Cyber security

Kali Linux

الاسم : حميد احمد حميد علي يحيى

جامعة الرازي المجموعة الثانية عملي

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

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

Ubuntu :

- It is stable and easy-to-use operating system.
- It is based on the GNOME GUL.
- It features strong support for various components and devise.
- It is widely used in office machines and portable.

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

root directory:

is the foundation of the Linux file system hierarch .it is represented by a forward slash (/) and is the parent of all other directories and file on the system.

Importance :

- **Starting Point:** The root directory is the starting point for all other

paths in the file system. All files and directories are organized

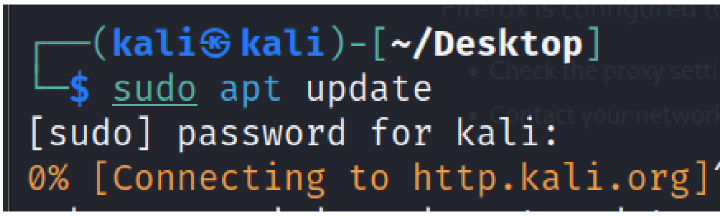
under it

- **System File :** **It house crucial system files, including :**
  - **Bootloaders and kernel-related files**
  - **Configuration file for system service**
  - **Libraries used by applications**
  - **Essential binaries**
- **User Data :** **While not directly storing user data < it contains directories like /home**

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

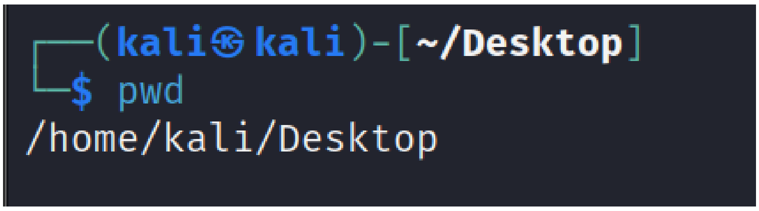
5. What command would you use to update the package list on a Debian-based system?



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt update
[sudo] password for kali:
0% [Connecting to http.kali.org]
```

Section 2: Basic Commands and Navigation:

6. Write the command to display the current working directory

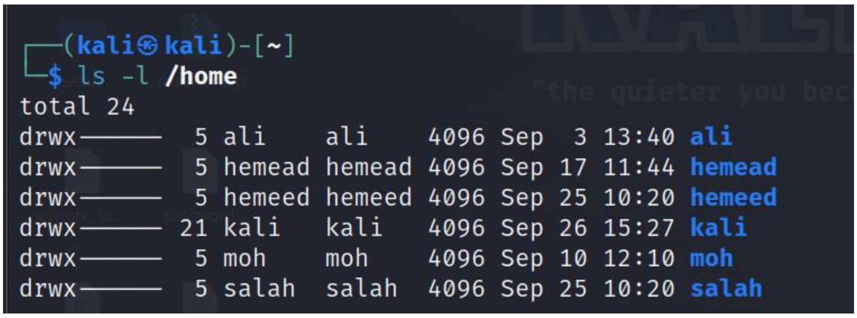


```
┌──(kali㉿kali)-[~/Desktop]
└─$ pwd
/home/kali/Desktop
```

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.



```
┌──(kali㉿kali)-[~]
└─$ ls -l /home
total 24
drwx------  5 ali    ali    4096 Sep  3 13:40 ali
drwx------  5 hemead hemead 4096 Sep 17 11:44 hemead
drwx------  5 hemeed hemeed 4096 Sep 25 10:20 hemeed
drwx------ 21 kali   kali   4096 Sep 26 15:27 kali
drwx------  5 moh    moh    4096 Sep 10 12:10 moh
drwx------  5 salah  salah  4096 Sep 25 10:20 salah
```

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 .

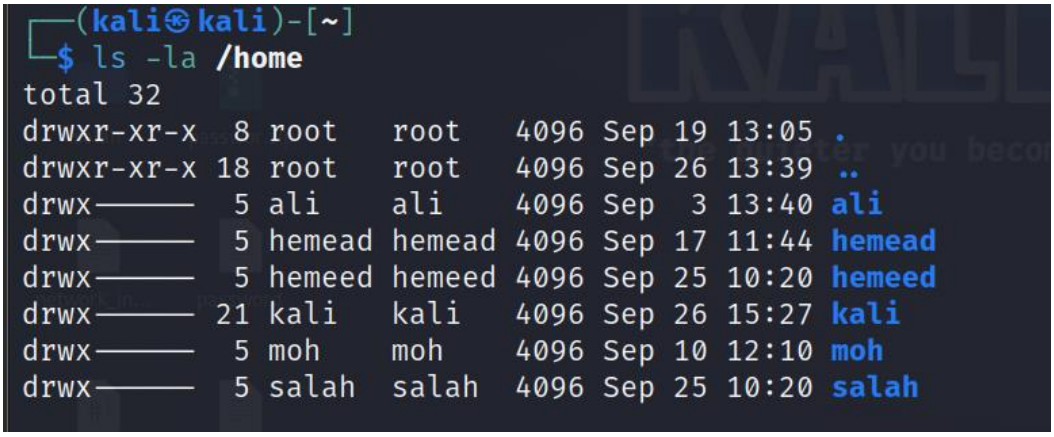
Owner Name: Shows who owns the file or directory

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

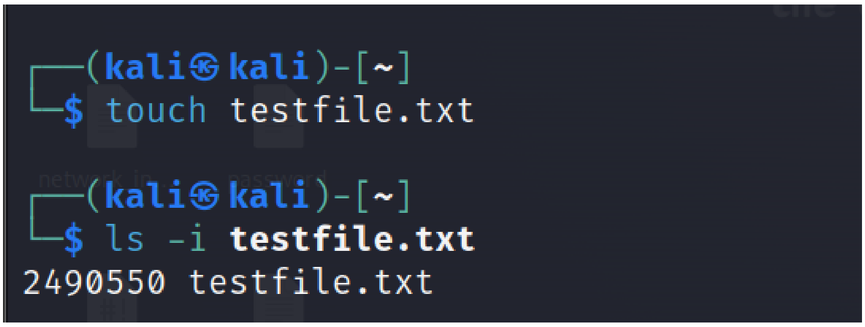
10. **What command can be used to return to your home directory from any location in the file system?**



```
┌──(kali㉿kali)-[~]
└─$ ls -la /home
total 32
drwxr-xr-x  8 root   root   4096 Sep 19 13:05 .
drwxr-xr-x 18 root   root   4096 Sep 26 13:39 ..
drwx------  5 ali    ali    4096 Sep  3 13:40 ali
drwx------  5 hemead hemead 4096 Sep 17 11:44 hemead
drwx------  5 hemeed hemeed 4096 Sep 25 10:20 hemeed
drwx------ 21 kali   kali   4096 Sep 26 15:27 kali
drwx------  5 moh    moh    4096 Sep 10 12:10 moh
drwx------  5 salah  salah  4096 Sep 25 10:20 salah
```

Section 3: File Management:

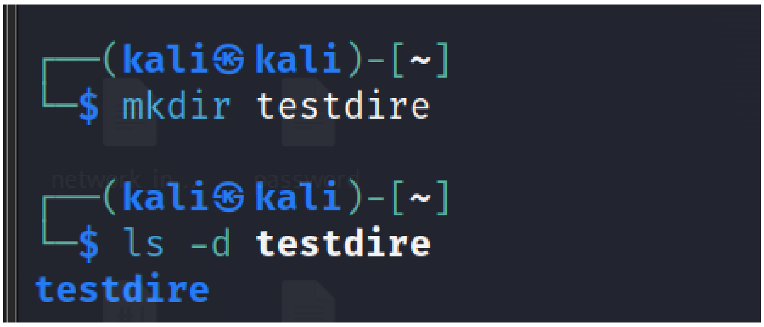
11. Write the command to create an empty file named `testfile.txt`.



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

┌──(kali㉿kali)-[~]
└─$ ls -i testfile.txt
2490550 testfile.txt
```

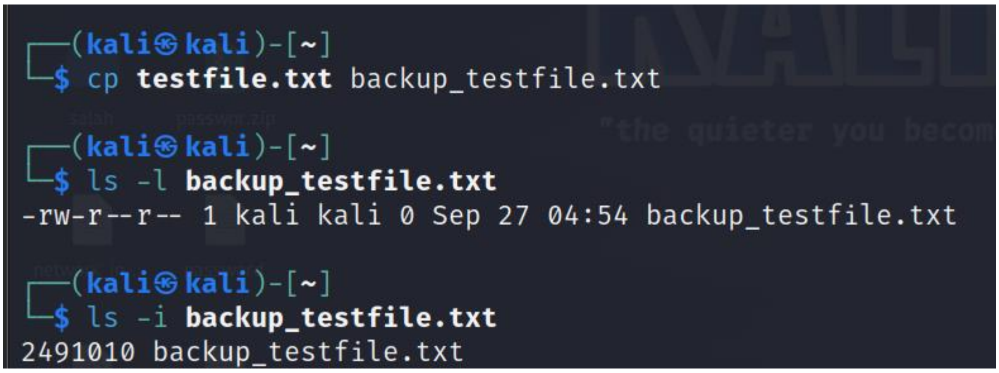
12. How do you create a directory named `testdir`?



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

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

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

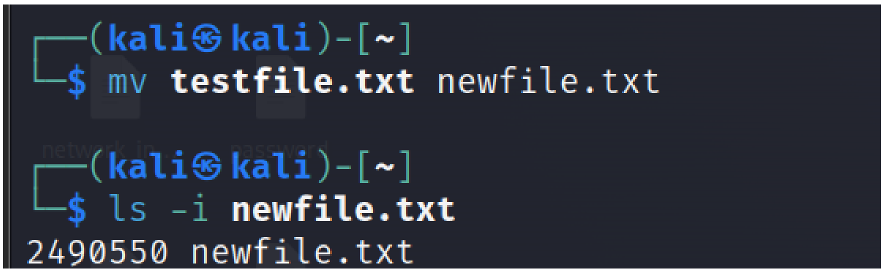


```
┌──(kali㉿kali)-[~]
└─$ cp testfile.txt backup_testfile.txt

┌──(kali㉿kali)-[~]
└─$ ls -l backup_testfile.txt
-rw-r--r-- 1 kali kali 0 Sep 27 04:54 backup_testfile.txt

┌──(kali㉿kali)-[~]
└─$ ls -i backup_testfile.txt
2491010 backup_testfile.txt
```

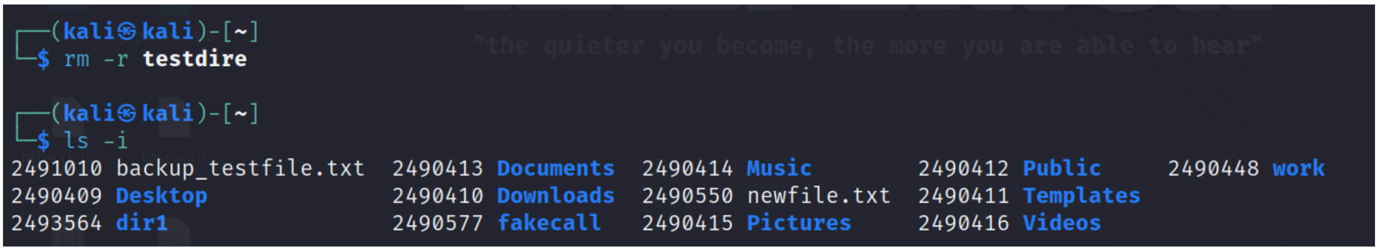
14. What command would you use to move (rename) `testfile.txt` to `newfile.txt`?



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

┌──(kali㉿kali)-[~]
└─$ ls -i newfile.txt
2490550 newfile.txt
```

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

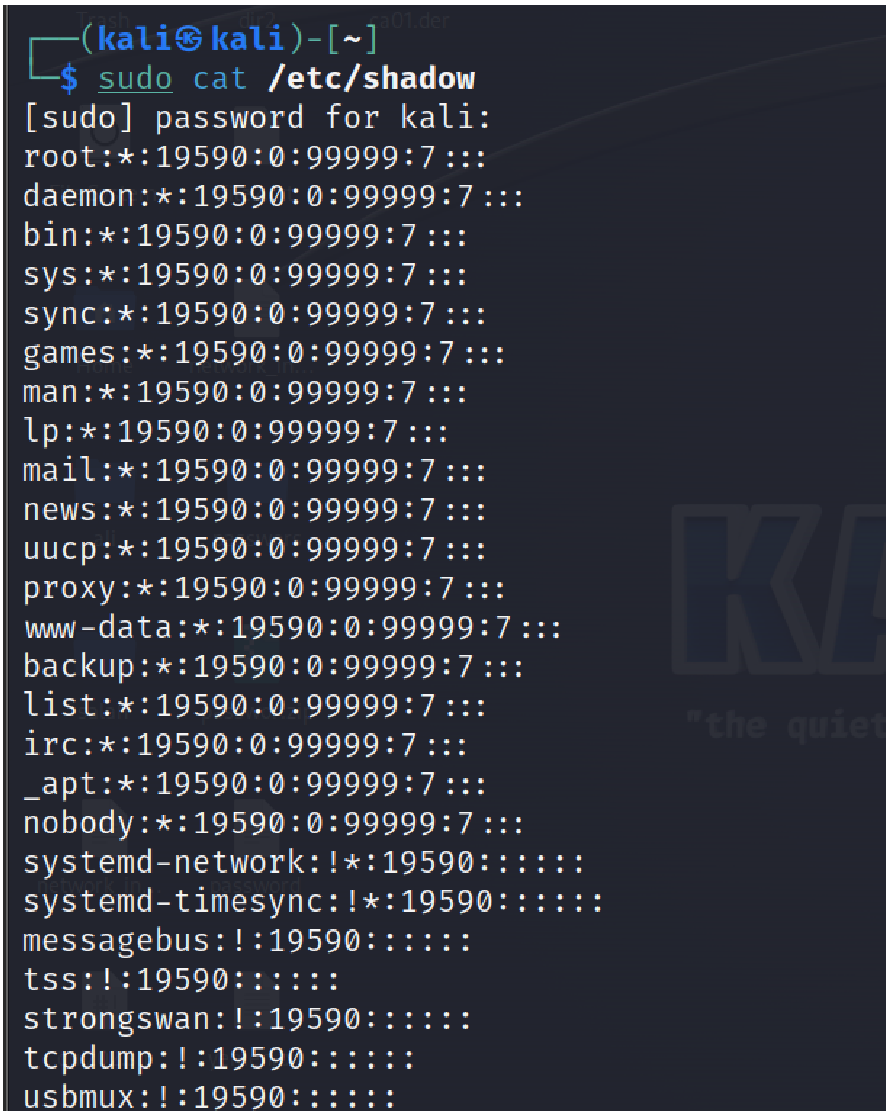


```
┌──(kali㉿kali)-[~]
└─$ rm -r testdire

┌──(kali㉿kali)-[~]
└─$ ls -i
2491010 backup_testfile.txt  2490413 Documents  2490414 Music        2490412 Public     2490448 work
2490409 Desktop              2490410 Downloads  2490550 newfile.txt  2490411 Templates
2493564 dir1                 2490577 fakecall   2490415 Pictures     2490416 Videos
```

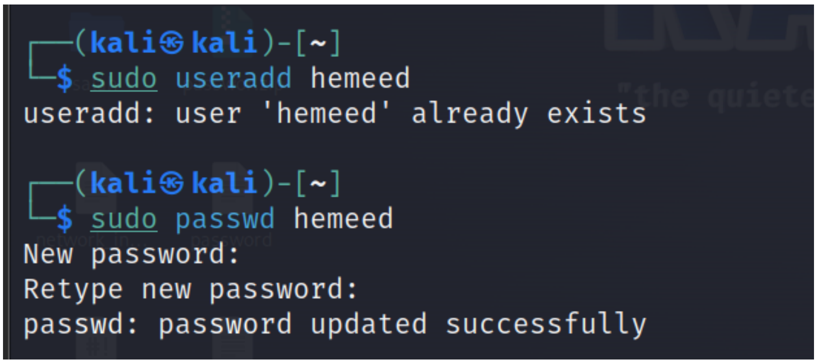
Section 4: User and Group Management:

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



```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
[sudo] password for kali:
root:*:19590:0:99999:7:::
daemon:*:19590:0:99999:7:::
bin:*:19590:0:99999:7:::
sys:*:19590:0:99999:7:::
sync:*:19590:0:99999:7:::
games:*:19590:0:99999:7:::
man:*:19590:0:99999:7:::
lp:*:19590:0:99999:7:::
mail:*:19590:0:99999:7:::
news:*:19590:0:99999:7:::
uucp:*:19590:0:99999:7:::
proxy:*:19590:0:99999:7:::
www-data:*:19590:0:99999:7:::
backup:*:19590:0:99999:7:::
list:*:19590:0:99999:7:::
irc:*:19590:0:99999:7:::
_apt:*:19590:0:99999:7:::
nobody:*:19590:0:99999:7:::
systemd-network:!*:19590::::::
systemd-timesync:!*:19590::::::
messagebus:!:19590::::::
tss:!:19590::::::
strongswan:!:19590::::::
tcpdump:!:19590::::::
usbmux:!:19590::::::
```

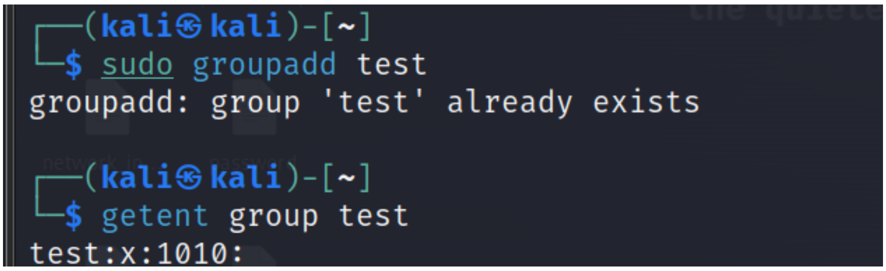
17. **Write the command to create a new user with the username `Hemeed`:**



```
┌──(kali㉿kali)-[~]
└─$ sudo useradd hemeed
useradd: user 'hemeed' already exists

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

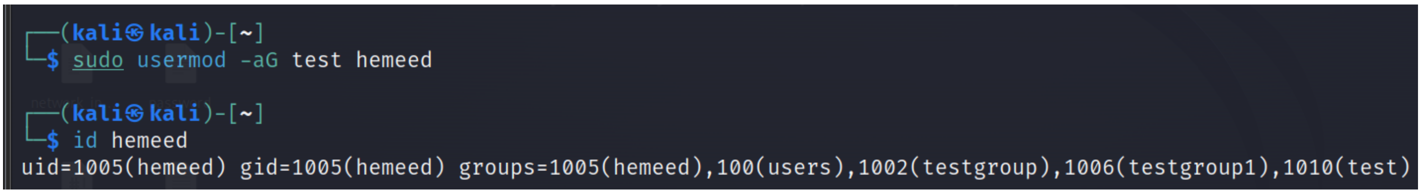
18. **How do you create a new group named `test`?**



```
┌──(kali㉿kali)-[~]
└─$ sudo groupadd test
groupadd: group 'test' already exists

┌──(kali㉿kali)-[~]
└─$ getent group test
test:x:1010:
```

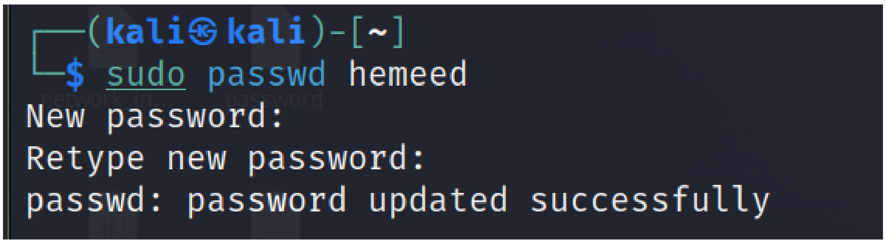
19. **Write the command to add the user `hemeed` to the group `test`.**



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

┌──(kali㉿kali)-[~]
└─$ id hemeed
uid=1005(hemeed) gid=1005(hemeed) groups=1005(hemeed),100(users),1002(testgroup),1006(testgroup1),1010(test)
```

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



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

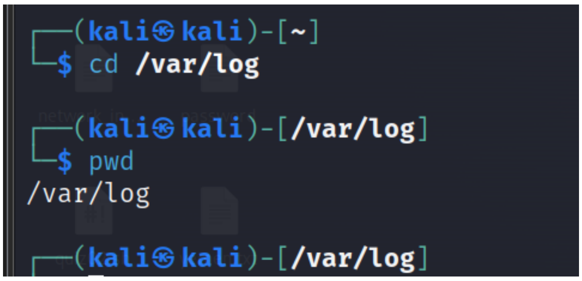
Section 5: Practical Application:

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`?

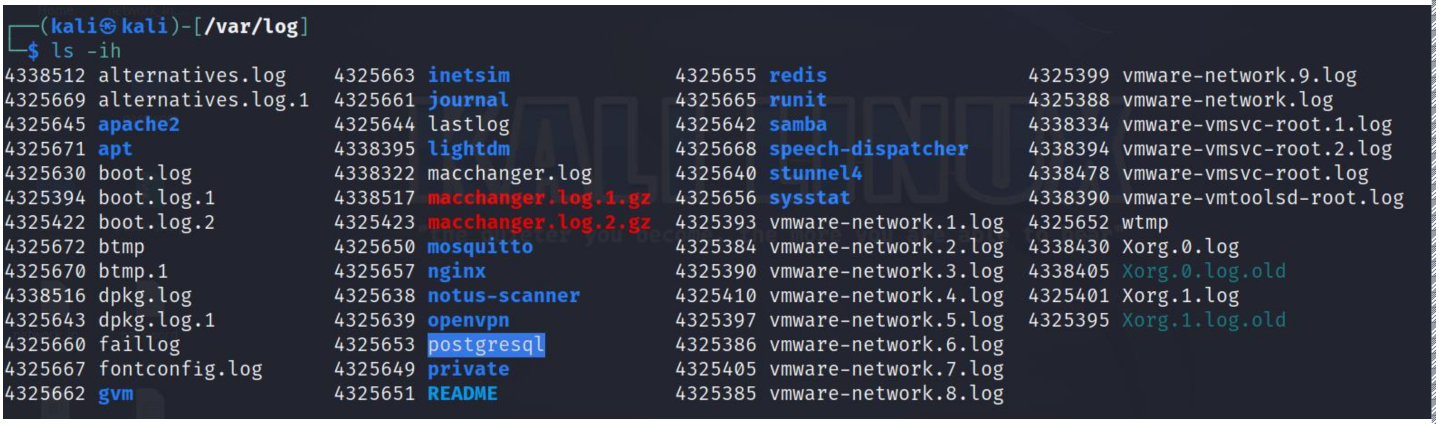


```
┌──(kali㉿kali)-[~]
└─$ cd /var/log

┌──(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?



```
┌──(kali㉿kali)-[/var/log]
└─$ ls -ih
4338512 alternatives.log    4325663 inetsim             4325655 redis                4325399 vmware-network.9.log
4325669 alternatives.log.1  4325661 journal             4325665 runit                4325388 vmware-network.log
4325645 apache2             4325644 lastlog             4325642 samba                4338334 vmware-vmsvc-root.1.log
4325671 apt                 4338395 lightdm             4325668 speech-dispatcher    4338394 vmware-vmsvc-root.2.log
4325630 boot.log            4338322 macchanger.log      4325640 stunnel4             4338478 vmware-vmsvc-root.log
4325394 boot.log.1          4338517 macchanger.log.1.gz 4325656 sysstat              4338390 vmware-vmtoolsd-root.log
4325422 boot.log.2          4325423 macchanger.log.2.gz 4325393 vmware-network.1.log 4325652 wtmp
4325672 btmp                4325650 mosquitto           4325384 vmware-network.2.log 4338430 Xorg.0.log
4325670 btmp.1              4325657 nginx               4325390 vmware-network.3.log 4338405 Xorg.0.log.old
4338516 dpkg.log            4325638 notus-scanner       4325410 vmware-network.4.log 4325401 Xorg.1.log
4325643 dpkg.log.1          4325639 openvpn             4325397 vmware-network.5.log 4325395 Xorg.1.log.old
4325660 faillog             4325653 postgresql          4325386 vmware-network.6.log
4325667 fontconfig.log      4325649 private             4325405 vmware-network.7.log
4325662 gvm                 4325651 README              4325385 vmware-network.8.log
```

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
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 .