Dated: 25 January,2024
SHUBHANKAR SHARMA 102118021 COBS1

Information Security

Lab Assignment 2

“Ipconfig and ifconfig(linux) commands used to see the IP’s connect to Operating System”
“Ipconfig /all”

Private IP Address:
A private IP address is an address used within a private network, such as a local area network (LAN) or an internal network within an organization. These addresses are not routable on the public internet and are reserved for use within private networks to facilitate communication between devices within the same network. Private IP addresses are defined by RFC 1918 and include the following ranges:
- 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

These addresses are commonly used for devices like computers, printers, routers, and other networked devices within a local network environment.

Public IP Address:
A public IP address is an address that is globally routable on the public internet. It uniquely identifies a device or network on the internet, allowing communication between devices across different networks. Public IP addresses are assigned by Internet Service Providers (ISPs) or network administrators and are used to access resources and services on the internet. These addresses are typically visible to other devices on the internet and can be used to communicate with servers, websites, and other internet-connected devices.

Public IP addresses can be static or dynamic. Static public IP addresses remain the same over time, while dynamic public IP addresses may change periodically, especially for residential internet connections.

When you access a website, for example, your device communicates with the website's server using your public IP address, enabling data exchange between your device and the server over the internet.

(It’s for our device)
A **gateway** in networking is a device or software component that acts as an entry and exit point between two different networks, allowing them to communicate with each other. Here's a simple breakdown:

Function: The gateway facilitates communication between devices on different networks by forwarding data packets between them.

Types:
- Default Gateway: This is the gateway through which devices on a local network connect to devices on external networks, such as the internet. It typically has an IP address assigned within the local network.

- Router: A common example of a gateway is a router, which connects a local network to the internet. It manages traffic between devices within the local network and devices on the internet.
- Firewall: Gateways can also include firewall functionality, providing security by filtering incoming and outgoing traffic based on predefined rules.
- Proxy Server: In some cases, a gateway can be a proxy server that acts as an intermediary between clients and servers, caching and filtering web content.

IP Address: Gateways have their own IP address, which is used by devices on the local network to send data outside the network.

Routing: Gateways use routing tables to determine the best path for forwarding data packets to their intended destinations. They may employ protocols such as IP routing (for IPv4) or ICMPv6 routing (for IPv6) to manage routing decisions.

In summary, a gateway serves as a bridge between different networks, enabling communication and traffic management between them.

Registry.in - Domain naim registration
Google Public DNS Server IP - 8.8.8.8
If i want to change the server then
Nslookup
> server 8.8.8.8
> website name

- **DNCP server provides IP to Machines**
- **Lease Expired and Lease Time**
- **DNS Server translates domain names to IP address (DNS Client is available to all devices)**
- **A MAC (Media Access Control) address, also known as a hardware or physical address, is a unique identifier assigned to network interfaces for communication on a network.**

1. Security Concepts

Security and OS Hardening:

Security: In the realm of computing, security refers to measures taken to protect systems, data, and networks from unauthorized access, misuse, or damage. It encompasses various techniques, protocols, policies, and tools designed to ensure confidentiality, integrity, and availability of resources.

OS Hardening: OS hardening involves implementing security measures to reduce the vulnerability of an operating system (OS) by eliminating potential attack vectors, minimizing the system's exposure to threats, and enhancing its resistance to unauthorized access and exploitation.

Differentiation between Windows and Linux OS Architecture:

Windows OS: Windows is a proprietary operating system developed by Microsoft. Its architecture is primarily based on a monolithic kernel design, where the kernel provides extensive services and runs in kernel mode, handling system calls, memory management, and hardware interactions directly.

Linux OS: Linux, on the other hand, is an open-source operating system kernel developed by Linus Torvalds and a large community of contributors. Linux follows a modular design with a monolithic kernel at its core but allows for dynamic loading and unloading of kernel modules. It also supports various kernel architectures, making it highly customizable and adaptable to different hardware platforms.

Importance of Linux Security:

- Linux is widely used in servers, embedded systems, and critical infrastructure due to its stability, performance, and open-source nature.
- Many internet-facing services and websites are hosted on Linux servers, making them prime targets for cyber attacks.
- As an open-source platform, Linux benefits from rapid security patching and community-driven development, but this also means vulnerabilities are quickly disclosed, requiring proactive security measures.
- Securing Linux systems is crucial to protect sensitive data, ensure uninterrupted service availability, and safeguard against cyber threats such as malware, ransomware, and unauthorized access.

Types of Security Breach:

1. Unauthorized Access: This occurs when an attacker gains entry to a system or network without proper authorization, often through exploiting vulnerabilities or using stolen credentials.

2. Data Breach: A data breach involves unauthorized access, disclosure, or theft of sensitive or confidential information, such as personal data, financial records, or intellectual property.

3. Malware Infection: Malware, including viruses, worms, trojans, and ransomware, can compromise system security by infecting and manipulating files, stealing data, or disrupting normal operations.

4. Denial of Service (DoS): DoS attacks aim to disrupt or disable services, applications, or networks by overwhelming them with excessive traffic, requests, or malicious packets, rendering them inaccessible to legitimate users.

5. Social Engineering: Social engineering techniques exploit human psychology to manipulate individuals into divulging confidential information, clicking on malicious links, or performing actions that compromise security.

6. Insider Threats: Insider threats involve individuals with authorized access to systems or networks intentionally or unintentionally abusing their privileges, stealing data, or sabotaging operations.

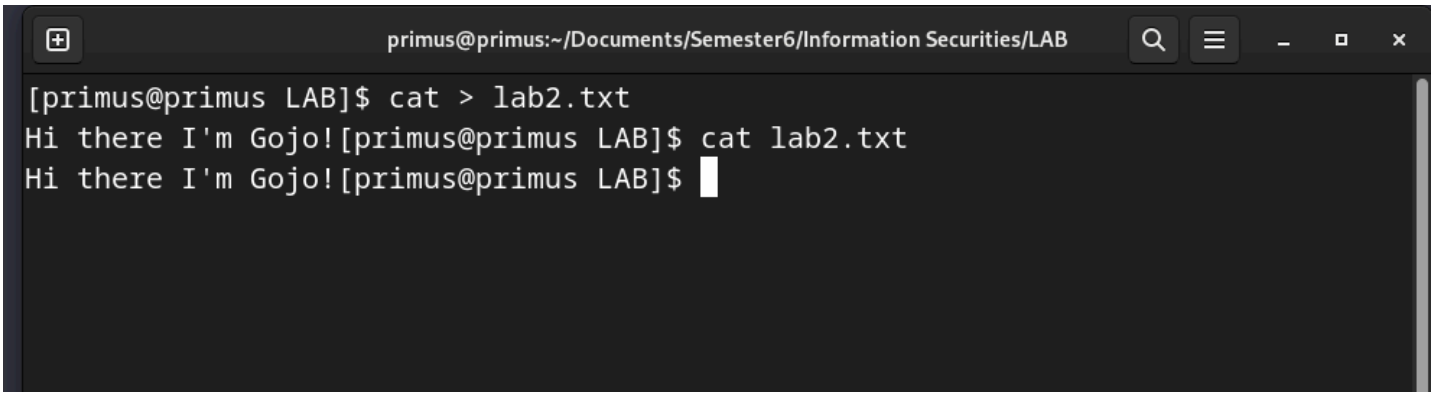
7. Phishing: Phishing attacks use deceptive emails, messages, or websites to trick users into revealing sensitive information, such as login credentials or financial details, or downloading malicious software.

2. Linux Commands

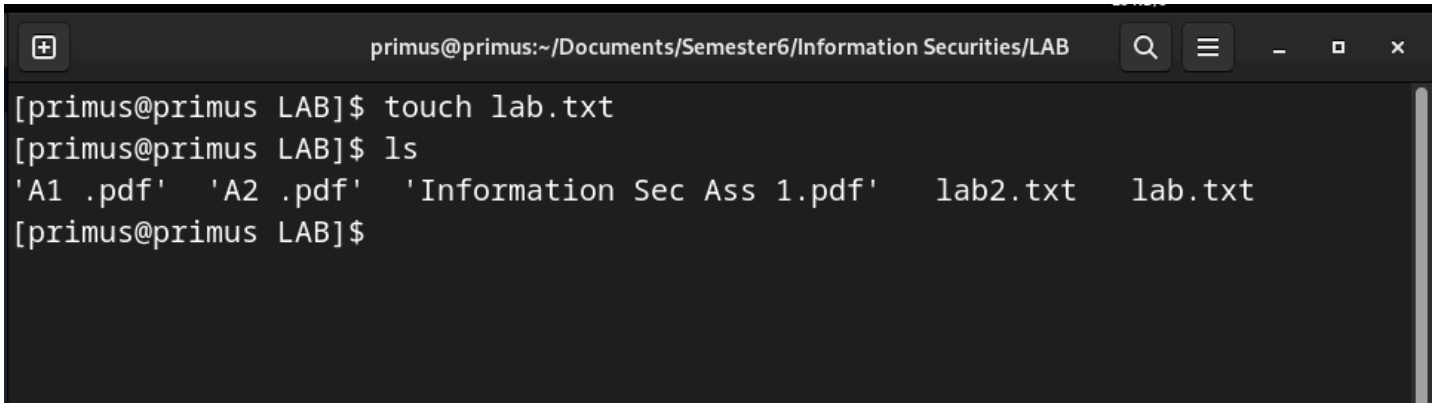
a. File Commands:

i. Creating Files:

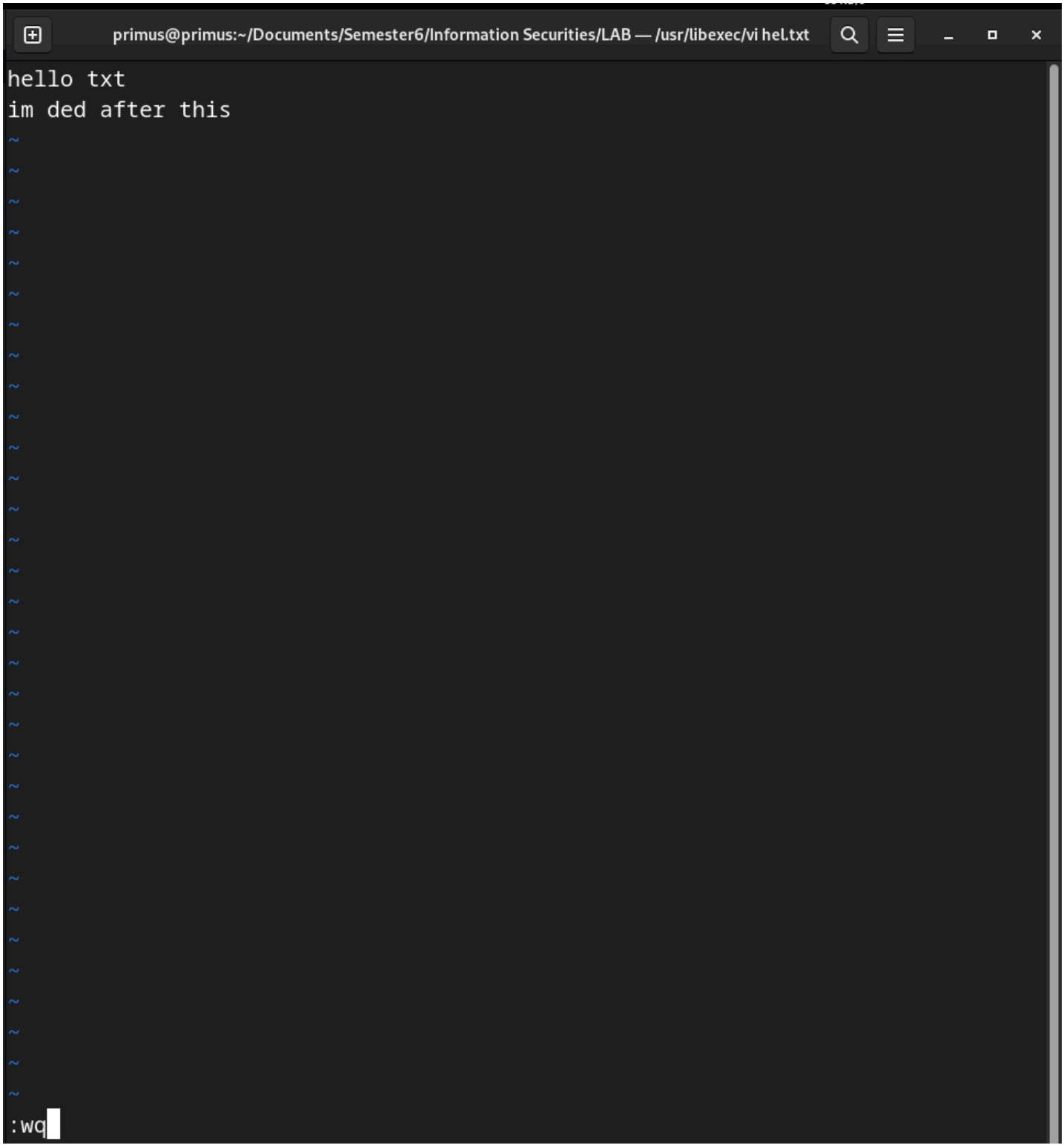
1. cat: Creates a file or concatenates files. Example: `cat > filename`

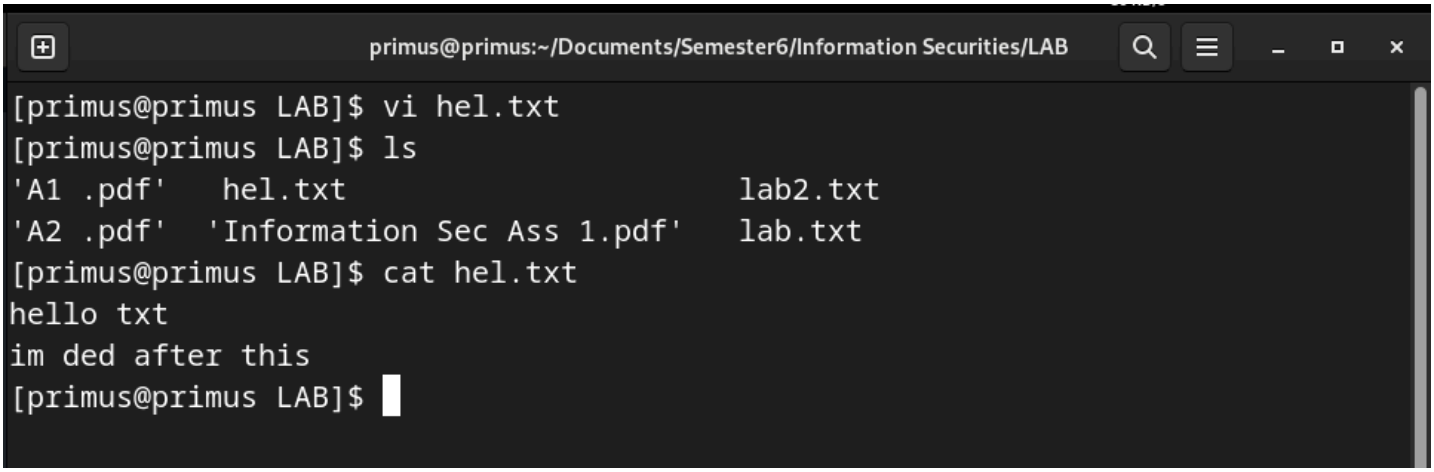


2. touch: Creates an empty file or updates the access and modification times of an existing file. Example: `touch filename`

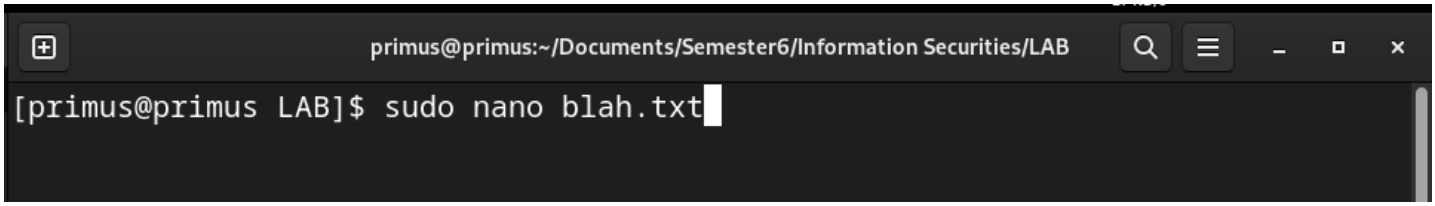


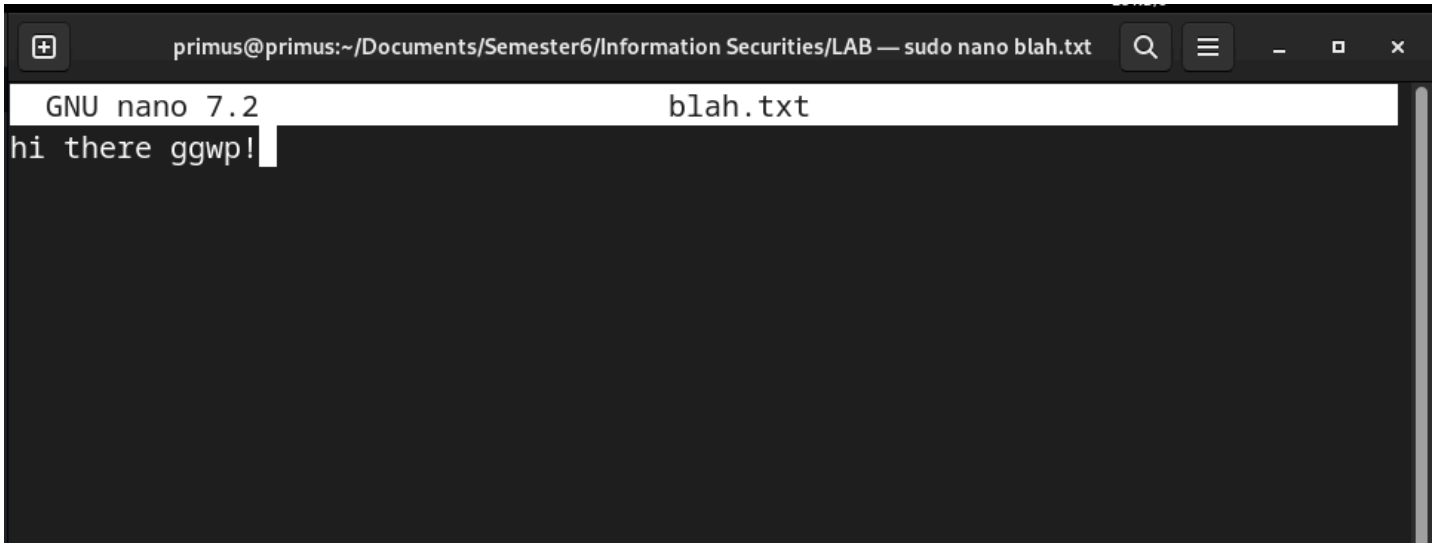
3. vi/vim: Text editors available in all Linux distributions. Example: `vi filename` or `vim filename`

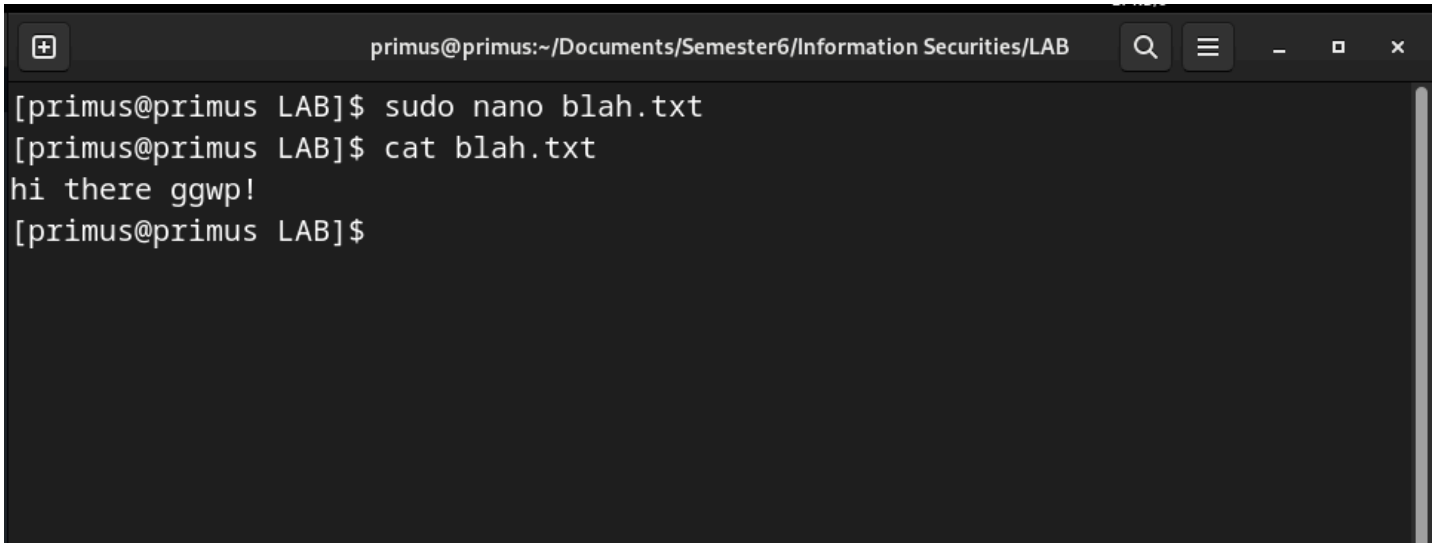

primus@primus:~/Documents/Semester6/Information Securities/LAB — /usr/libexec/vi hel.txt
hello txt
im ded after this
:wq



4. nano: A text editor not always built-in but commonly available. Example: `nano filename`

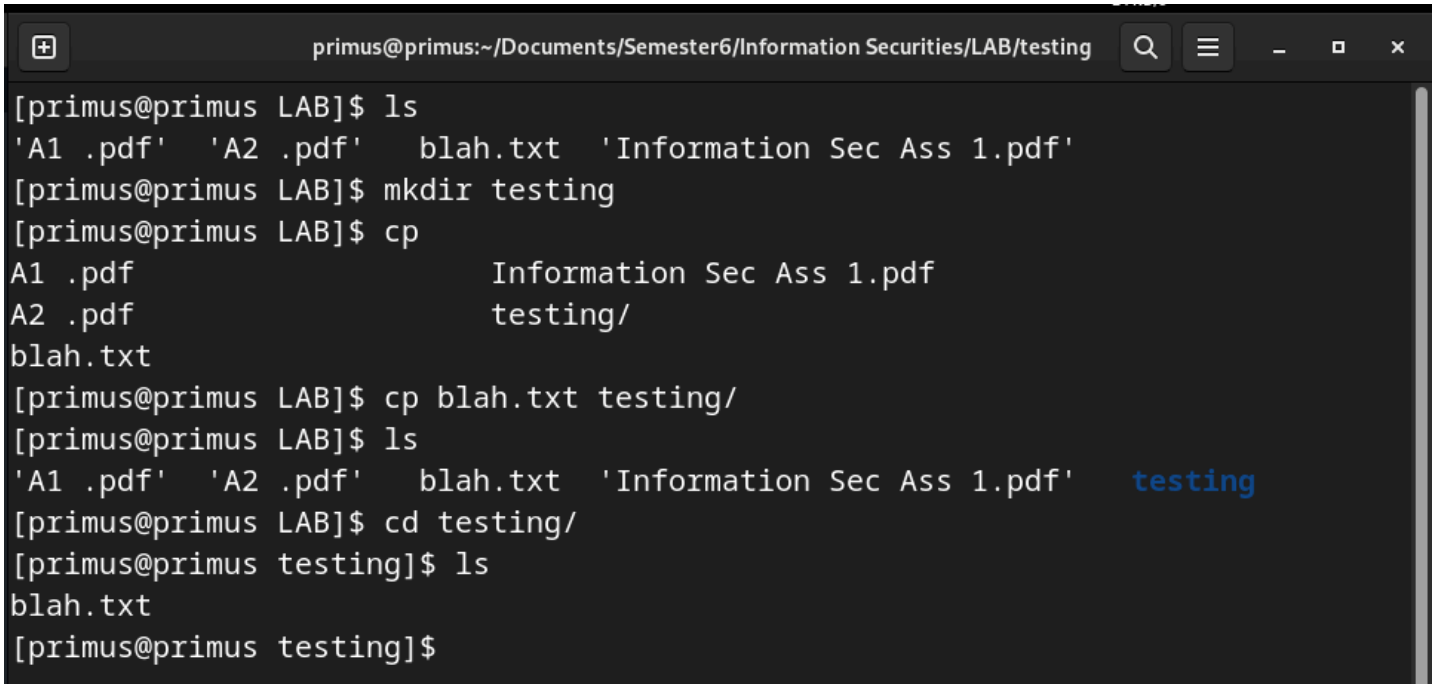






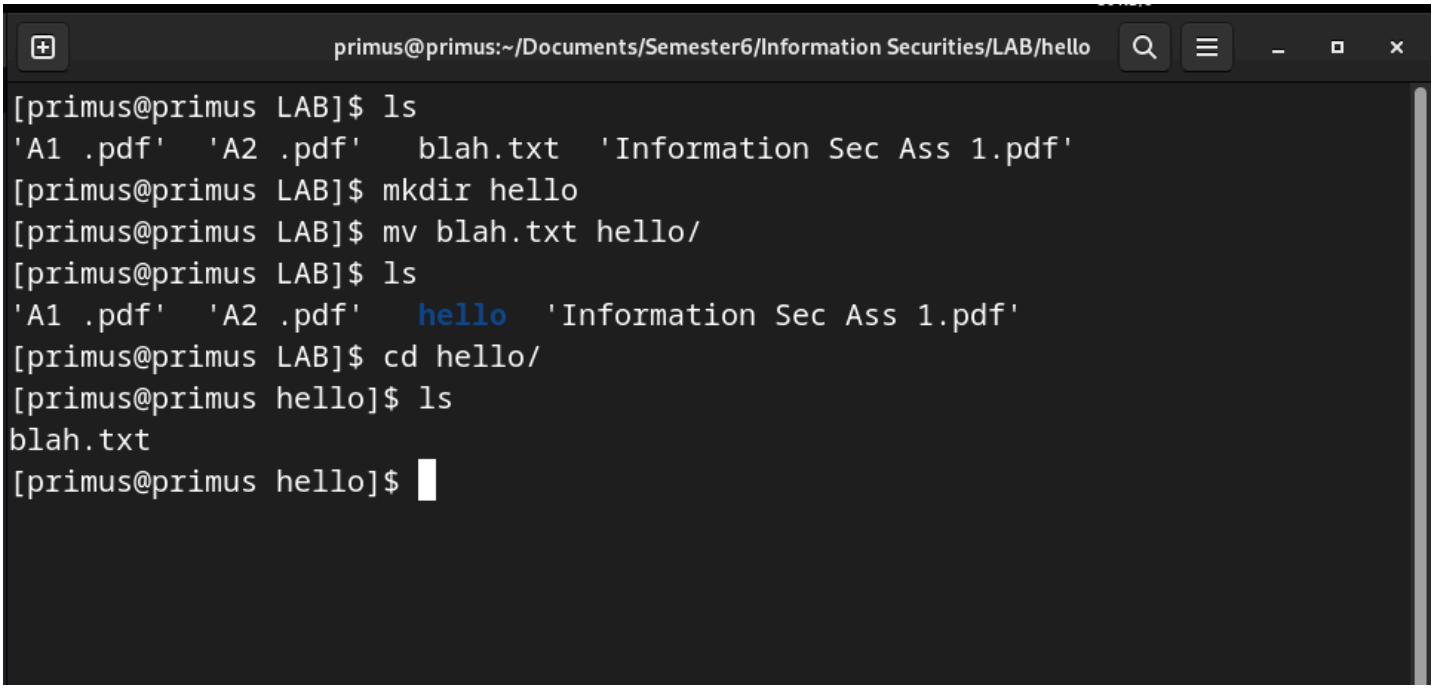
b. Copying Files:

i. cp: Copies files or directories. Example: `cp source_file destination_file`



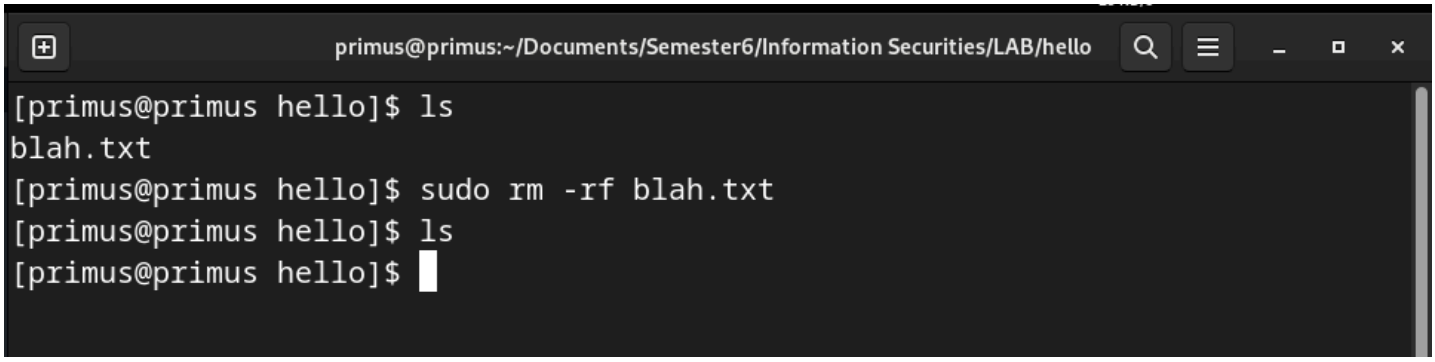
c. Moving Files:

i. mv: Moves or renames files or directories. Example: `mv source_file destination_file`



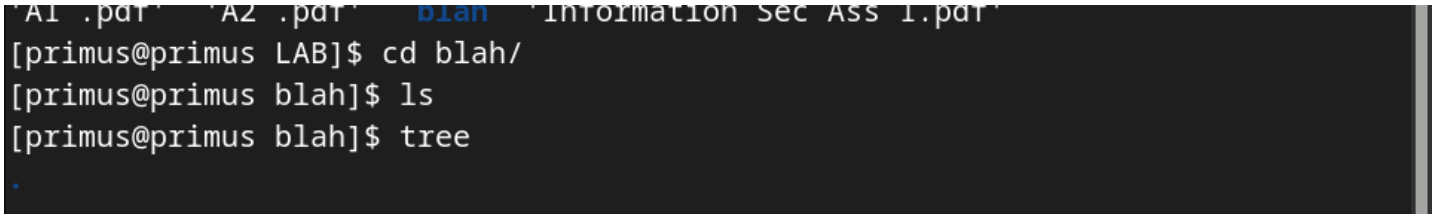
d. Removing Files:

i. rm: Removes files or directories.
ii. p: Removes parent directories as well if empty.
iii. -pv: Shows each file as it's being removed.
iv. -rf: Forcefully removes files or directories recursively without prompting.
v. -rp: Removes directories and their contents recursively.
vi. -r: Removes directories and their contents recursively.

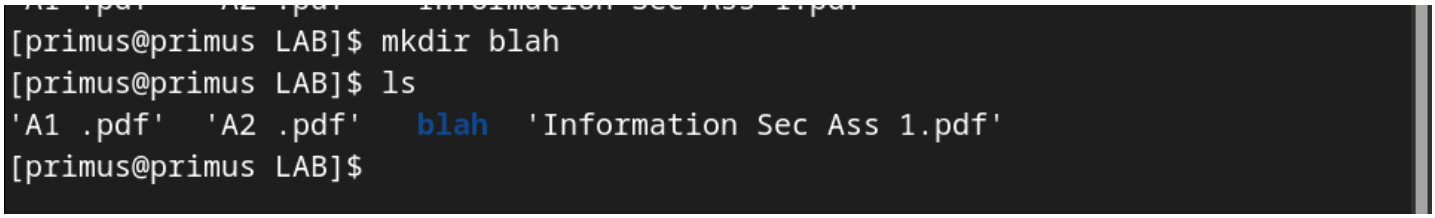


e. Directory Commands:

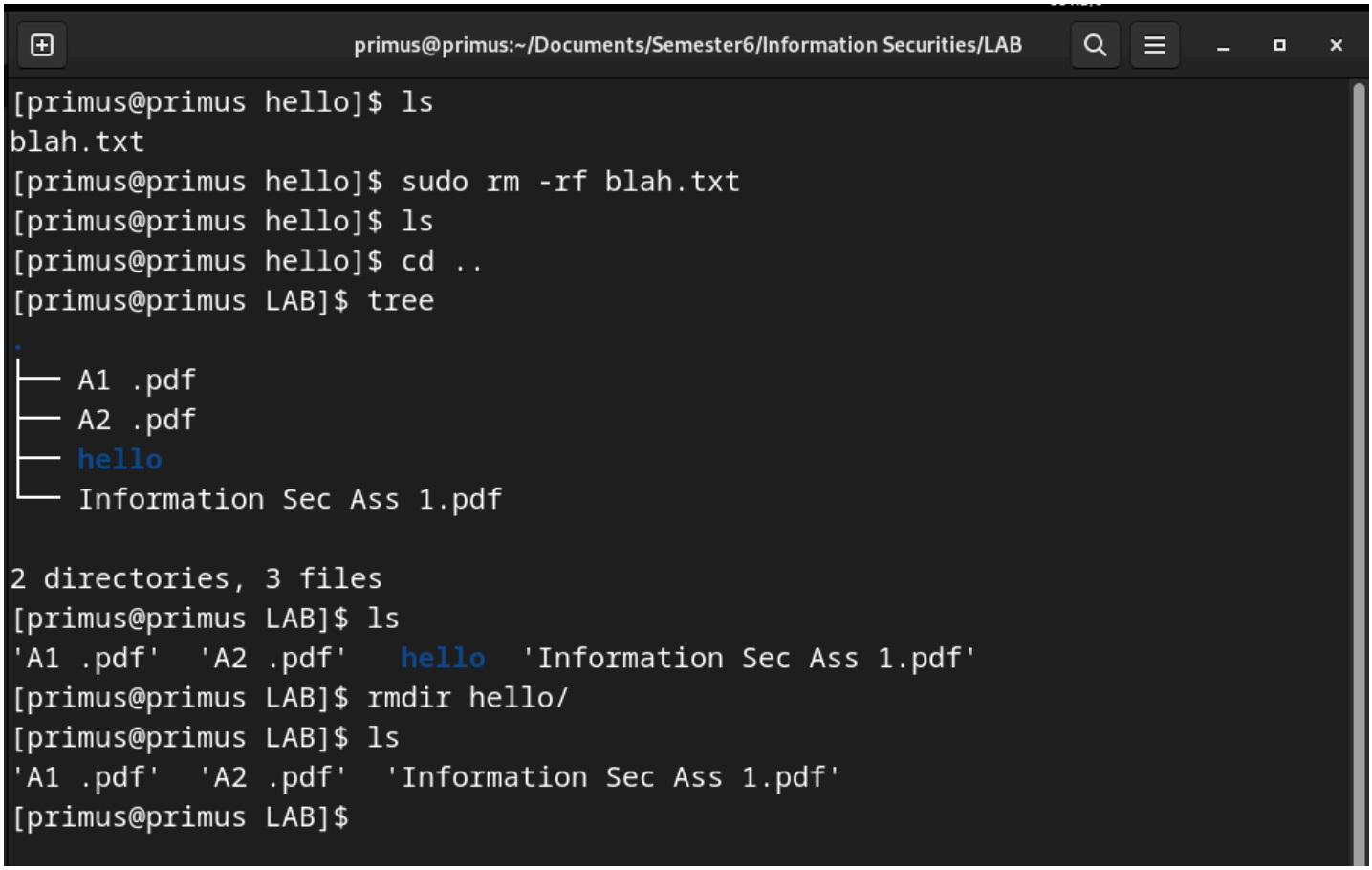
i. sudo: Executes a command with superuser privileges
ii. sudo su: Switches user to root.
iii. cd: Changes the current directory. Example: `cd directory_path`



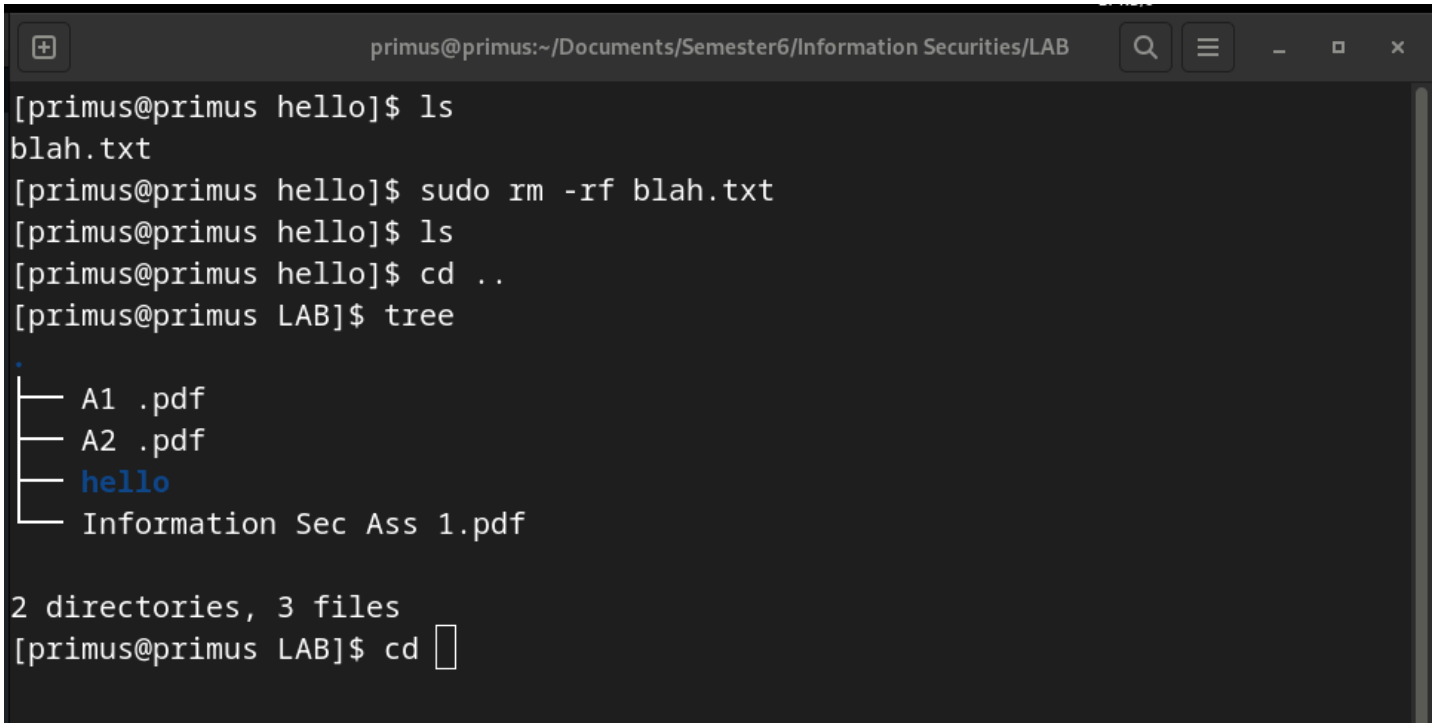
iv. mkdir: Creates a new directory. Example: `mkdir directory_name`



v. rmdir: Removes empty directories. Example: `rmdir directory_name`

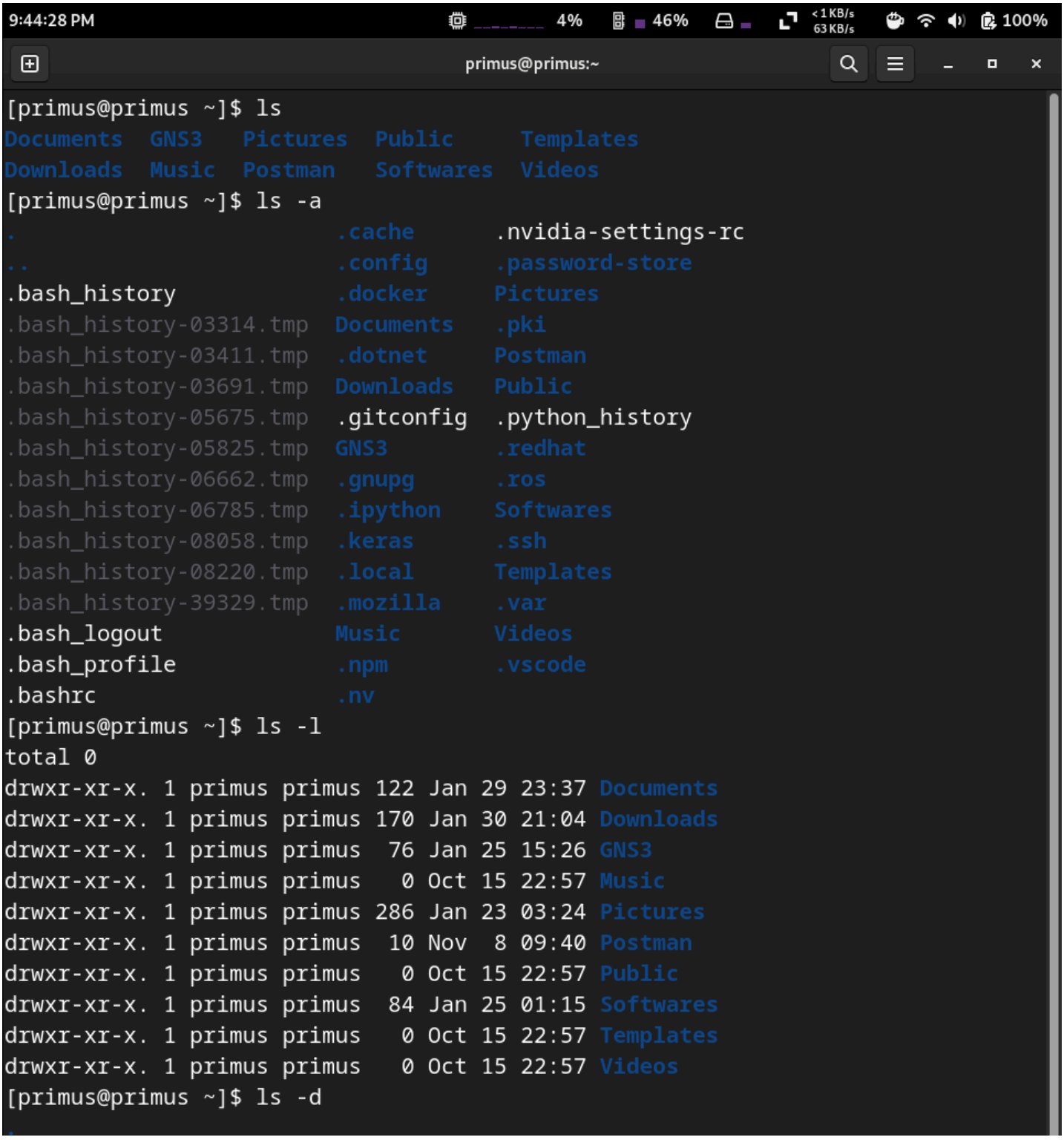


vi. tree: Displays the directory tree structure. Example: `tree directory_path`



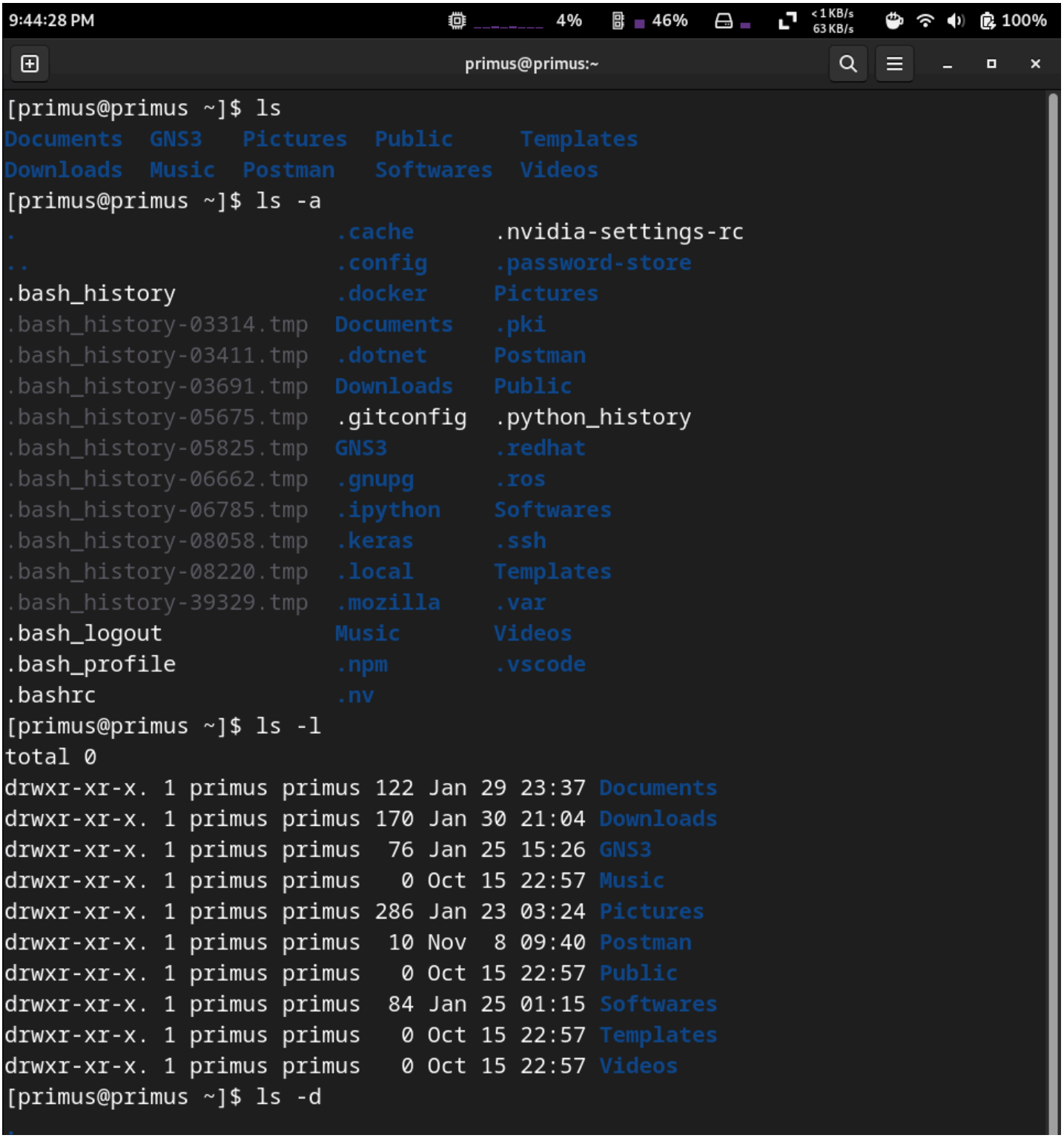
f. Miscellaneous Commands:

- **i.** -ls: Lists files and directories.
    1. -a: Lists all files, including hidden ones.
    2. -l: Displays detailed information about files.
- **ii.** -d: Lists only directories.

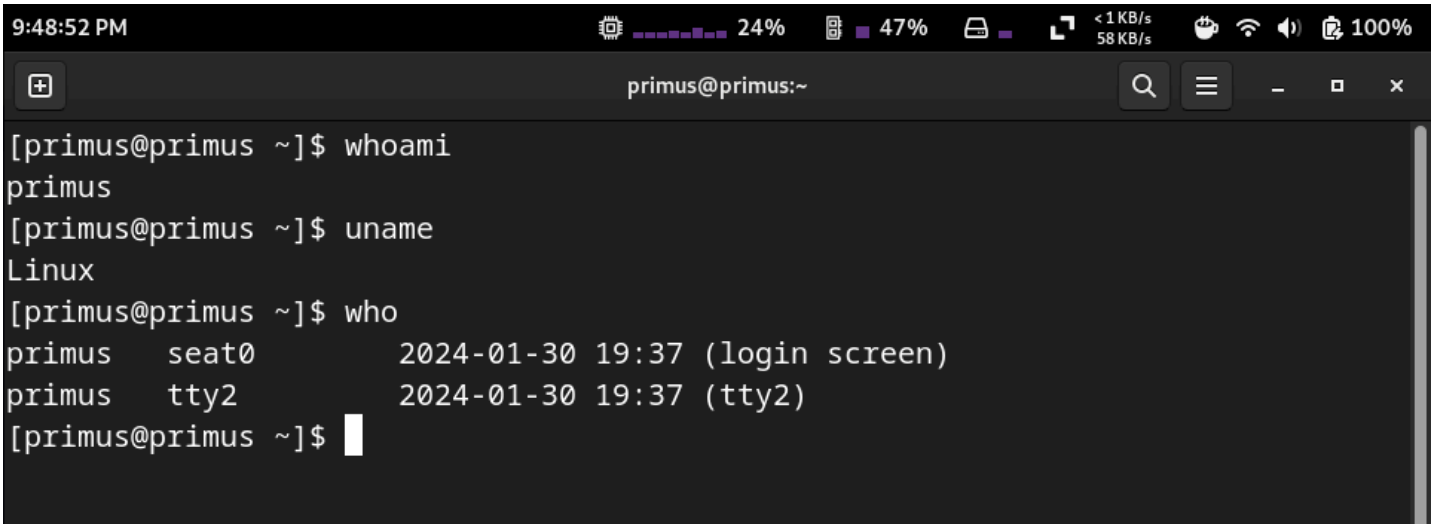


iii. history: Displays a list of previously executed commands.
iv. pwd: Prints the current working directory.
v. head: Outputs the first part of files. Example: `head filename`
vi. tail: Outputs the last part of files. Example: `tail filename`

vii. ps: Displays information about active processes. Example: `ps aux`
viii. kill: Terminates processes. Example: `kill process_id

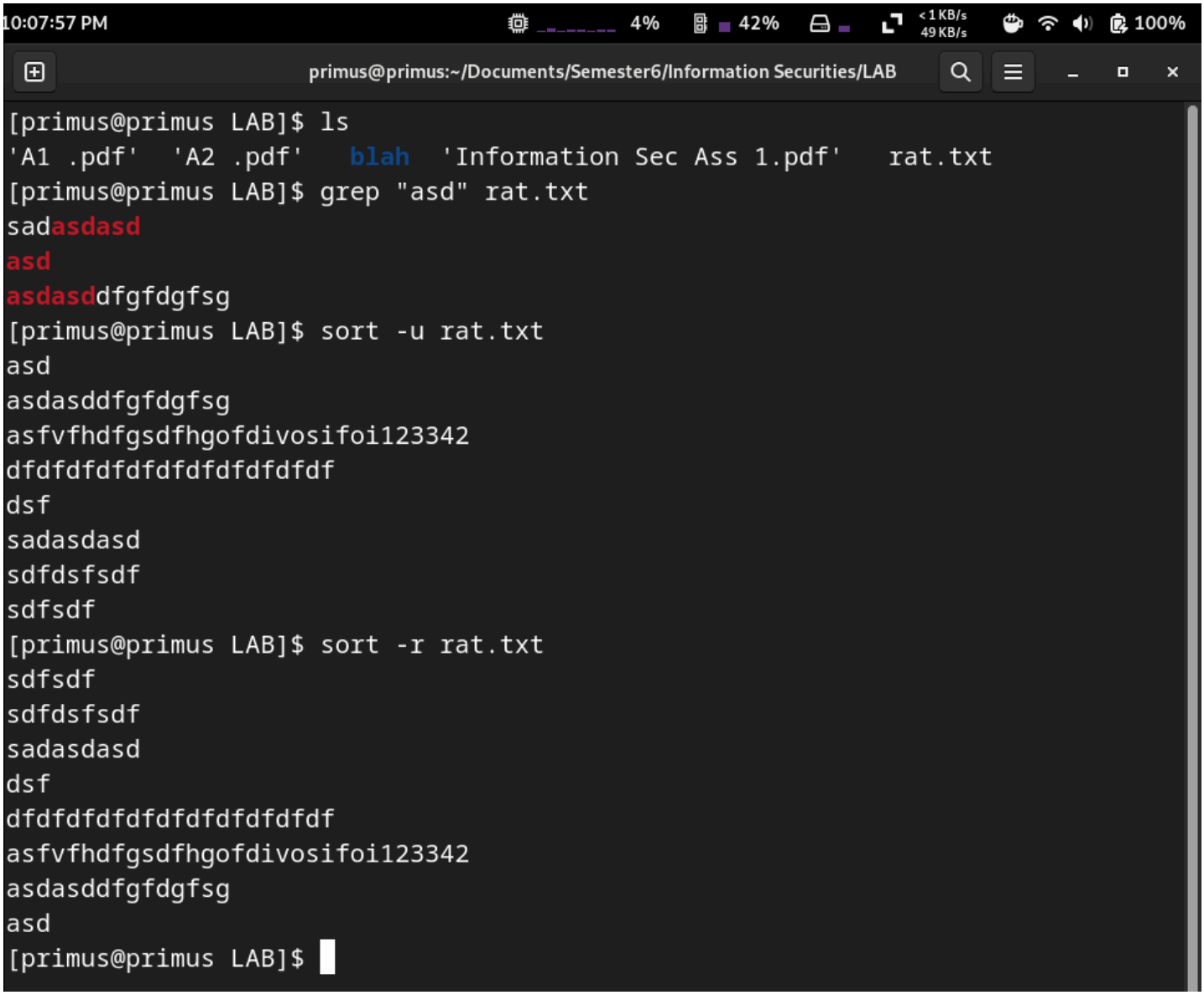


ix. **whoami** - to see the user name



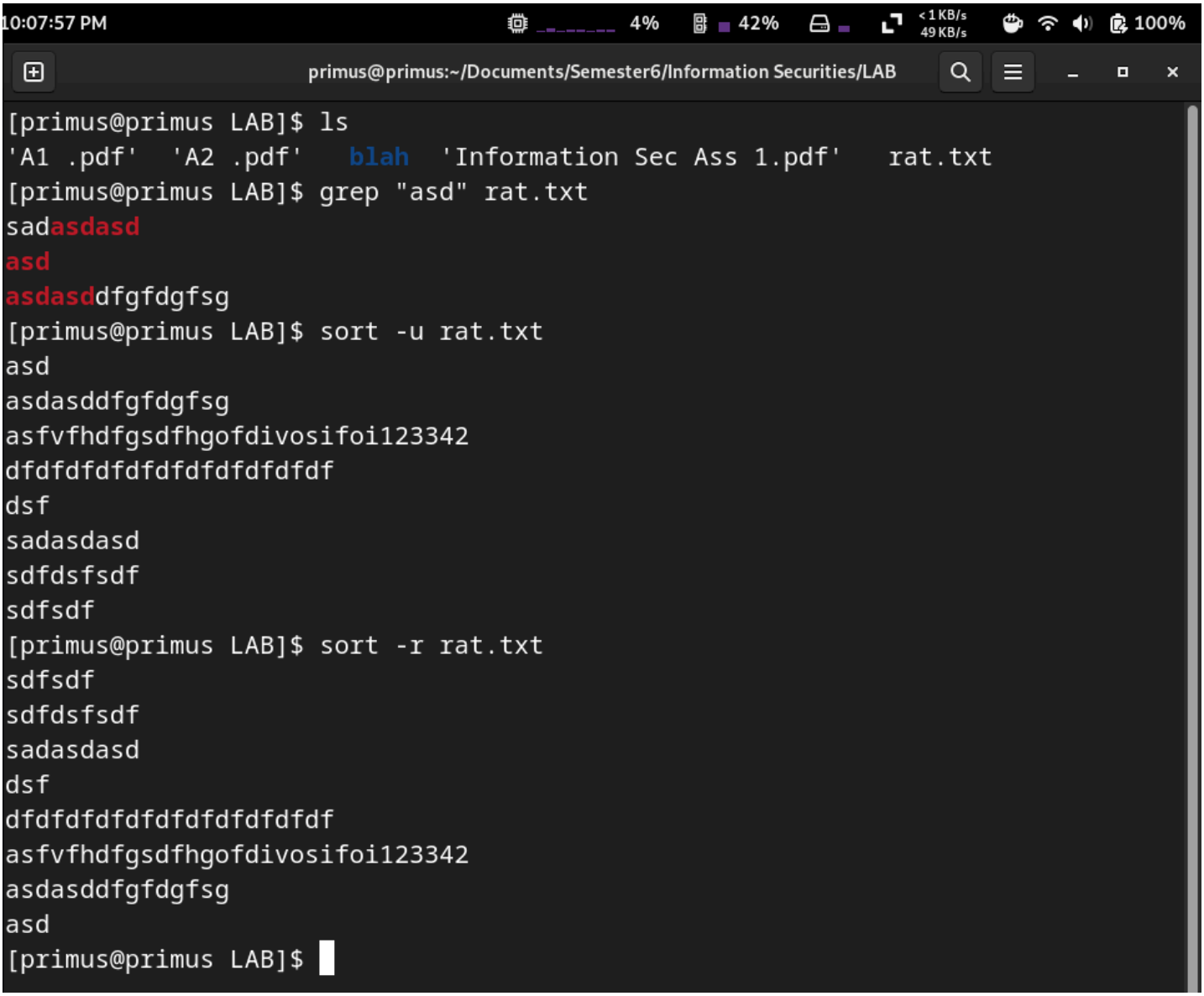
g. Filter Commands:

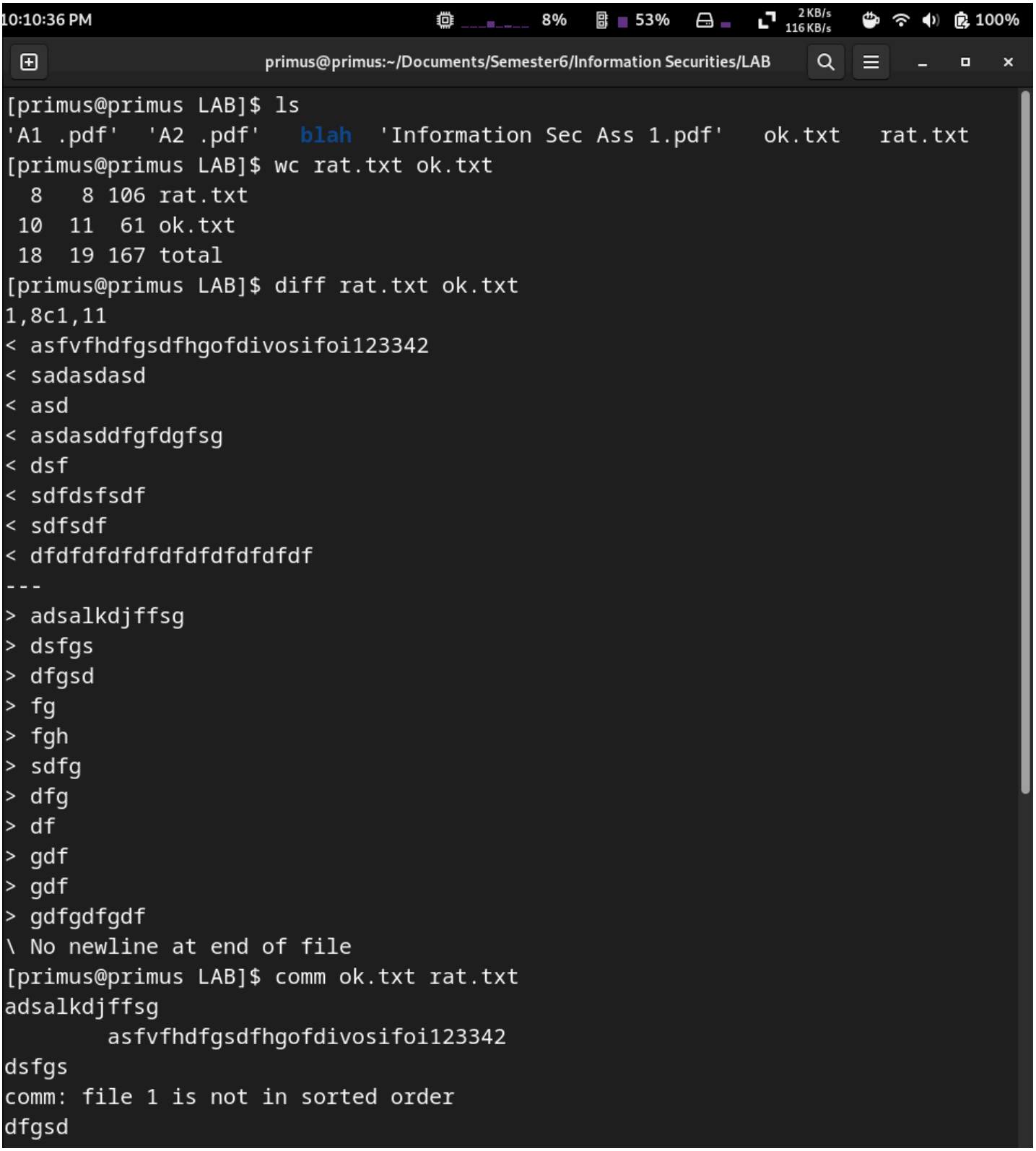
- **i.** grep: A command-line utility for searching plain-text data using regular expressions. It filters lines that match a specified pattern.
- **ii.** sort: This command sorts the lines of text files in ascending or descending order.



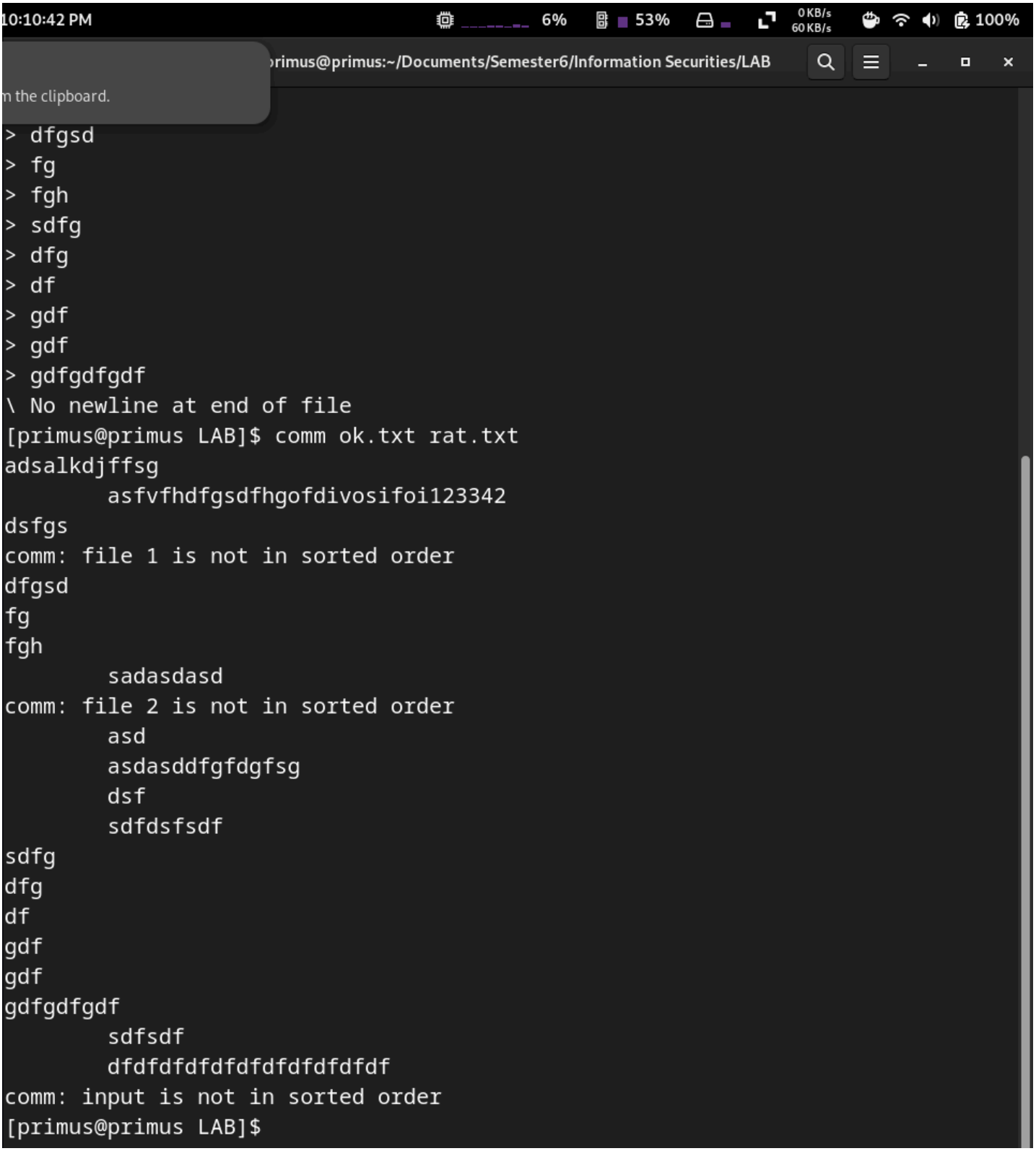
h. File Comparison Commands:

- **i.** cmp: Compares two files byte by byte and displays the first mismatch.
- **ii.** diff: Compares the contents of two files line by line and displays the differences between them.
- **iii.** comm: Compares two sorted files line by line and displays lines unique to each file and common to both.
- **iv.** wc: Counts the number of lines, words, and characters in a file or standard input.
- **v.** uniq: Filters adjacent matching lines from a sorted file and displays unique lines.


10:07:57 PM
4%
42%
< 1 KB/s
49 KB/s
100%
primus@primus:~/Documents/Semester6/Information Securities/LAB
[primus@primus LAB]$ ls
'A1 .pdf' 'A2 .pdf'   blah 'Information Sec Ass 1.pdf'   rat.txt
[primus@primus LAB]$ grep "asd" rat.txt
sadasdasd
asd
asdasddfgfdgfsg
[primus@primus LAB]$ sort -u rat.txt
asd
asdasddfgfdgfsg
asfvfhdfgsdfhgofdivosifoi123342
dfdfdfdfdfdfdfdfdfdfdf
dsf
sadasdasd
sdfdsfsdf
sdfsdf
[primus@primus LAB]$ sort -r rat.txt
sdfsdf
sdfdsfsdf
sadasdasd
dsf
dfdfdfdfdfdfdfdfdfdfdf
asfvfhdfgsdfhgofdivosifoi123342
asdasddfgfdgfsg
asd
[primus@primus LAB]$

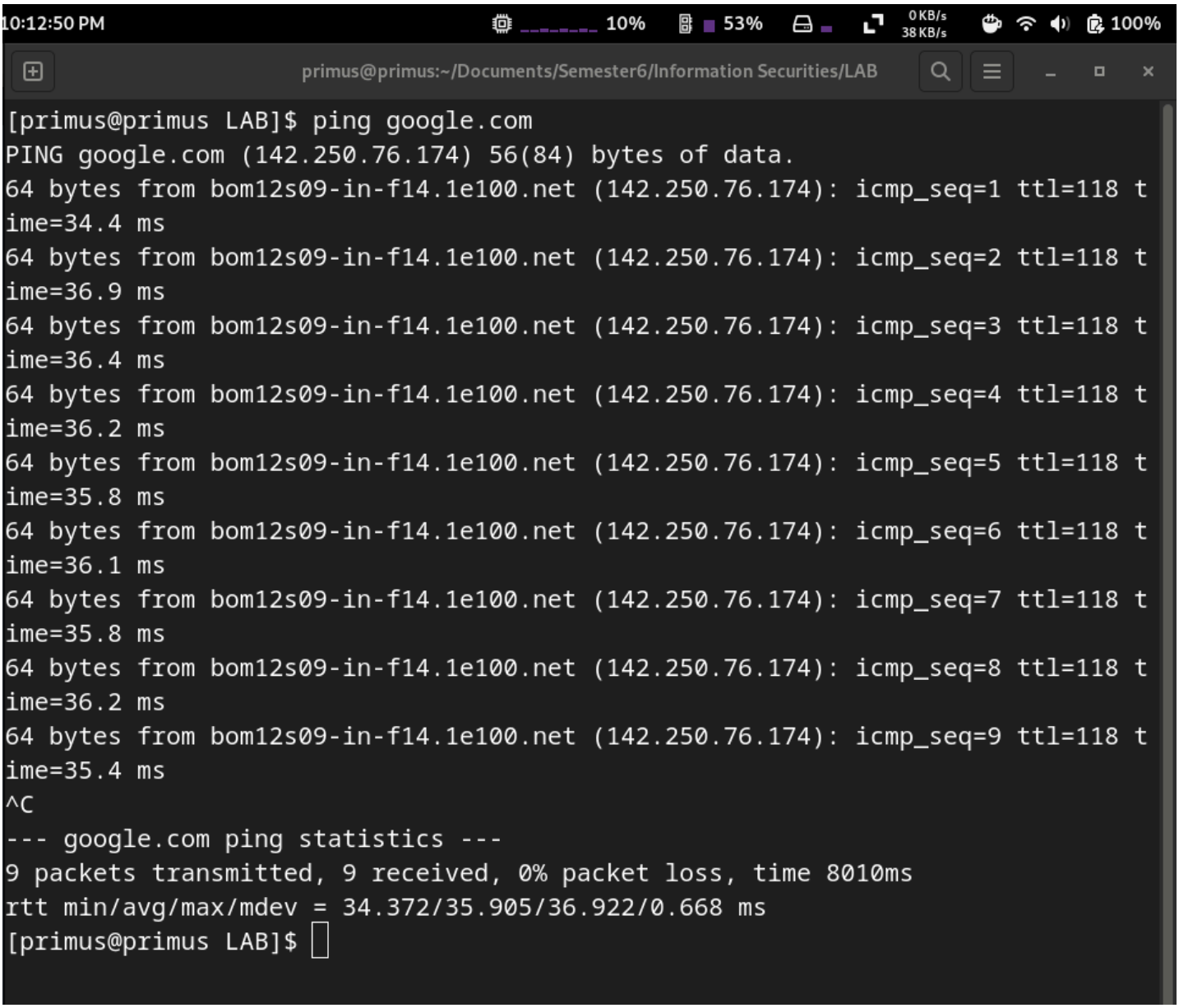

10:10:36 PM
8%
53%
2 KB/s
116 KB/s
100%
primus@primus:~/Documents/Semester6/Information Securities/LAB
[primus@primus LAB]$ ls
'A1 .pdf' 'A2 .pdf'   blah 'Information Sec Ass 1.pdf'   ok.txt   rat.txt
[primus@primus LAB]$ wc rat.txt ok.txt
  8   8 106 rat.txt
 10 11 61 ok.txt
 18 19 167 total
[primus@primus LAB]$ diff rat.txt ok.txt
1,8c1,11
< asfvfhdfgsdfhgofdivosifoi123342
< sadasdasd
< asd
< asdasddfgfdgfsg
< dsf
< sdfdsfsdf
< sdfsdf
< dfdfdfdfdfdfdfdfdfdf

> adsalkdjffsg
> dsfgs
> dfgsd
> fg
> fgh
> sdfg
> dfg
> df
> gdf
> gdf
> gdfgdfgdf
\ No newline at end of file
[primus@primus LAB]$ comm ok.txt rat.txt
adsalkdjffsg
        asfvfhdfgsdfhgofdivosifoi123342
dsfgs
comm: file 1 is not in sorted order
dfgsd



i. **Networking Commands:**
   i. Ping:

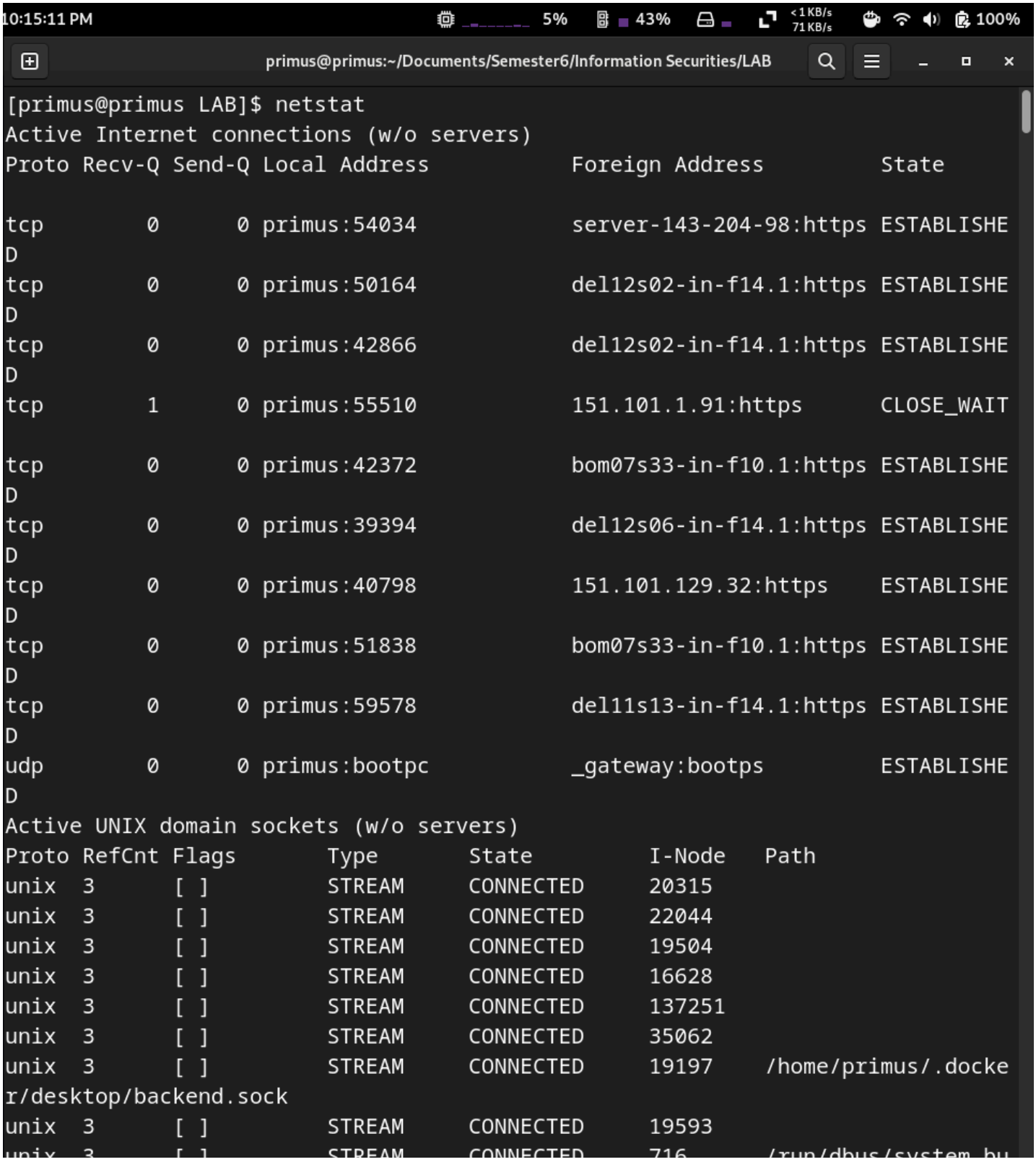
1. **ping [hostname or IP address]:** Sends ICMP echo request packets to the specified host and waits for a response. Example: `ping google.com` or `ping 8.8.8.8`.



2. **ping -c [count]**: Specifies the number of ICMP echo request packets to send. Example: `ping -c 5 google.com` will send 5 packets
3. **ping -t [ttl]**: Sets the Time-To-Live (TTL) value for outgoing packets. Example: `ping -t 10 google.com` sets the TTL to 10.
4. **ping -i [interval]:** Specifies the interval between sending ICMP echo request packets. Example: `ping -i 2 google.com` sets the interval to 2 seconds.

ii. Netstat:

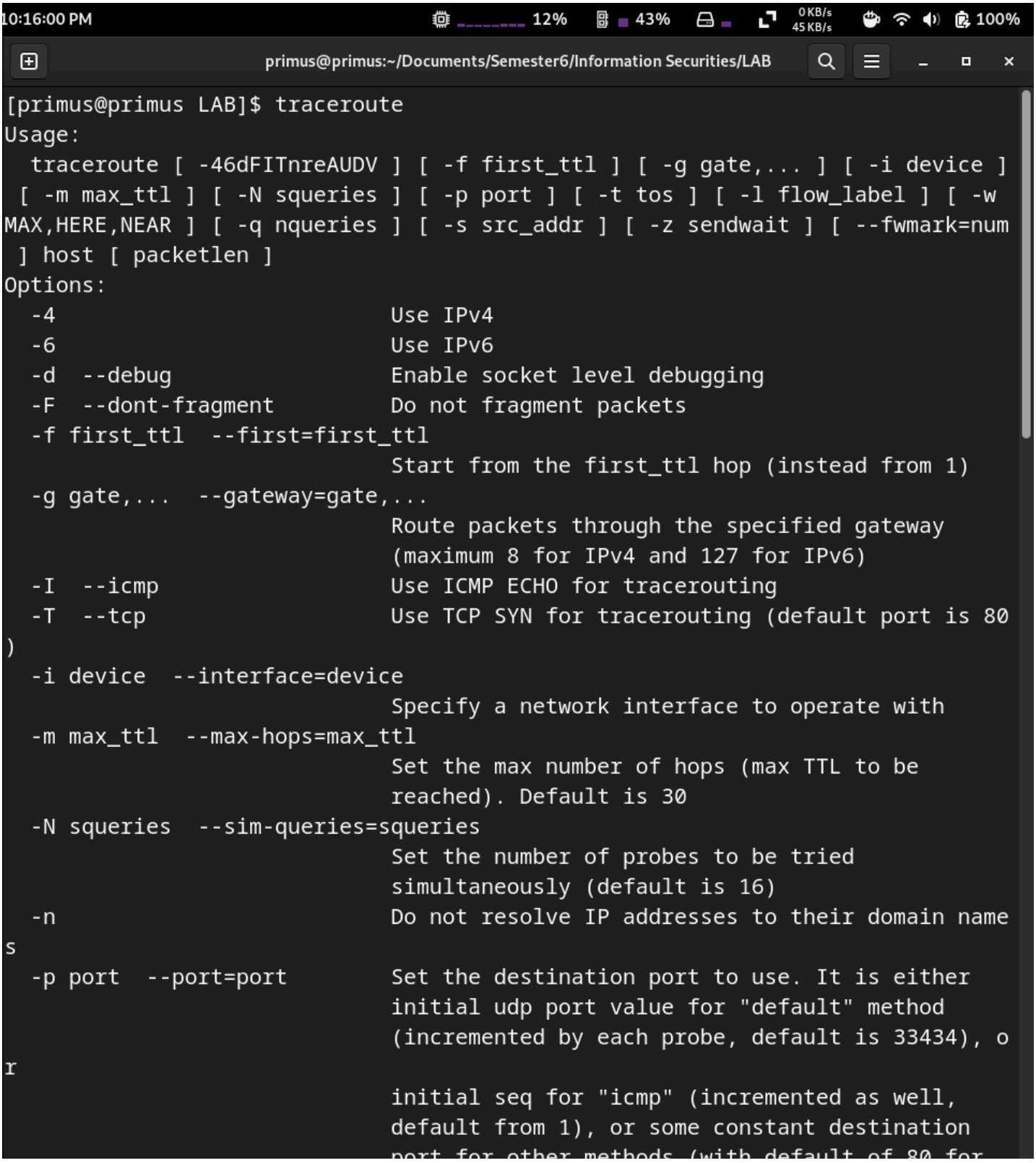
1. **netstat -a**: Displays all active connections and listening ports.



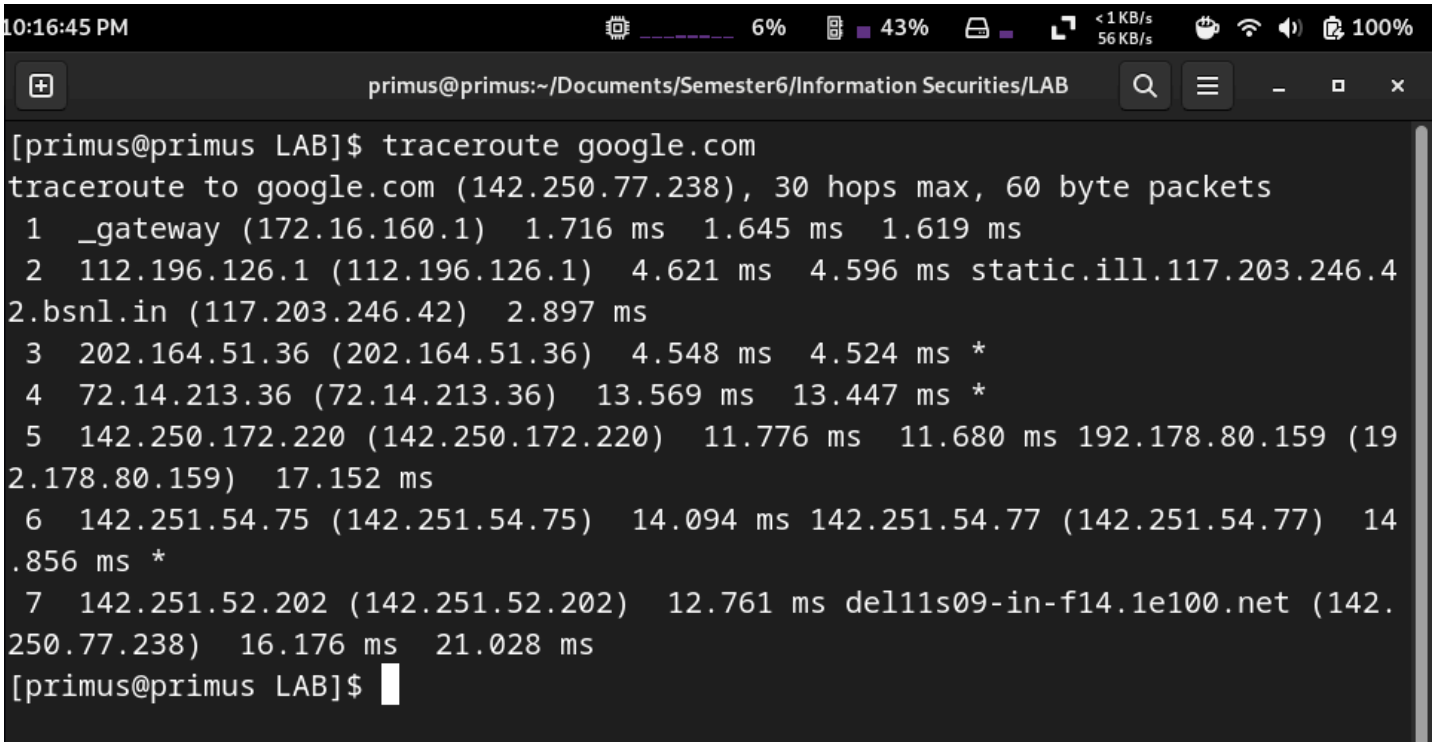
2. **netstat -r**: Shows the routing table, including the default gateway and interface-specific routes.

3. **netstat -n:** Displays numerical addresses and port numbers instead of resolving them to hostnames and service names.
4. **netstat -t:** Shows TCP connections.
5. **netstat -u:** Displays UDP connections.
6. **netstat -p:** Shows the process IDs (PIDs) of the processes associated with each connection.

iii. tracert (traceroute): traceroute is for linux

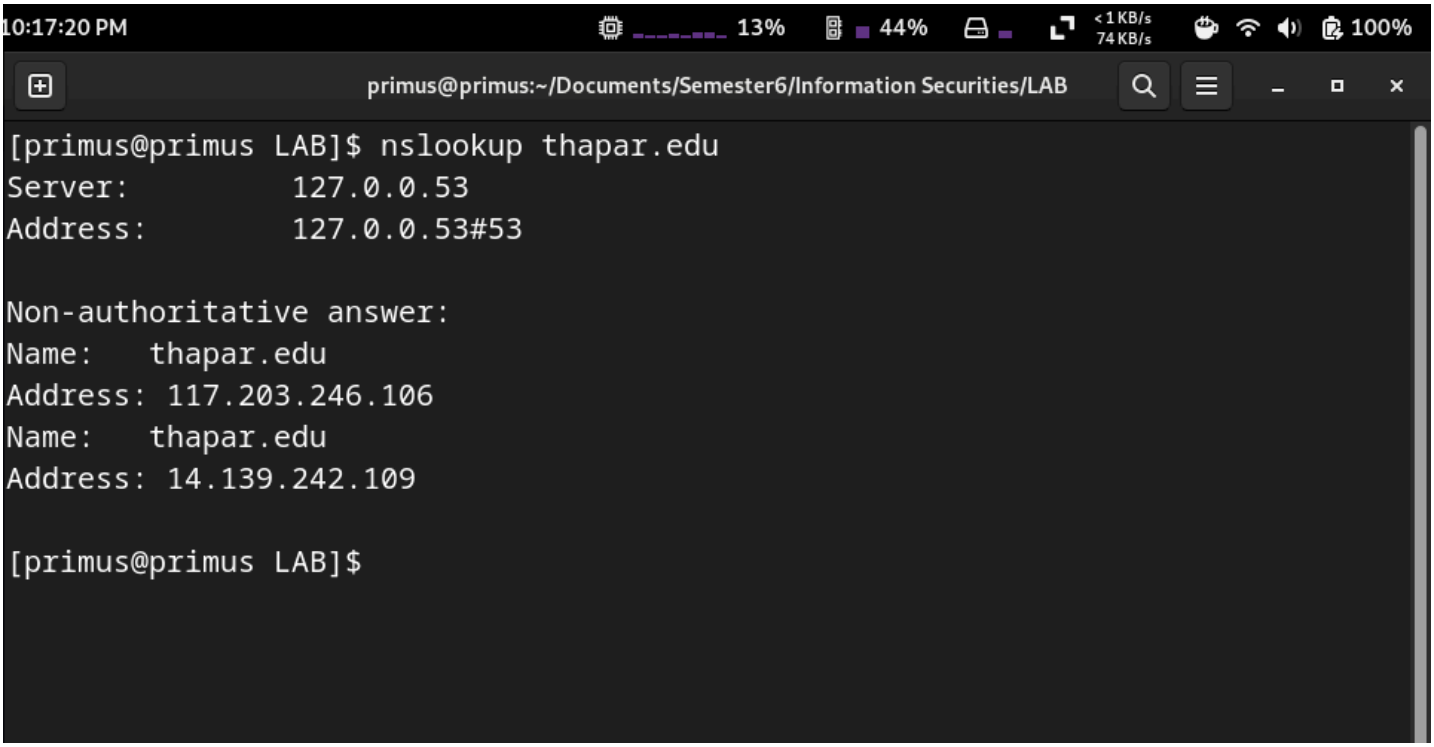


1. **tracert [hostname or IP address]:** Traces the route taken by packets from the source to the destination, displaying the IP addresses of routers along the way. Example: `tracert google.com` or `traceroute 8.8.8.8`.



2. **tracert -d:** Performs a trace without attempting to resolve IP addresses to hostnames.
3. **tracert -h [max_hops]:** Specifies the maximum number of hops (routers) in the path. Example: `tracert -h 10 google.com` limits the trace to 10 hops.

iv. Nslookup:



1. **nslookup [hostname]:** Queries the DNS to obtain domain name or IP address information for the specified hostname. Example: `nslookup google.com`.
2. **nslookup -type=[query_type] [hostname]:** Specifies the type of DNS record to query. Example: `nslookup -type=mx google.com` queries the MX (Mail Exchange) records for google.com.
3. **nslookup -querytype=[query_type] [hostname]:** Similar to the above, but with a different syntax. Example: `nslookup -querytype=ns google.com` queries the NS (Name Server) records for google.com.