments like KDE and XFCE through variants such as Kubuntu and Xubuntu.
- **Regular Updates:** Ubuntu follows a predictable release cycle with Long Term Support (LTS) versions released every two years. These LTS releases are supported for five years, providing users with stability and security updates over an extended period.
- **Community Support:** Ubuntu has a large and active community, offering extensive documentation, forums, and support channels. This makes it easy for users to find help and resources for troubleshooting and learning.
- **Wide Range of Applications:** Ubuntu provides access to a vast repository of open-source software through its software center, as well as support for popular third-party applications like Spotify, Steam, and Microsoft Teams.

- **Strong Security:** Ubuntu is known for its focus on security, offering regular updates and patches, as well as features like built-in firewall and encryption options to protect user data.

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

In Linux, the root directory is denoted by a single forward slash (/). It's the topmost directory in the filesystem hierarchy, and everything on the system is organized within it. Here's why it's significant:

1. **Hierarchy:** The root directory serves as the starting point for the filesystem hierarchy. All other directories and files are organized under this root.
2. **System Structure:** Essential system directories like `/bin` (binaries), `/etc` (configuration files), `/home` (user directories), `/lib` (libraries), and `/var` (variable data) are located directly under the root directory.
3. **Permissions:** Typically, only the root user (superuser) has unrestricted access to the root directory and its subdirectories. This helps in maintaining system security and integrity.
4. **Mount Points:** Additional filesystems or partitions can be mounted at various points within the root directory. For example, an external drive might be mounted at `/mnt/external`.

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

Feature	Absolute Path	Relative Path
Definition	A complete path from the root directory (/) to the specified file or directory	A path relative to the current working directory to the target file or directory
Starts With	Starts with a forward slash (/)	Does not start with a forward slash (/)
Example	<code>/home/user/Documents/report.txt</code>	<code>Documents/report.txt</code>
Usage	Used to specify the exact location of a file or directory regardless of the current working directory	Used for navigation within the current directory structure easily
Changes with Directory Change	Does not change, as it specifies the location based on the root	Changes based on the current working directory

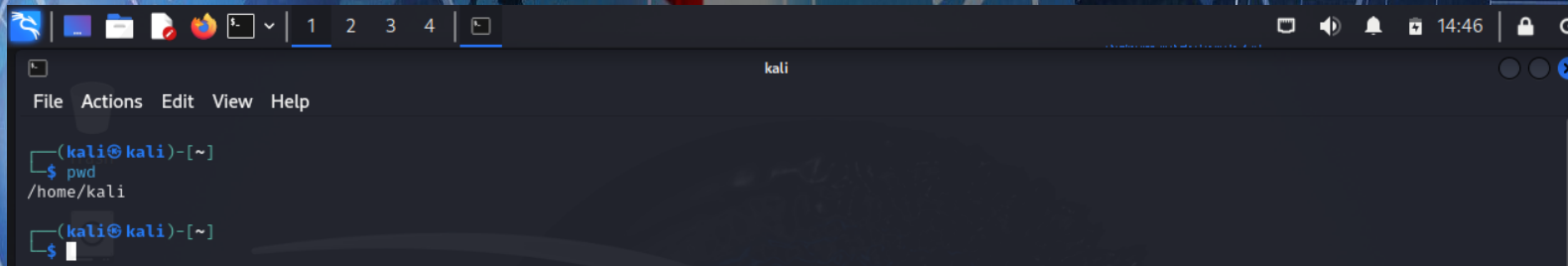
5. What command would you use to update the package list on a Debian-based system?

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
19% [2 Packages 4,478 kB/19.9 MB 23%] 19.9 kB/s 54min 5s^
20% [2 Packages 5,110 kB/19.9 MB 26%] 19.9 kB/s 53min 33s^
20% [2 Packages 5,210 kB/19.9 MB 26%] 22.5 kB/s 47min 12s^
20% [2 Packages 5,230 kB/19.9 MB 26%] 22.5 kB/s 47min 11s^
20% [2 Packages 5,338 kB/19.9 MB 27%] 21.1 kB/s 50min 20s^
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.6 MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Err:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
File has unexpected size (47556274 ≠ 47554462). Mirror sync in progress? [IP: 104.17.254.239 80]
Err:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
File has unexpected size (47556274 ≠ 47554462). Mirror sync in progress? [IP: 104.17.254.239 80]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [267 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [863 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 21.4 MB in 10min 59s (32.5 kB/s)
Reading package lists... Done
E: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/main/Contents-amd64 File has unexpected size (47556274 ≠ 47554462). Mirror sync in progr
ess? [IP: 104.17.254.239 80]
E: Some index files failed to download. They have been ignored, or old ones used instead.
N: Repository 'Kali Linux' changed its 'firmware component' value from 'non-free' to 'non-free-firmware'
N: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/
(kali@kali)-[~]
$

```


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

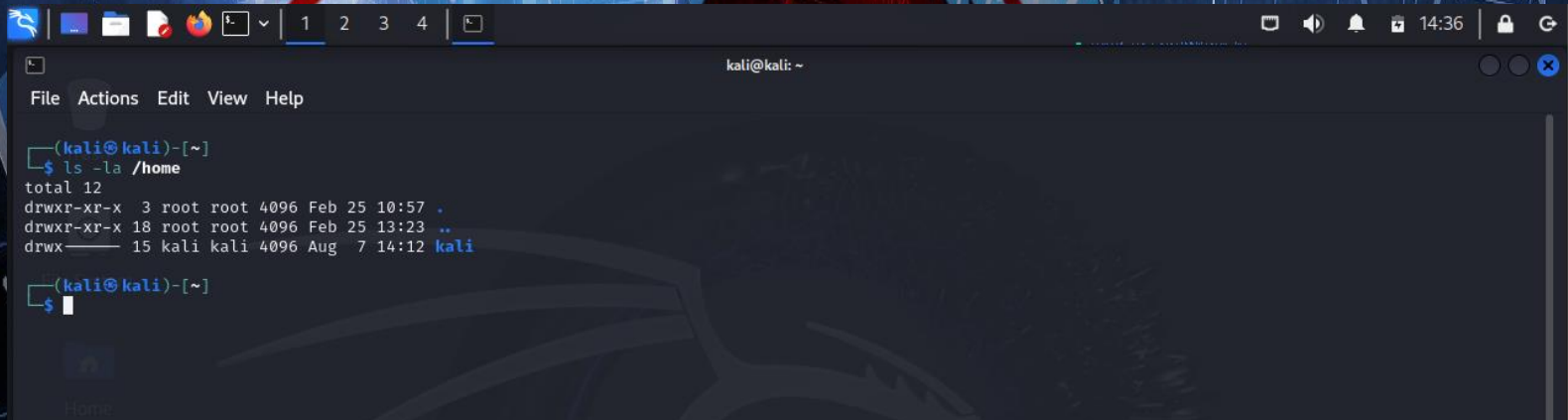


```
kali
File Actions Edit View Help

(kali@kali)-[~]
$ pwd
/home/kali

(kali@kali)-[~]
$
```

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

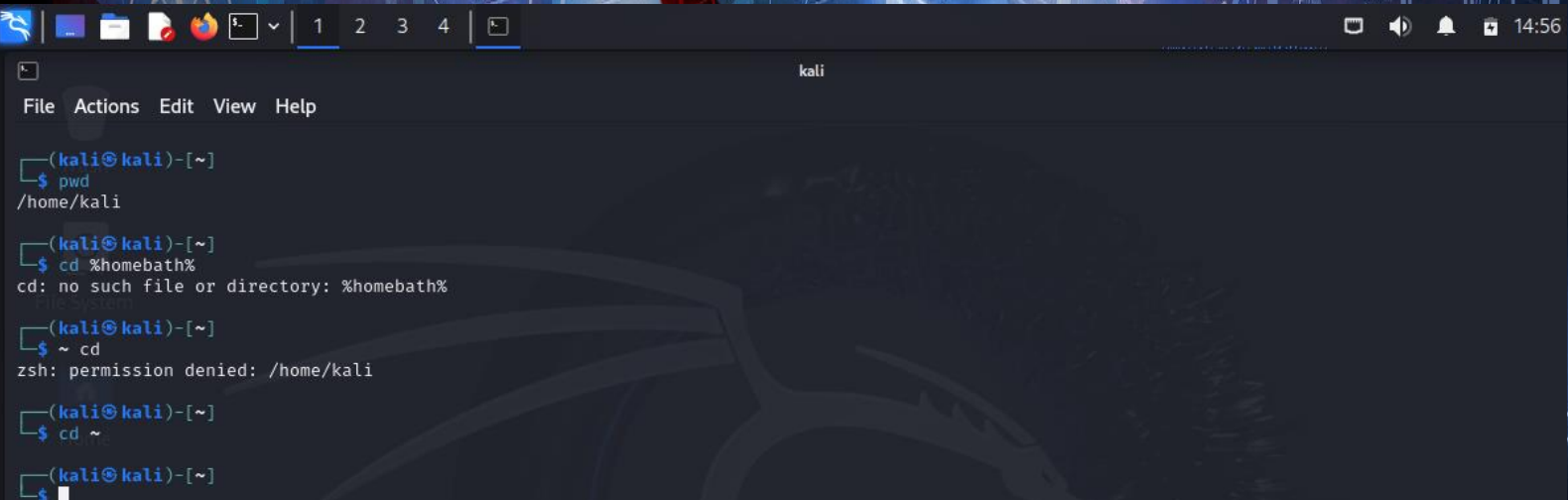


```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ls -la /home
total 12
drwxr-xr-x  3 root root 4096 Feb 25 10:57 .
drwxr-xr-x 18 root root 4096 Feb 25 13:23 ..
drwx----- 15 kali kali 4096 Aug  7 14:12 kali

(kali@kali)-[~]
$
```

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



```
kali
File Actions Edit View Help

(kali@kali)-[~]
$ pwd
/home/kali

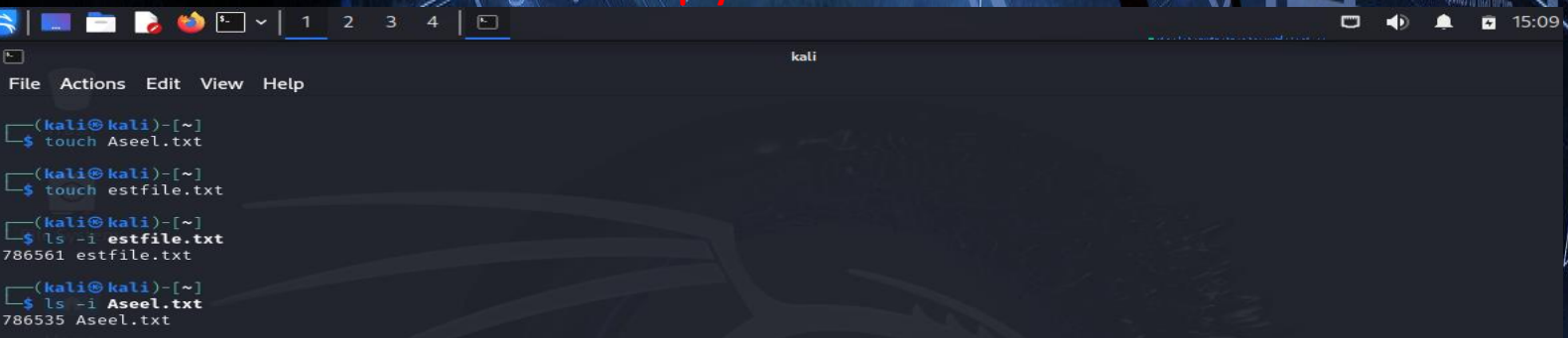
(kali@kali)-[~]
$ cd %homebath%
cd: no such file or directory: %homebath%

(kali@kali)-[~]
$ ~ cd
zsh: permission denied: /home/kali

(kali@kali)-[~]
$ cd ~

(kali@kali)-[~]
$
```

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



```
kali
File Actions Edit View Help

(kali@kali)-[~]
$ touch Aseel.txt

(kali@kali)-[~]
$ touch estfile.txt

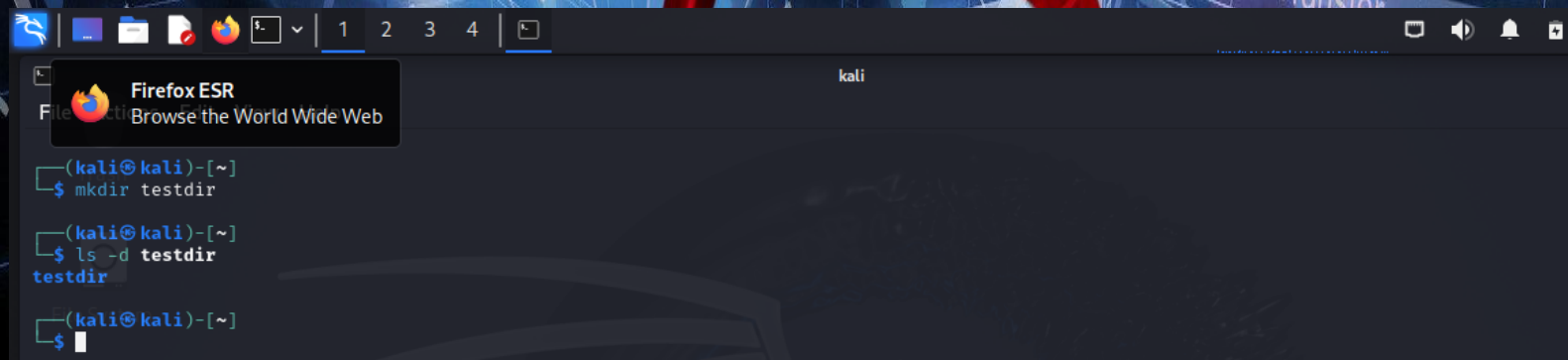
(kali@kali)-[~]
$ ls -l estfile.txt
786561 estfile.txt

(kali@kali)-[~]
$ ls -l Aseel.txt
786535 Aseel.txt
```

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

Type	Description	Command
Absolute Path	Refers to the <code>/etc</code> directory using the full path from the root.	<code>cd /etc</code>
Relative Path	Refers to the <code>/etc</code> directory based on the current location. In this case, a relative path is not suitable since <code>/etc</code> is an absolute path.	Not applicable here, as <code>/etc</code> is an absolute path.

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

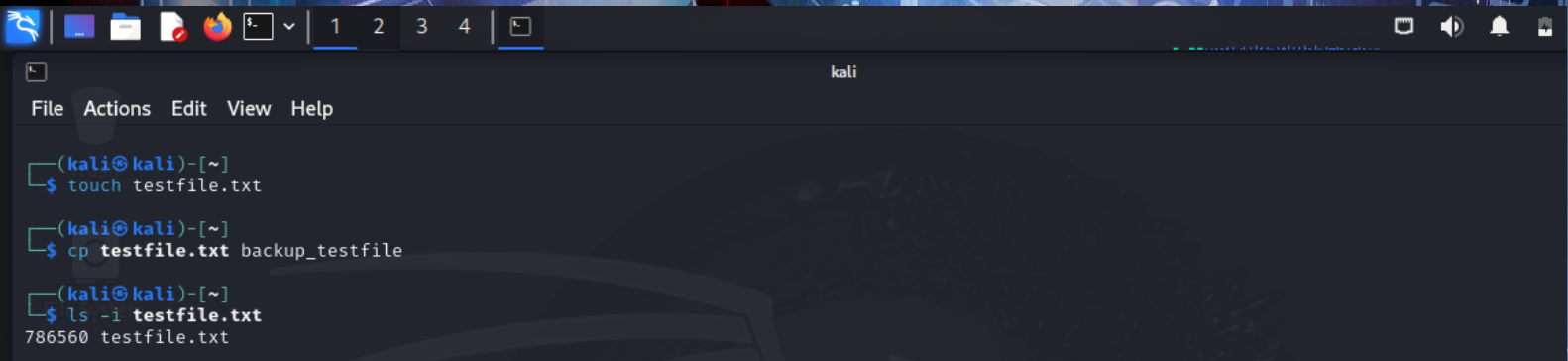


```
(kali㉿kali)-[~]
$ mkdir testdir

(kali㉿kali)-[~]
$ ls -ld 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

(kali㉿kali)-[~]
$ ls -li testfile.txt
786560 testfile.txt
```

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

When you run `ls -l`, the output includes the following columns:

1. **File Type and Permissions:**
 - **Example:** `-rwxr-xr--`

- The first character indicates the type of file (- for a regular file, d for a directory, l for a symbolic link). The next nine characters show file permissions (read, write, execute) for the owner, group, and others.
- 2. **Number of Links:**
 - **Example:** 1
 - The number of hard links to the file or directory. For directories, this counts links to subdirectories.
- 3. **Owner:**
 - **Example:** user
 - The username of the file's owner.
- 4. **Group:**
 - **Example:** group
 - The group name associated with the file.
- 5. **File Size:**
 - **Example:** 4096
 - The size of the file in bytes.
- 6. **Modification Date and Time:**
 - **Example:** Aug 7 12:34
 - The date and time when the file was last modified.
- 7. **File or Directory Name:**
 - **Example:** example.txt
 - The name of the file or directory.

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

```
kali
File Actions Edit View Help

(kali@kali)~$ mv testfile.txt newfile.txt

(kali@kali)~$ ls -li newfile.txt
786560 newfile.txt

(kali@kali)~$
```

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

```
kali
File Actions Edit View Help

(kali@kali)~$ rm -r testdir

(kali@kali)~$ ls -li
786518 aseel      786564 backup_testfile  786476 Documents  786561 estfile.txt  786560 newfile.txt  786475 Public      786479 Videos
786535 Aseel.txt  786472 Desktop          786473 Downloads  786477 Music       786478 Pictures    786474 Templates
```


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

```
kali
File Actions Edit View Help

(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:!:19778:0:99999:7:::
systemd-timesync:!:19778:0:99999:7:::
messagebus:!:19778:0:99999:7:::
tss:!:19778:0:99999:7:::
strongswan:!:19778:0:99999:7:::
tcpdump:!:19778:0:99999:7:::
```

17. Write the command to create a new user with the username 'aseel'

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo useradd Aseel
[sudo] password for kali:

(kali@kali)-[~]
$ sudo passwd Aseel
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
$
```

18. How do you create a new group named 'aseel'?

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo groupadd aseelgroup

(kali@kali)-[~]
$ getent group aseelgroup
aseelgroup:x:1003:

(kali@kali)-[~]
$
```


19. Write the command to add the user `aseel` to the group `aseel`

```
(kali㉿kali)-[~]
$ sudo usermod -aG Aseelgroup Aseel
usermod: group 'Aseelgroup' does not exist

(kali㉿kali)-[~]
$ getent group Aseelgroup

(kali㉿kali)-[~]
$ id Aseel
uid=1001(Aseel) gid=1001(Aseel) groups=1001(Aseel)

(kali㉿kali)-[~]
$
```

20. What command would you use to change the password for the user

```
(kali㉿kali)-[~]
$ sudo passwd Aseel
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ sudo chage -l Aseel
Last password change           : Aug 07, 2024
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

(kali㉿kali)-[~]
$
```

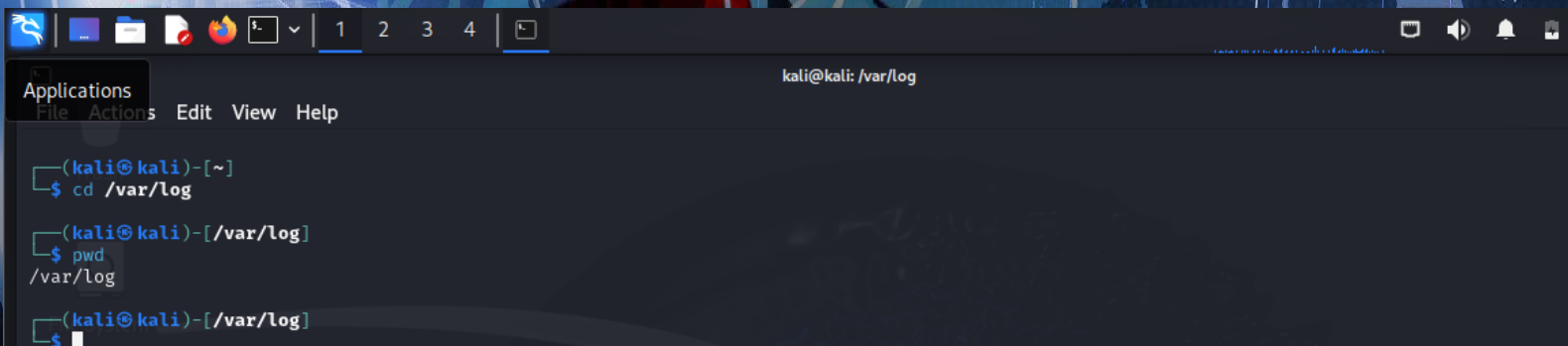
21. Describe the steps you would take to install a Linux distribution on a virtual machine.

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.

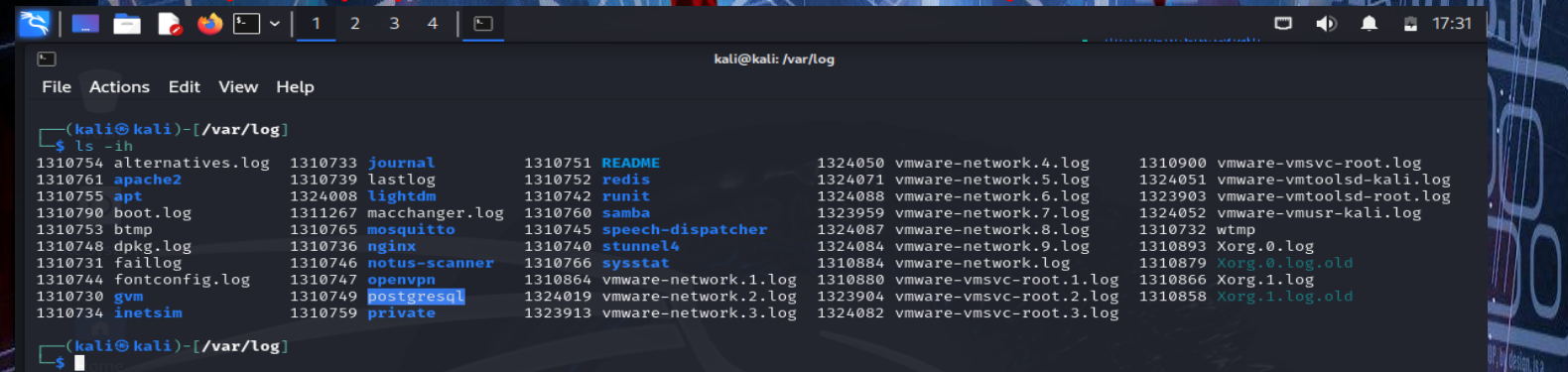
22. If you are in the `/home/user` directory, what command would you use to navigate to `/var/log`?



A terminal window titled 'kali@kali: /var/log' showing the process of navigating to the /var/log directory. The user starts at the home directory (~) and enters 'cd /var/log'. The prompt changes to show the current directory is /var/log. The user then enters 'pwd' and the output is /var/log.

```
(kali@kali)-[~]  
$ cd /var/log  
  
(kali@kali)-[/var/log]  
$ pwd  
/var/log  
  
(kali@kali)-[/var/log]  
$
```

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



A terminal window titled 'kali@kali: /var/log' showing the output of the 'ls -lh' command. The output lists various log files in a human-readable format, including alternatives.log, apache2, apt, boot.log, btmap, faillog, fontconfig.log, gvm, inetsim, journal, lastlog, lightdm, macchanger.log, mosquitto, nginx, notus-scanner, openvpn, postgresql, private, README, redis, runit, samba, speech-dispatcher, stunnel4, sysstat, vmware-network.1.log, vmware-network.2.log, vmware-network.3.log, vmware-network.4.log, vmware-network.5.log, vmware-network.6.log, vmware-network.7.log, vmware-network.8.log, vmware-network.9.log, vmware-network.log, vmware-vmtoolsd-kali.log, vmware-vmtoolsd-root.log, vmware-vmusr-kali.log, wtmp, Xorg.0.log, Xorg.0.log.old, Xorg.1.log, and Xorg.1.log.old.

```
(kali@kali)-[/var/log]  
$ ls -lh  
1310754 alternatives.log 1310733 journal 1310751 README 1324050 vmware-network.4.log 1310900 vmware-vmtoolsd-kali.log  
1310761 apache2 1310739 lastlog 1310752 redis 1324071 vmware-network.5.log 1324051 vmware-vmtoolsd-root.log  
1310755 apt 1324008 lightdm 1310742 runit 1324088 vmware-network.6.log 1323903 vmware-vmtoolsd-root.log  
1310790 boot.log 1311267 macchanger.log 1310760 samba 1323959 vmware-network.7.log 1324052 vmware-vmusr-kali.log  
1310753 btmap 1310765 mosquitto 1310745 speech-dispatcher 1324087 vmware-network.8.log 1310732 wtmp  
1310748 dpkg.log 1310736 nginx 1310740 stunnel4 1324084 vmware-network.9.log 1310893 Xorg.0.log  
1310731 faillog 1310746 notus-scanner 1310766 sysstat 1310884 vmware-network.log 1310879 Xorg.0.log.old  
1310744 fontconfig.log 1310747 openvpn 1310864 vmware-network.1.log 1310880 vmware-vmtoolsd-root.1.log 1310866 Xorg.1.log  
1310730 gvm 1310749 postgresql 1324019 vmware-network.2.log 1323904 vmware-vmtoolsd-root.2.log 1310858 Xorg.1.log.old  
1310734 inetsim 1310759 private 1323913 vmware-network.3.log 1324082 vmware-vmtoolsd-root.3.log  
  
(kali@kali)-[/var/log]  
$
```


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

Part	Description
<code>cp</code>	The basic command for copying files and directories.
<code>-r</code>	The option that stands for "recursive." It copies directories and their contents recursively.
<code>/home/user/docs</code>	The path to the source directory that you want to copy.
<code>/home/user/docs_backup</code>	The path to the destination. If <code>docs_backup</code> does not exist, it will be created, and the <code>docs</code> directory will be copied into it.

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

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

The `/etc` directory in Linux is crucial because it contains system-wide configuration files and directories. It holds:

- **Configuration Files:** Settings for the system and applications (e.g., `/etc/fstab`, `/etc/passwd`).
- **Service Configurations:** Files for system services and daemons (e.g., `/etc/ssh/sshd_config`).
- **Security Settings:** Security and user permissions (e.g., `/etc/sudoers`).
- **Initialization Scripts:** Scripts run during system startup and shutdown.

System Defaults: Default configurations for various applications



Information Transfer

Vulnerability Report

GEN-07:18:13pm

Subsystem Organization

Molecular Assembly

Technology Level Increase

Technological Singularity



UDP, by design, is a connection-less protocol that does not update source IP addresses. Unless the application layer protocol uses a connection-less protocol such as UDP, it is very easy to forge the IP packet diagram to include an arbitrary source IP address [1]. When multiple packets have their source IP address forged to a single address, the server responds to that victim, creating a reflected Denial of Service (DoS) Attack. Recently, certain UDP protocols have been found to have particular