**Task 2: Kali Linux – Hands on**

1. **Objective:**

Practice Linux commands from basic to Advanced levels, install Kali Linux tools from GitHub, and perform a specific attack using one of the tools.

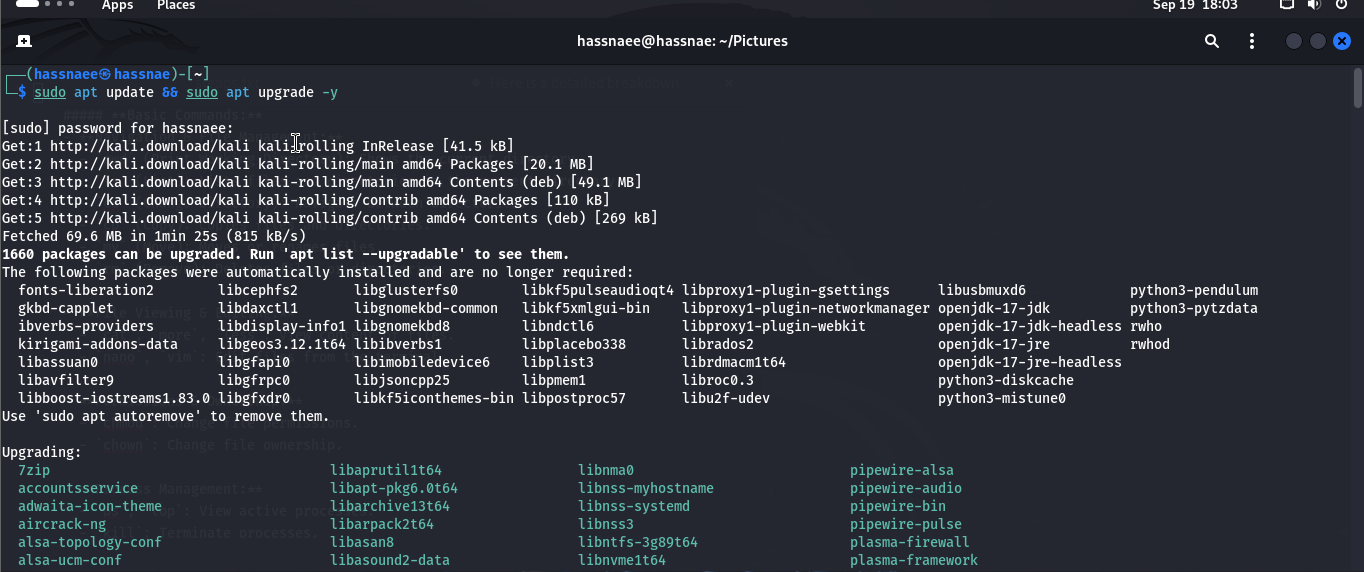
**Steps to Complete the Task:**

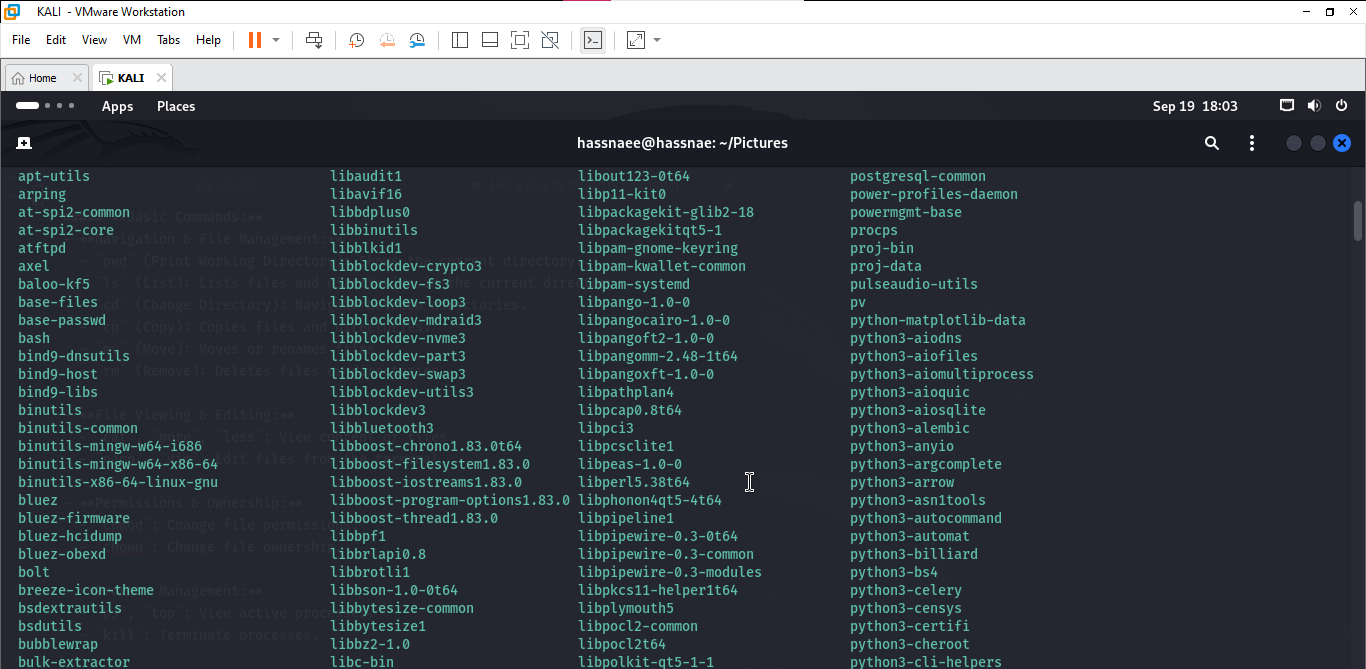
**1. Install Kali Linux:**

* Download the Kali Linux ISO from the official website: **Kali Linux Download.**
* Install Kali Linux either on a physical machine, in a virtual environment (using VMware or VirtualBox), or as a dual boot with another OS.

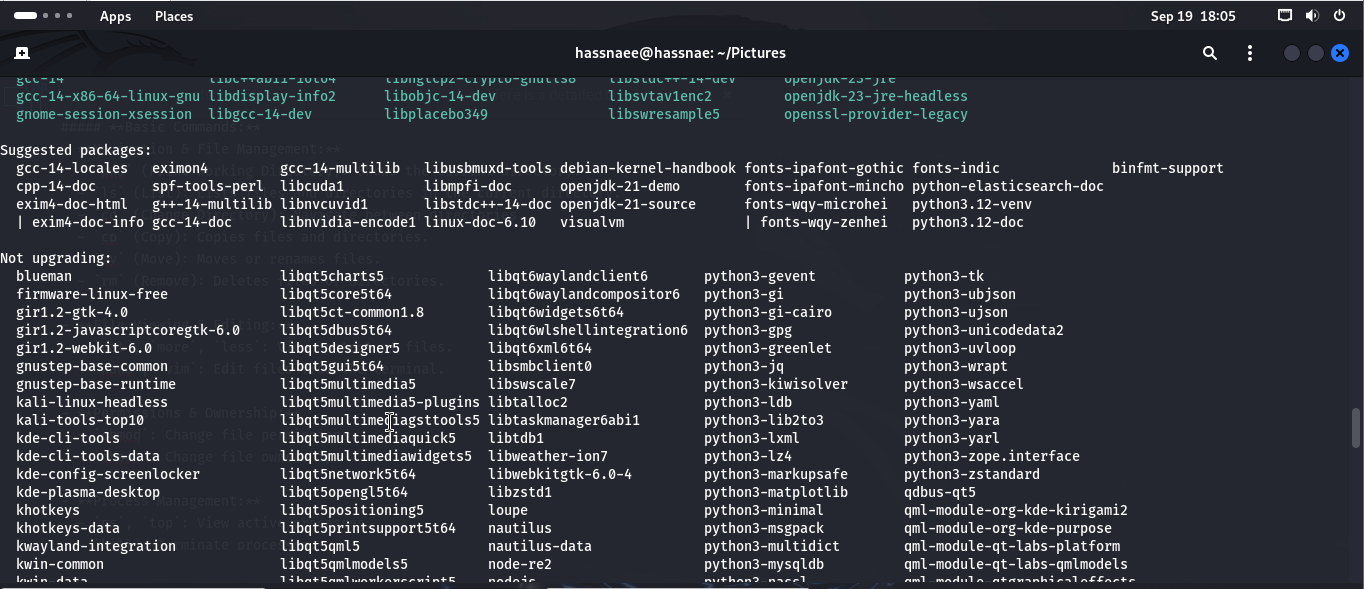
**##(**this steps is already done)

**After installation, we need to make sure to update the system by running:**

** sudo apt update && sudo apt upgrade -y**









**2. Practice Basic to Advanced Linux Commands:**

We start by familiarizing with essential Linux commands. Here are categories of commands that we should practice:

**Basic Commands:**

* **Navigation & File Management:**
  + pwd (Print Working Directory): Shows the current directory.
  + ls (List): Lists files and directories in the current directory.
  + cd (Change Directory): Navigate between directories.
  + cp (Copy): Copies files and directories.
  + mv (Move): Moves or renames files.
  + rm (Remove): Deletes files or directories.
* **File Viewing & Editing:**
  + cat, more, less: View content of files.
  + nano, vim: Edit files from the terminal.
* **Permissions & Ownership:**
  + Chmod: Change file permissions.
  + Chown: Change file ownership.
* **Process Management:**
  + ps, top: View active processes.
  + Kill: Terminate processes.

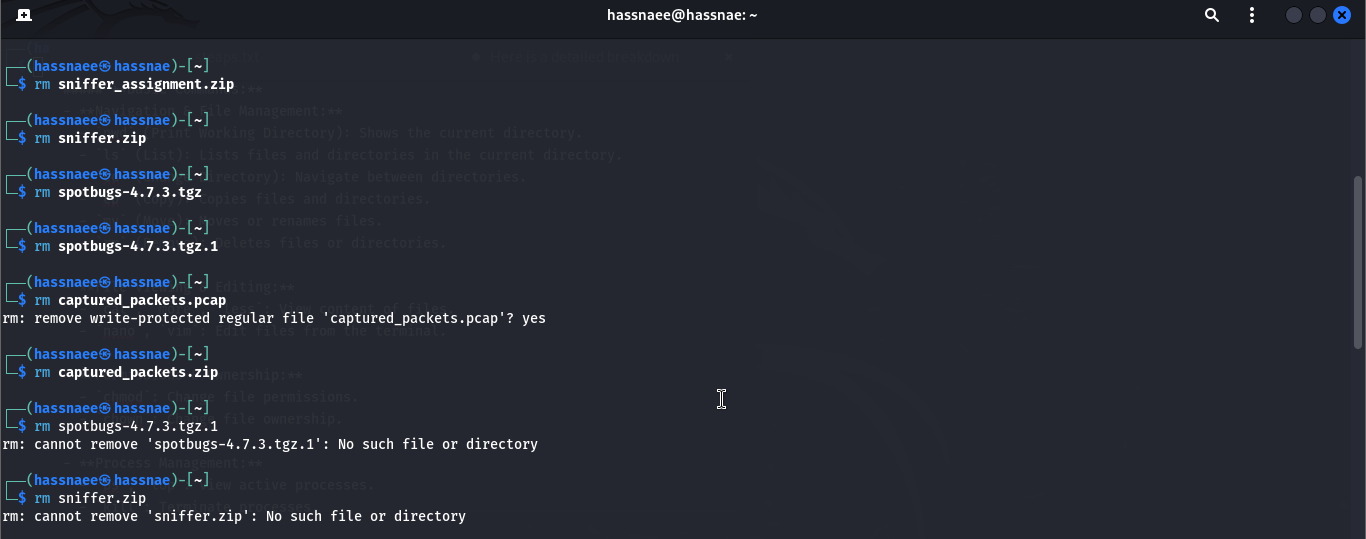
**Intermediate Commands:**

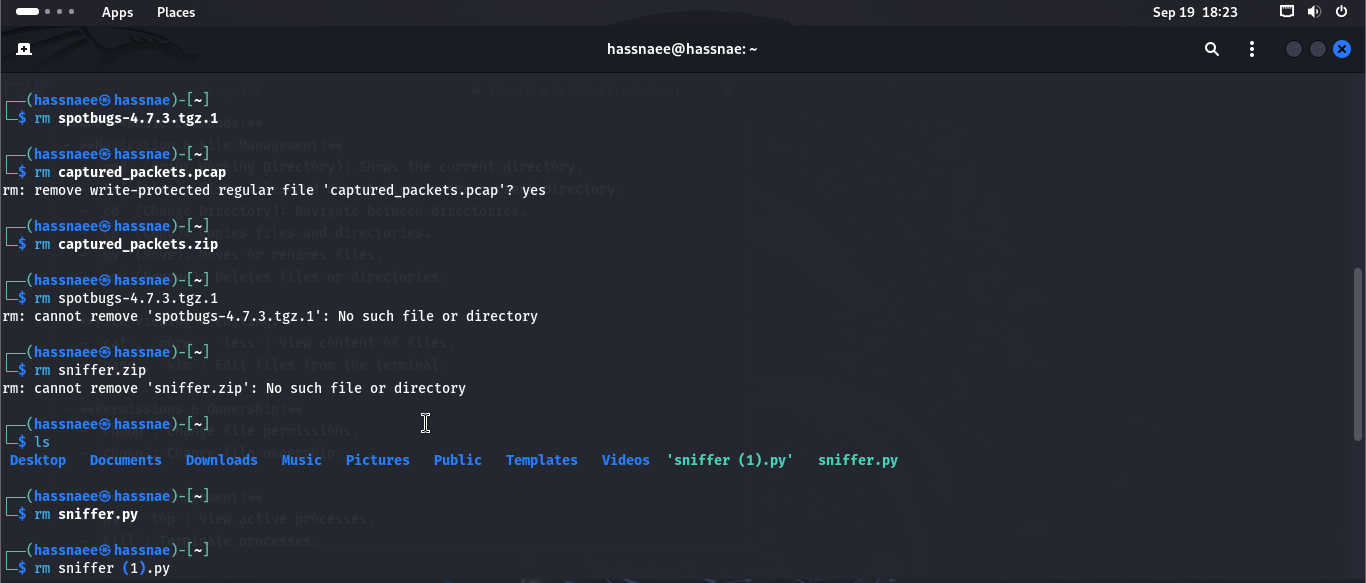
* **Networking:**
  + ifconfig or ip a: Check network configuration.
  + ping: Test network connectivity.
  + netstat: Check open ports and network connections.
* **System Information:**
  + df -h: Check disk space usage.
  + free -h: Check memory usage.
  + uname -a: View system information.
* **Archiving & Compression:**
  + tar, gzip, gunzip: Archive and compress files.

**Advanced Commands:**

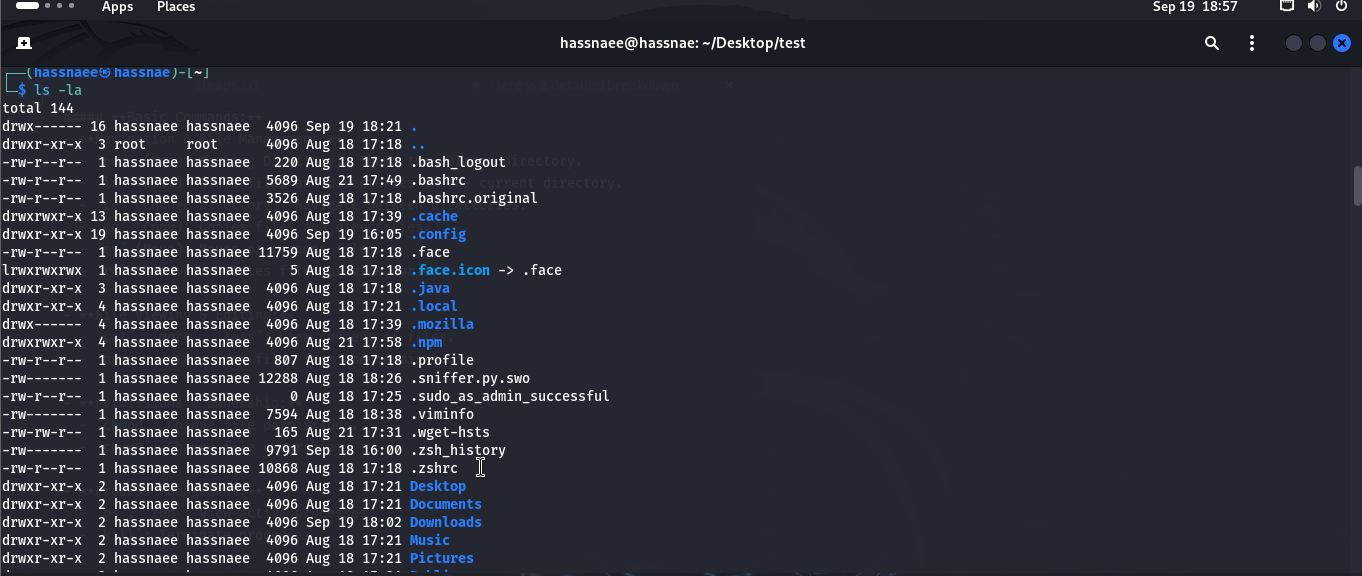
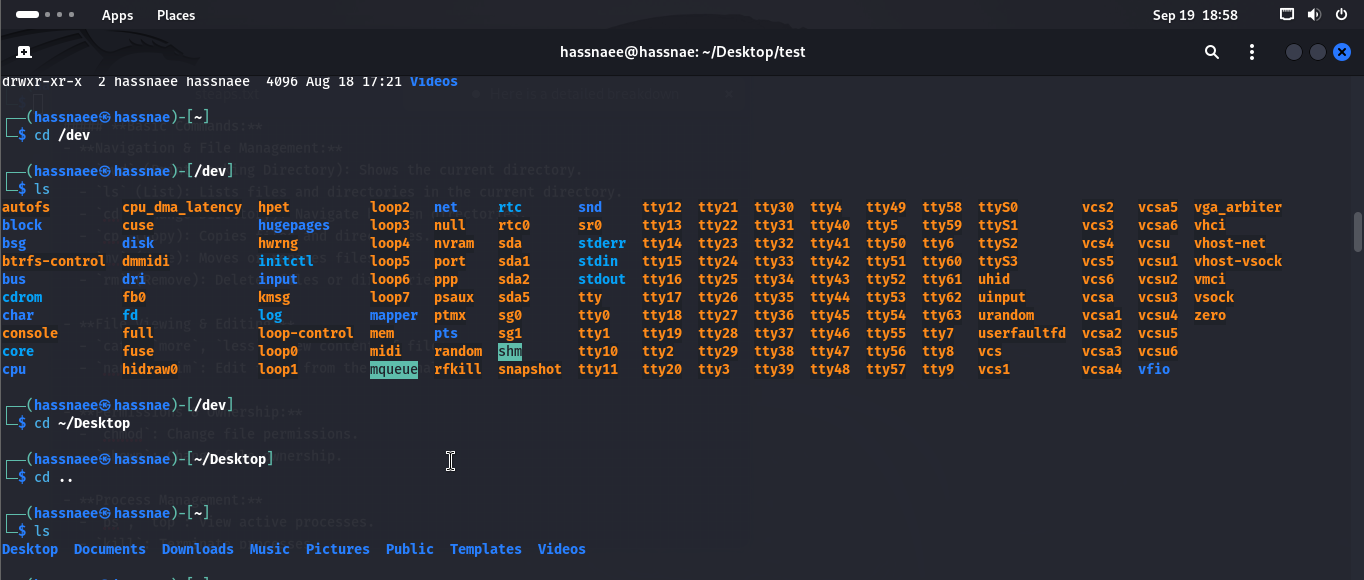
* **Scripting:**
  + Write and execute simple shell scripts (.sh).
* **Firewall & Security:**
  + ufw: Manage the firewall.
  + iptables: Advanced network traffic control.
* **User Management:**
  + useradd, passwd, usermod, userdel: Manage users.
  + groupadd, groupdel, gpasswd: Manage groups.



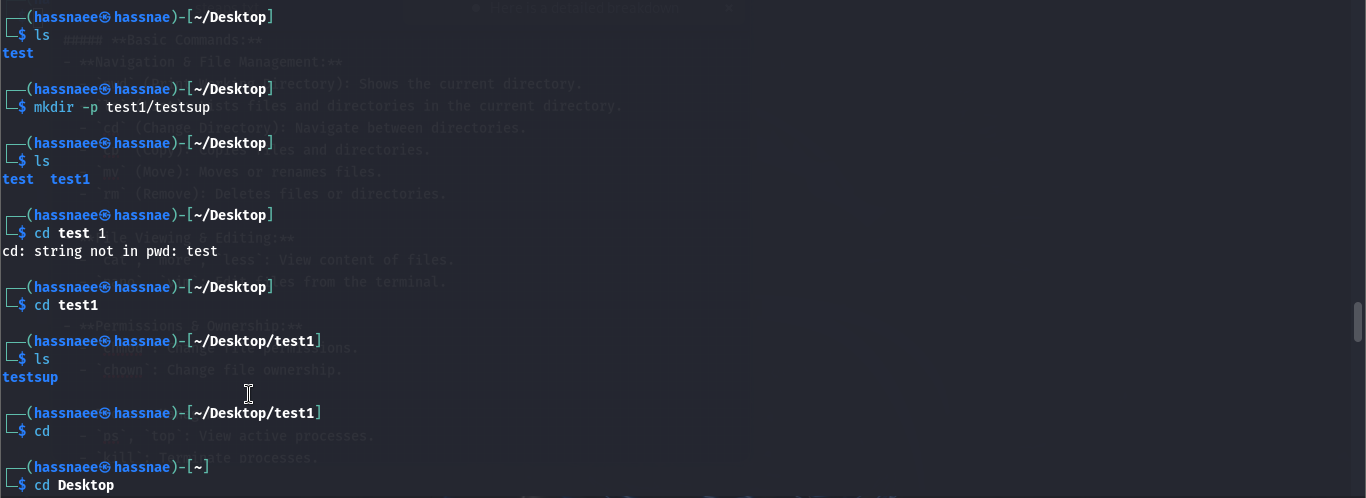


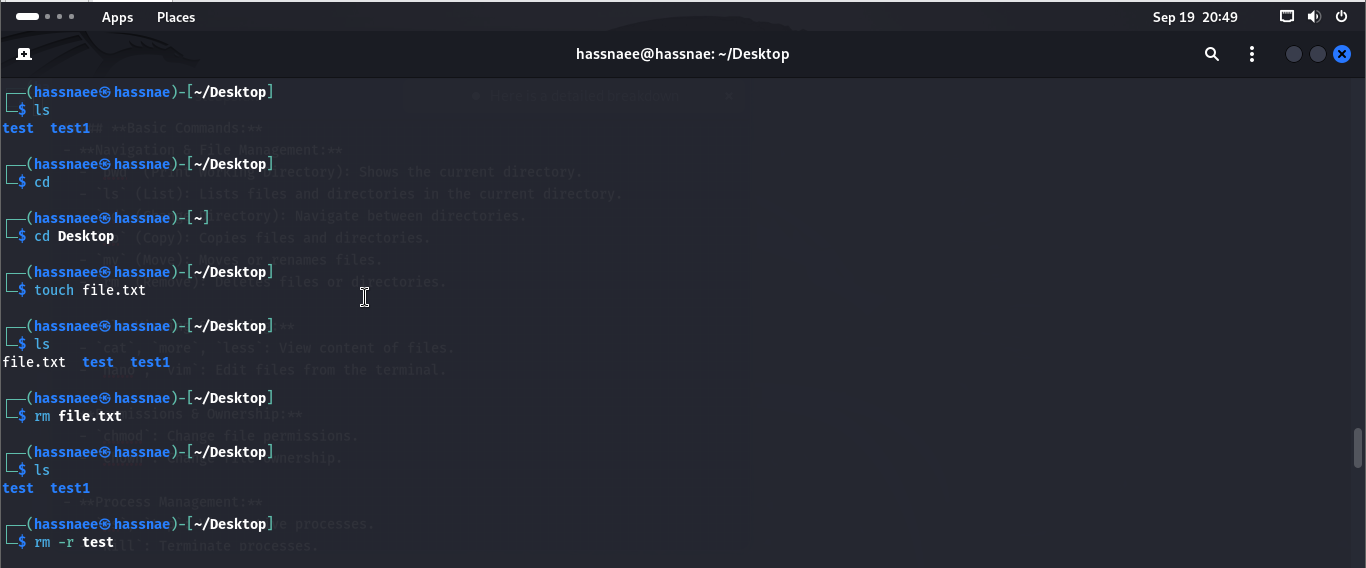


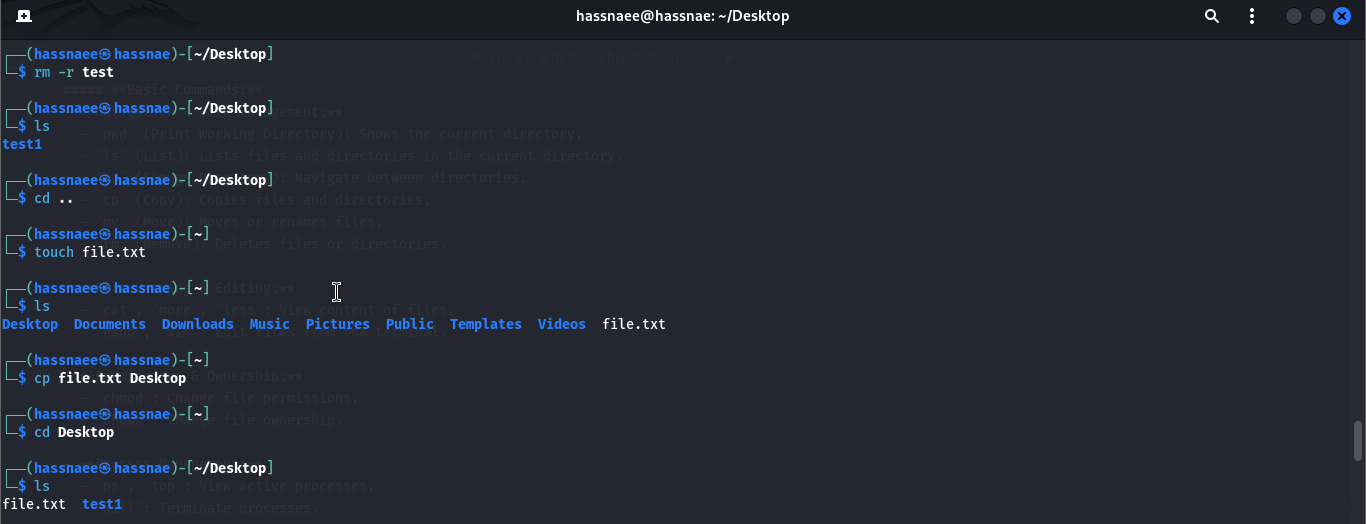


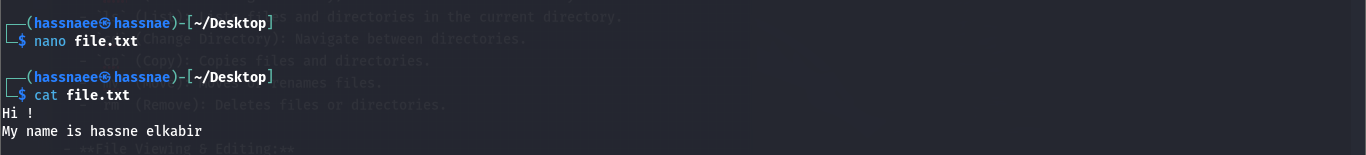


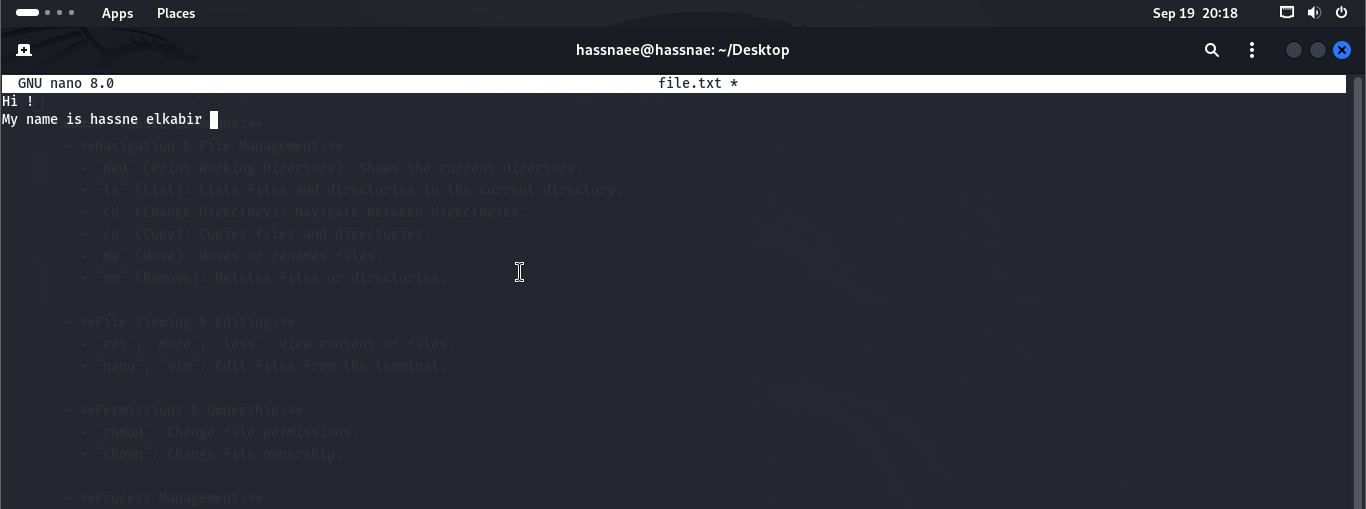


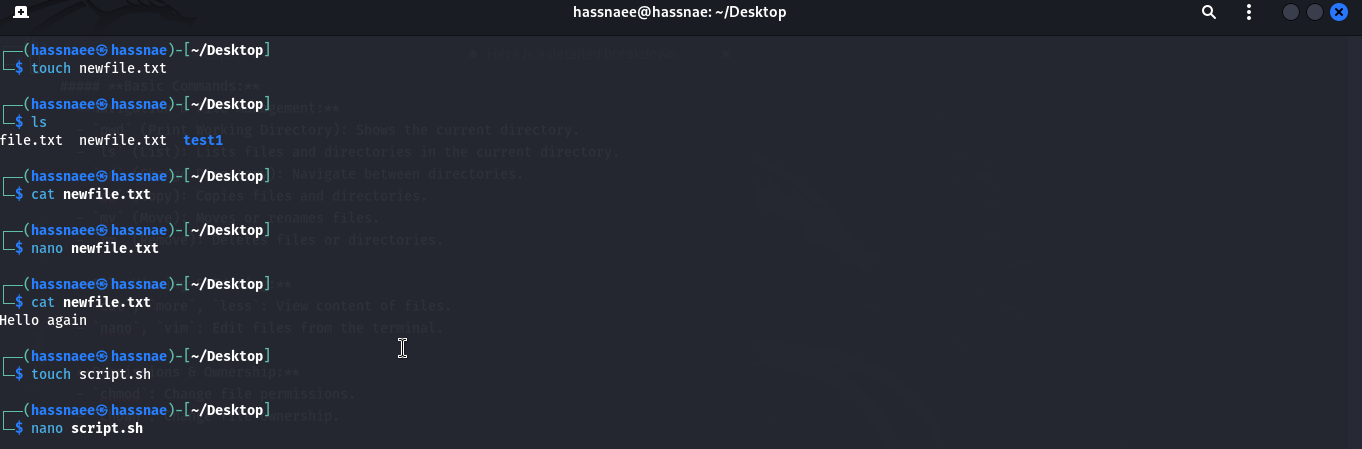




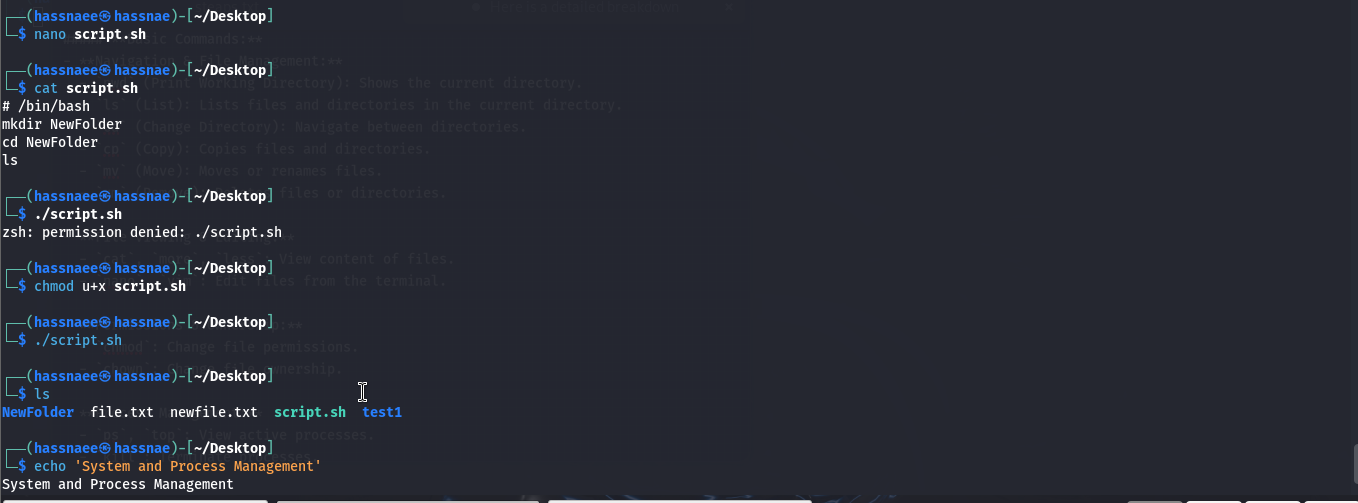


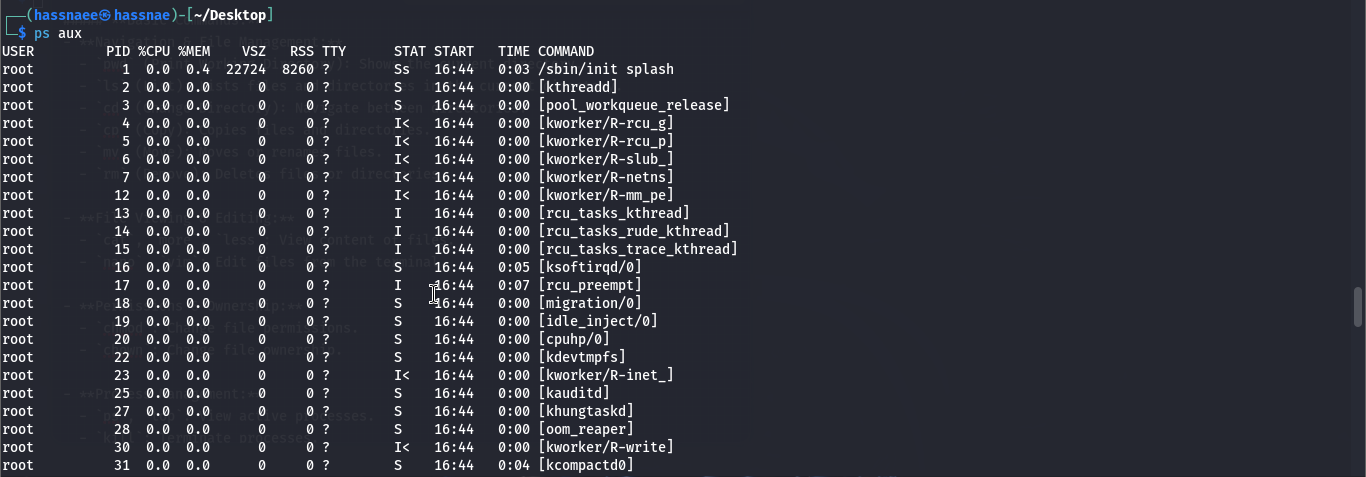


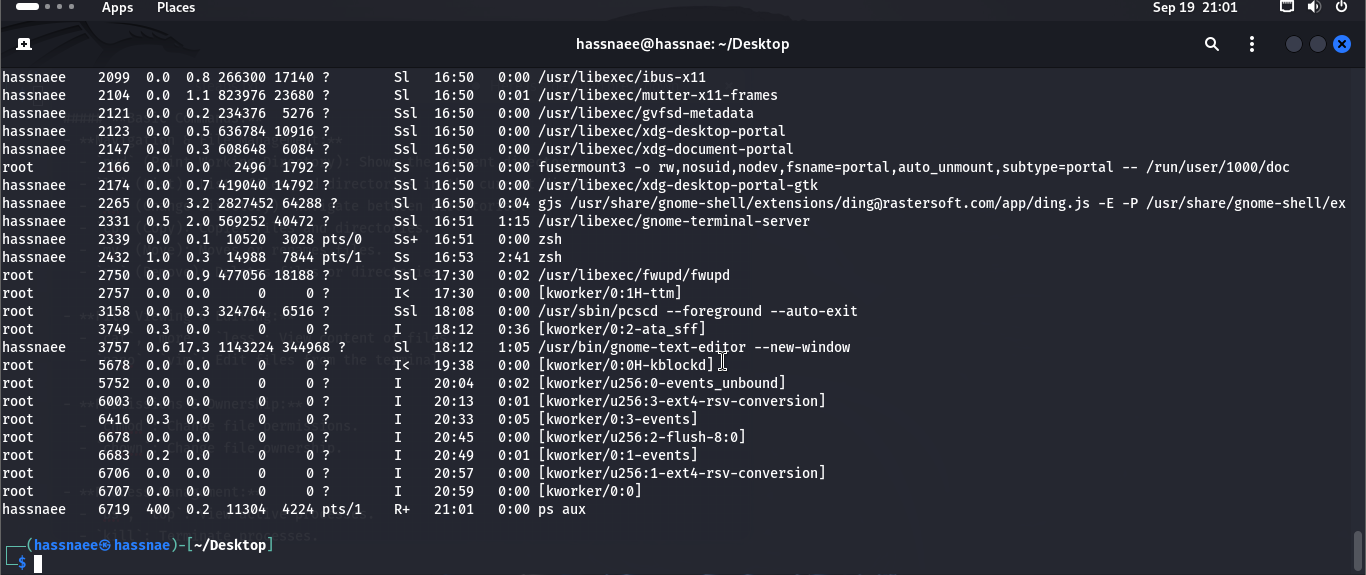


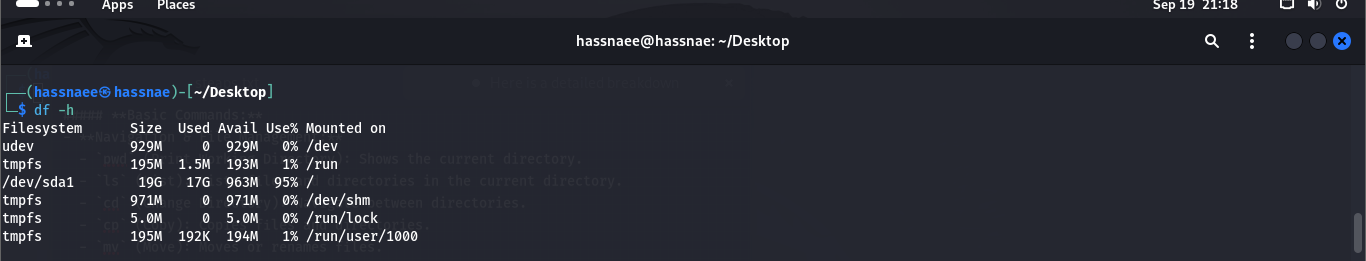


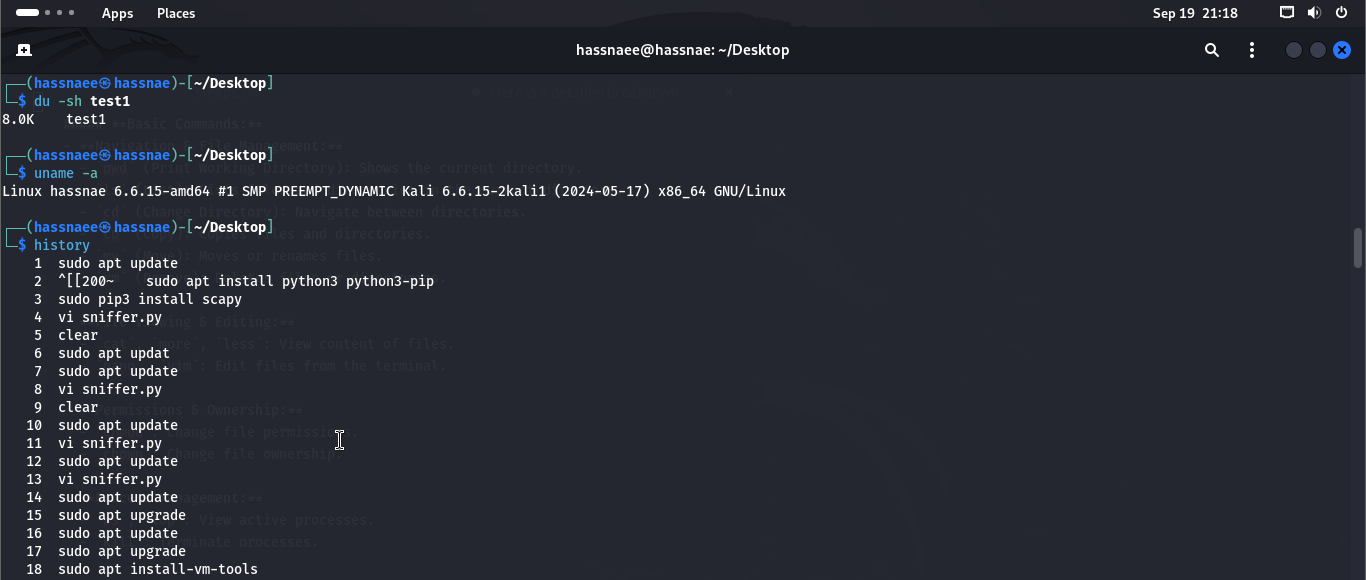




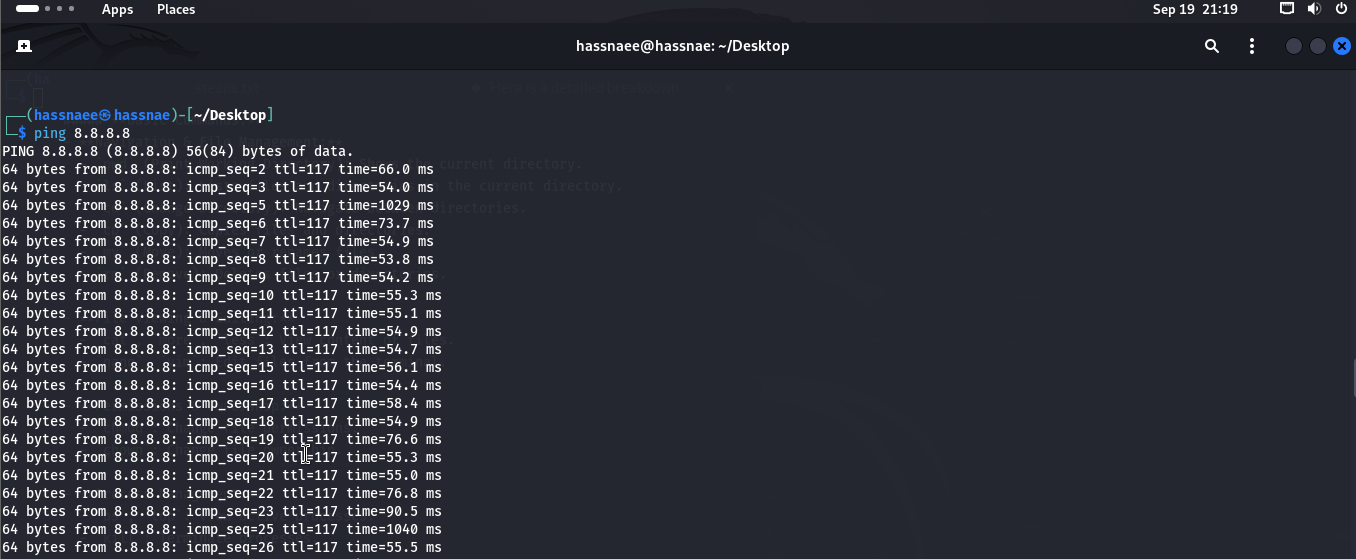


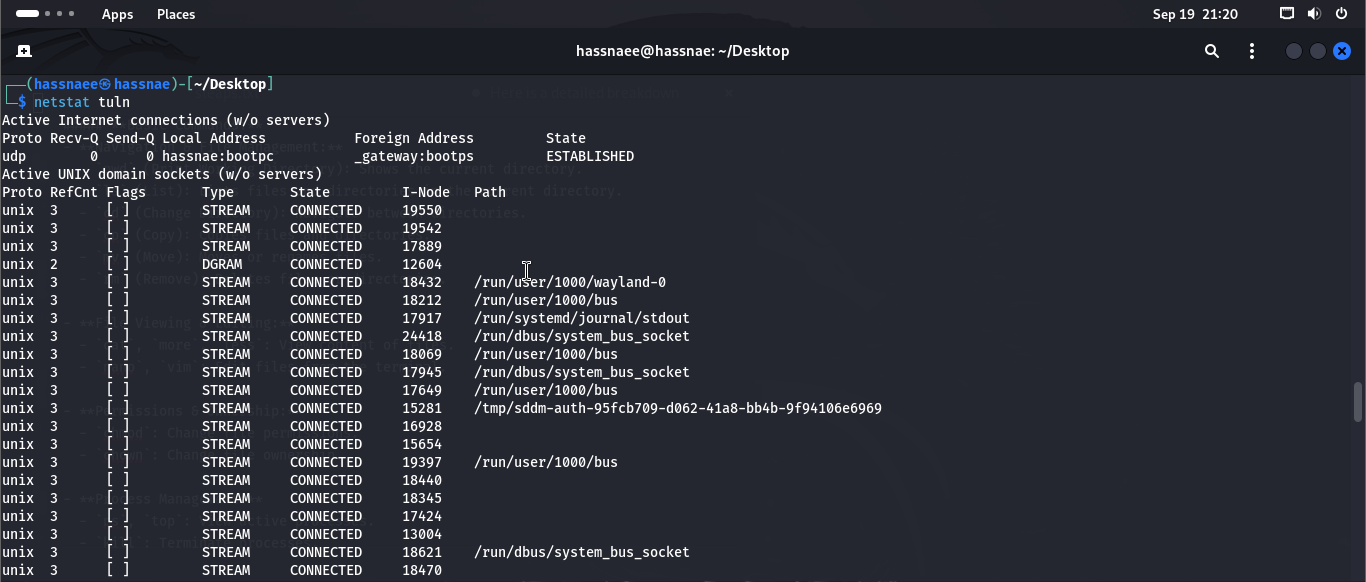


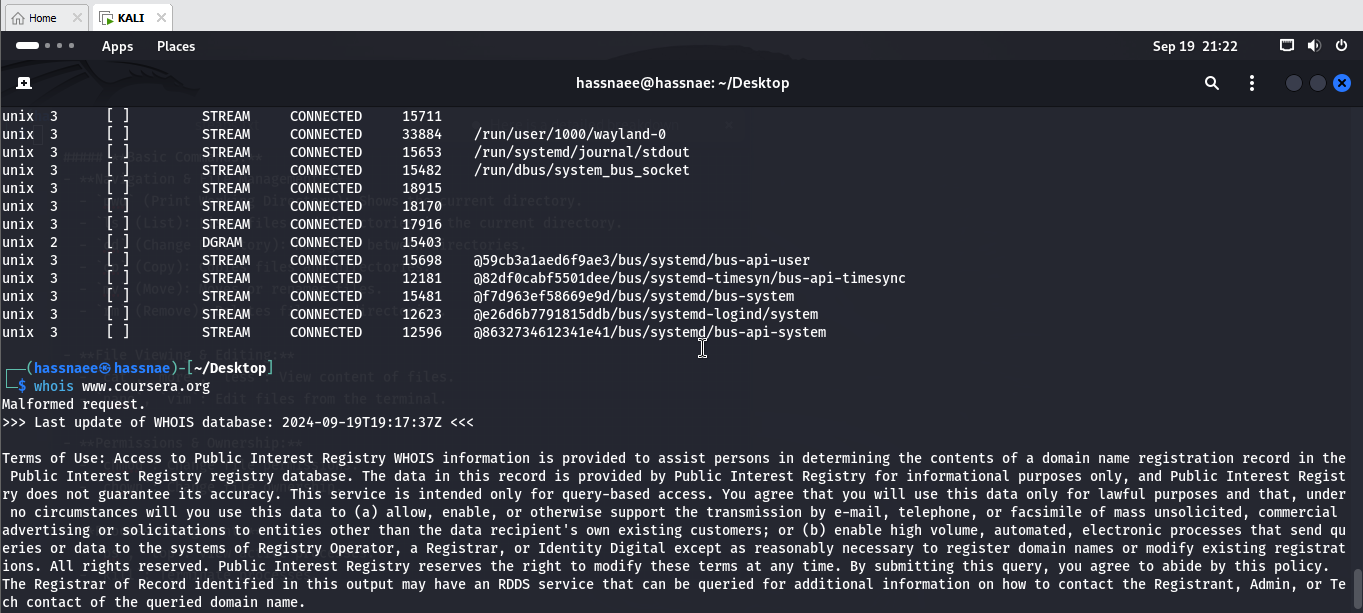


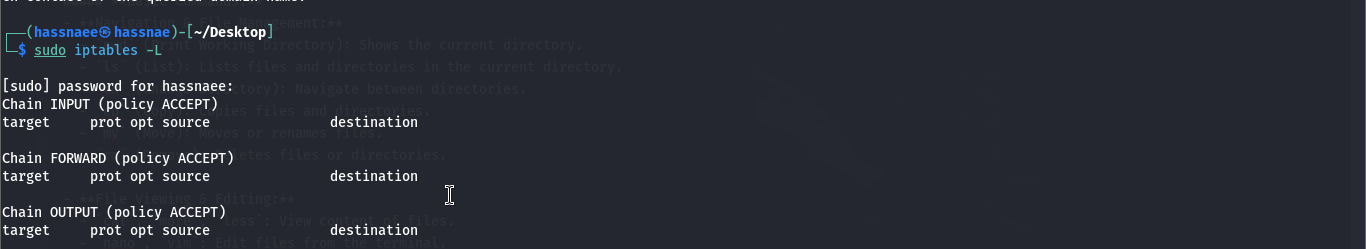












**3. Install Kali Linux Tools from GitHub:**

We can install various hacking tools from GitHub on Kali Linux. Here's how you can do it :

* Search for a tool on GitHub, for example, a network scanner or password cracker.

Let's use nmap (network scanning tool) as an example:

**Steps:**

**Clone the repository**:

In this example, SQLmap was cloned using this command:

**git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git**

This downloaded the SQLmap tool onto the desktop.

**Navigate to the tool directory**:

Use the cd command to move to the directory:

**cd sqlmap**

**Run the tool**:

To run SQLmap, we need to execute the following:

**python sqlmap.py**

**Perform a test scan**:

Test with a vulnerable URL:

**sqlmap -u http://testphp.vulnweb.com/login.php --dbs**

This will initiate SQLmap to scan for databases on the target site.



