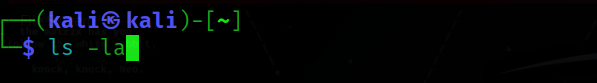
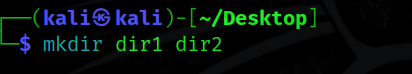
Mid Exam

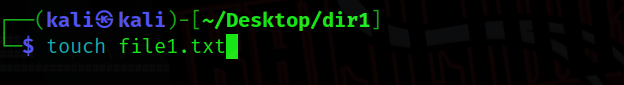
Section 1: File and Directory Management

1. Display the current working directory.

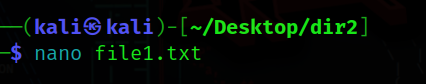
2. List all the contents of your current directory, including hidden files.

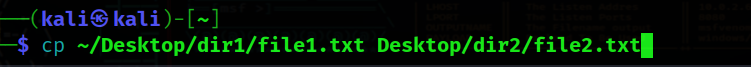
3. Change your directory to the `Desktop`.

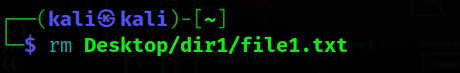
4. Create two directories named `dir1` and `dir2` on the Desktop.

5. Inside `dir1`, create a file named `file1.txt`.

6. Inside `dir2`, create a file named `file2.txt`.

7. Using nano or vim Write the numbers 1 to 9 into `file1.txt`.

8. From the home directory Copy the contents of `file1.txt` into `file2.txt`.

9. From the home directory, delete `file1.txt` inside `dir1`.

11. Redirect the output of the network configuration command to a file named `network\_info.txt` on the Desktop.

12. Open the Desktop folder and show all files with detailed information.

Section 2: Users and Groups Management

13. Create a new user with your name.



14. Set a password for your user.



15. Open the file that contains user information and verify that your user has been added.



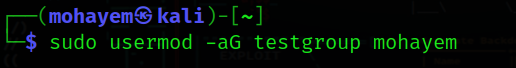
16. Add your user to the file that gives administrative privileges.

17. Switch to your user and confirm the user identity.

18. Create a new group named `testgroup`.



19. Add your user to `testgroup`.



20. Add the group `testgroup` to the file that gives administrative privileges.



21. Remove your user from the file that gives administrative privileges.



22. Check if your user still have administrative privileges.



23. Check which groups your user belongs to.



Section 3: Permissions and Ownership

24. Set the permissions of `file2.txt` on the Desktop to allow the owner to read, write, and execute; the group to read and execute; and others to read

 .

25. Check the permissions of `file2.txt` to verify the change

.

26. Change the ownership of `file2.txt` to your user.

27. verify the ownership of `file2.txt

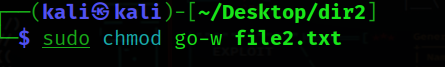
`.

28. Change back the ownership of a file `file2.txt` .

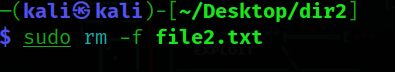
29. Grant write permission to everyone for `file2.txt`.



30. Remove the write permission for the group and others for `file2.txt`.



31. Delete `file2.txt` after making the necessary ownership and permission changes.



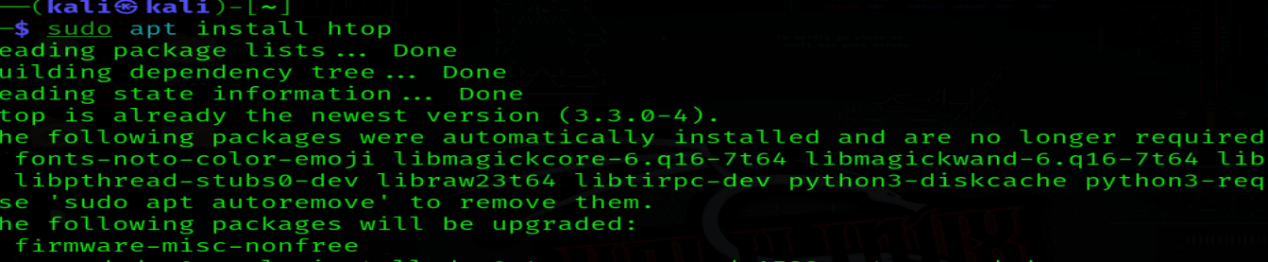
32. What command would you use to recursively change the permissions of all files and directories inside

a folder named `project` to `755`

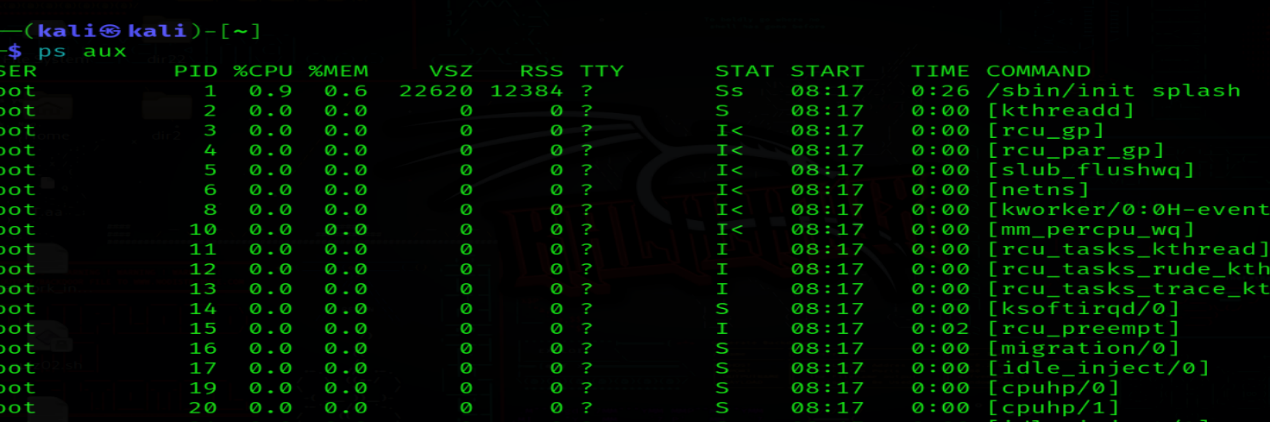
.

Section 4: Process Management

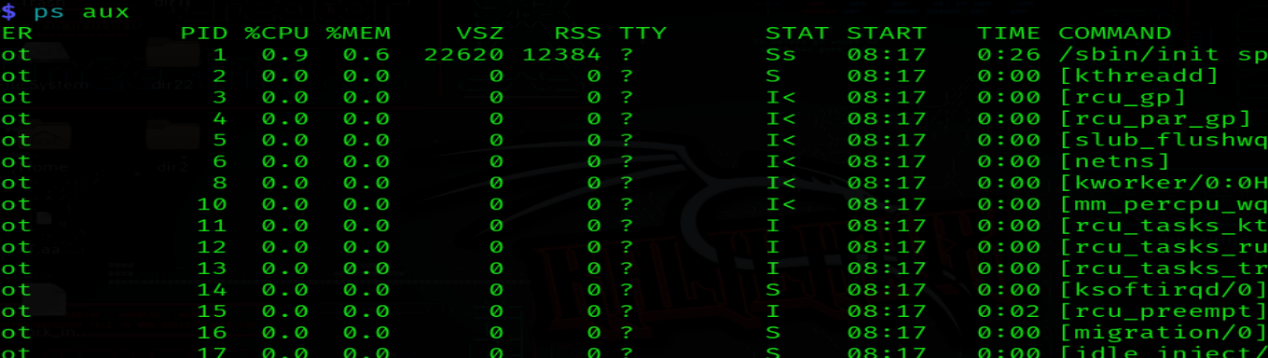
33. Install a system monitor tool that provides an interactive process viewer(htop)

.

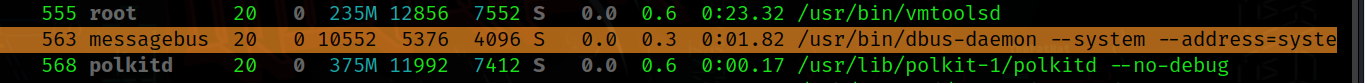
34. Display all running processes.



35. Display a tree of all running processes.

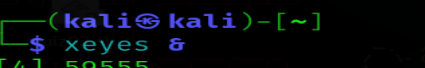


36. Open the interactive process viewer and identify a process by its PID.



37. Kill a process with a specific PID.

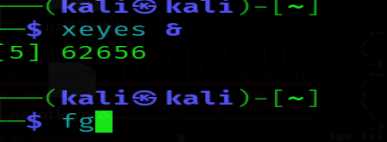
38. Start an application and stop it using a command that kills processes by name(exeyes).



39. Restart the application, then stop it using the interactive process viewer.



40. Run a command in the background, then bring it to the foreground(exeyes).



41. Check how long the system has been running.

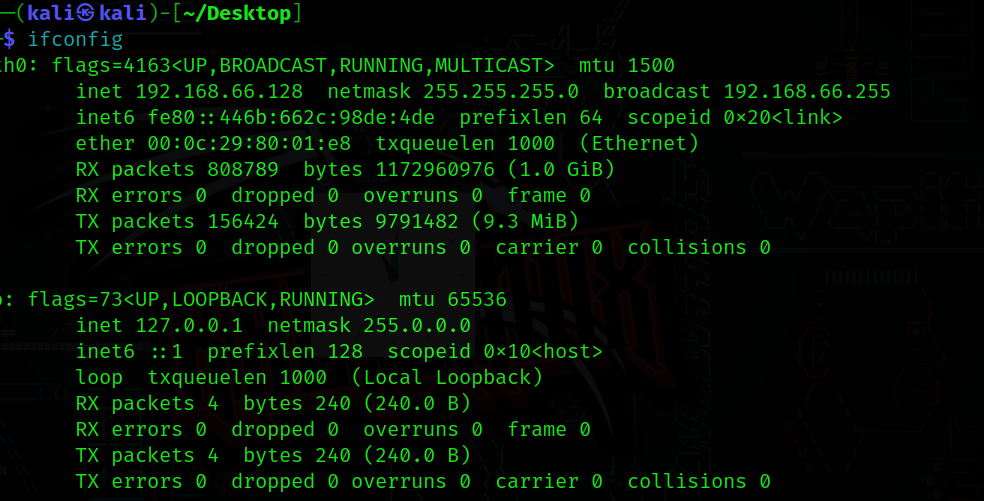


42. List all jobs running in the background.

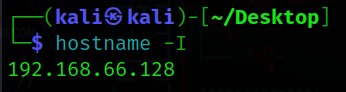


Section 5: Networking Commands

43. Display the network configuration

.

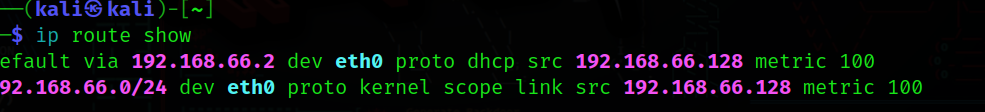
44. Check the IP address of your machine

.

45. Test connectivity to an external server.



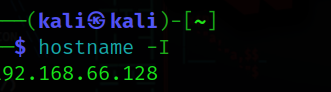
46. Display the routing table.

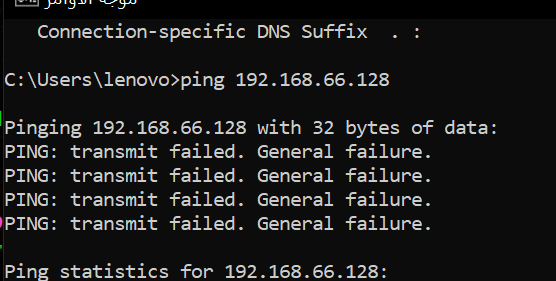


47. Check the open ports and active connections.



48. Show the IP address of the host machine and the VM, and verify if they are on the same network.

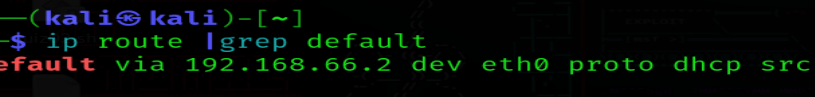




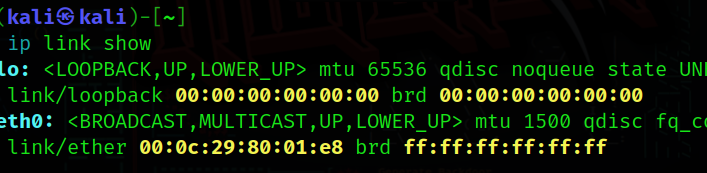
49. Trace the route to an external server.



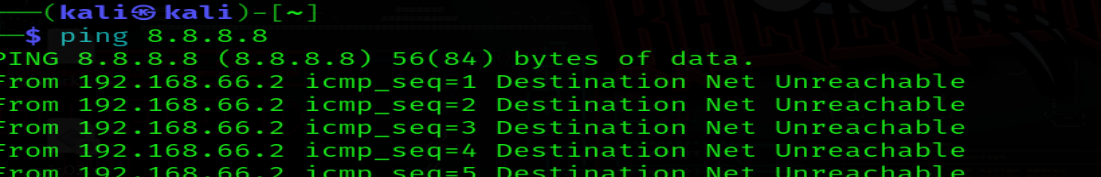
50. Find out the default gateway.



51. Check the MAC address of your network interface.

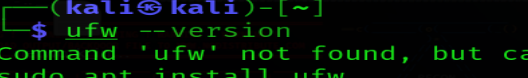


52. Ensure that the VM can access external networks.



Section 6: UFW Firewall

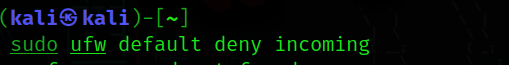
53. Enable the firewall.



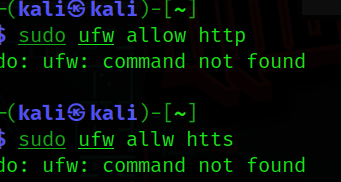
54. Allow SSH connections through the firewall

.

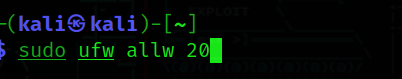
55. Deny all incoming traffic by default.



56. Allow HTTP and HTTPS traffic.



57. Allow port 20



58. Reset the firewall settings.



59. Delete a rule from the firewall.



60. Disable the firewall.



61. View the status of the firewall.



62. Log firewall activity and view it.

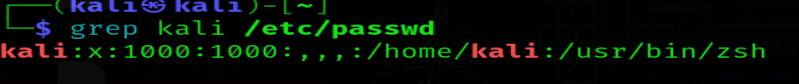


Section 7: Searching and System Information

63. Delete the command history.



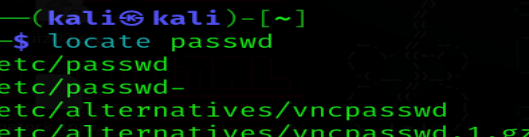
64. Search for a kali in the `/etc/passwd` file.



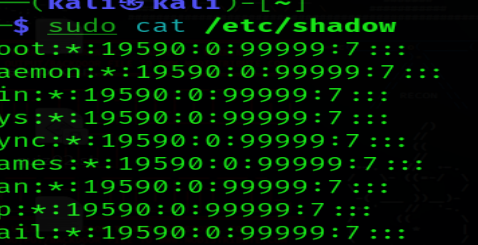
65. Search for a kali in the `/etc/group` file.



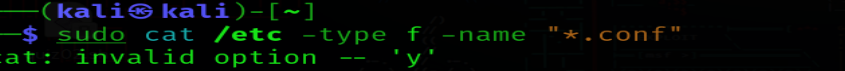
66. Locate the `passwd` file.



67. Locate the shadow file and open it.



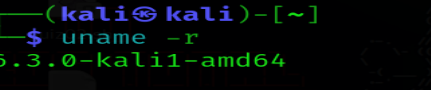
68. Search for all configuration files in the `/etc` directory.



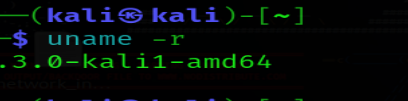
69. Search recursively for a specific word in the `/var/log` directory.



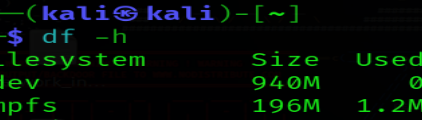
70. View the system’s kernel version.



71. Display the system’s memory usage.



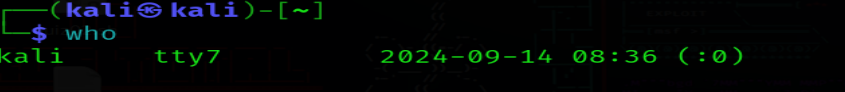
72. Show the system’s disk usage.



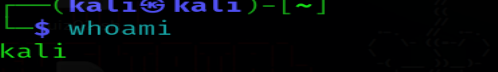
73. Check the system's uptime and load average.



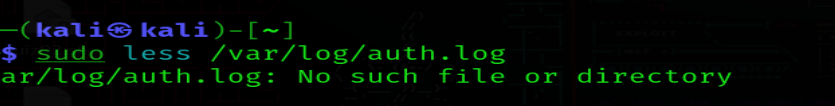
74. Display the current logged-in users.



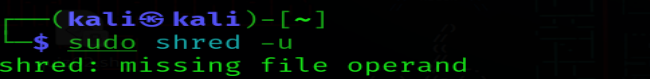
75. Check the identity of the current user.



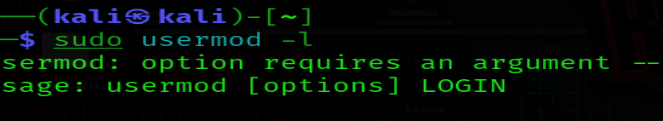
76. View the `/var/log/auth.log` file.



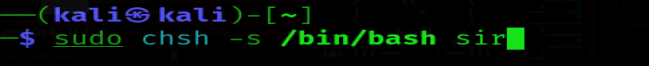
77. Shred the `auth.log` file securely.



78. How do you lock a user account to prevent them from logging in.



79. What command would you use to change a user's default shell.



80. Display the system's boot messages.

