LINUX SYSTEM ADMINISTRATION LAB FILE

BCE- C762

Submitted By:	Submitted To:
ASHISH BIBYAN 196301016 B.Tech, CSE,VII Sem	Dr. NISHANT KUMAR Assistant Professor CSE Department, FET, GKV

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
FACULTY OF ENGINEERING AND TECHNOLOGY
GURUKUL KANGRI UNIVERSITY
2022-2023

Certificate by student

This is to certify that the programs in this file are compiled and executed by me, and I have not copied them from anywhere. This work is done by me and I have not presented it anywhere else.

Name : ASHISH BIBYAN
ROLL NO: 196301016
BRANCH : CSE

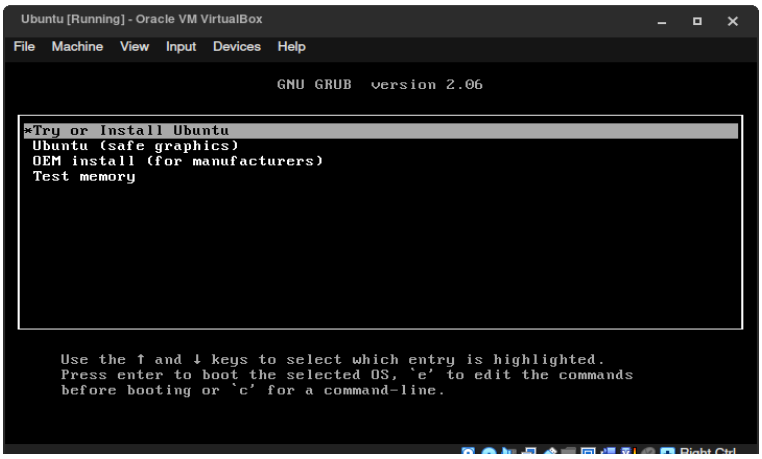
Certificate by Teacher

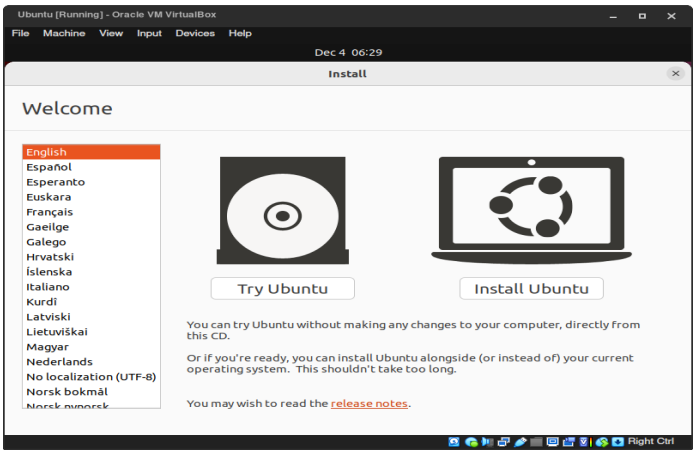
This is to certify that the programs in this file are done under my supervision and are not being copied from anywhere or presented anywhere for any sort of benefit.

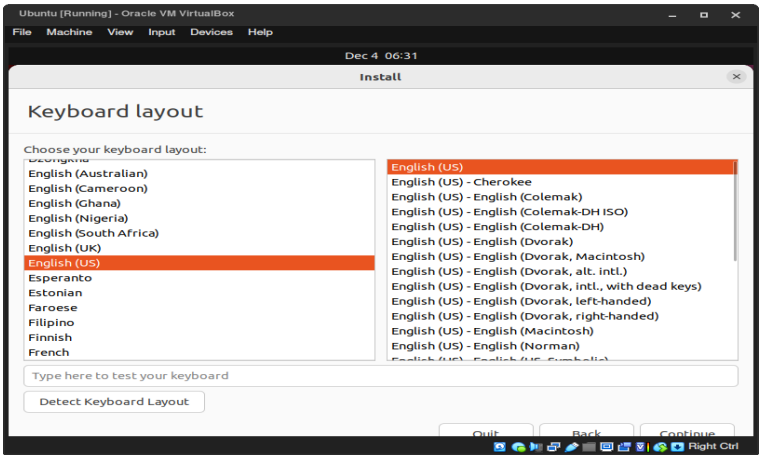
Dr. Nishant Kumar
Assistant Professor
Department of Computer Science & Engineering
Faculty of Engineering and Technology

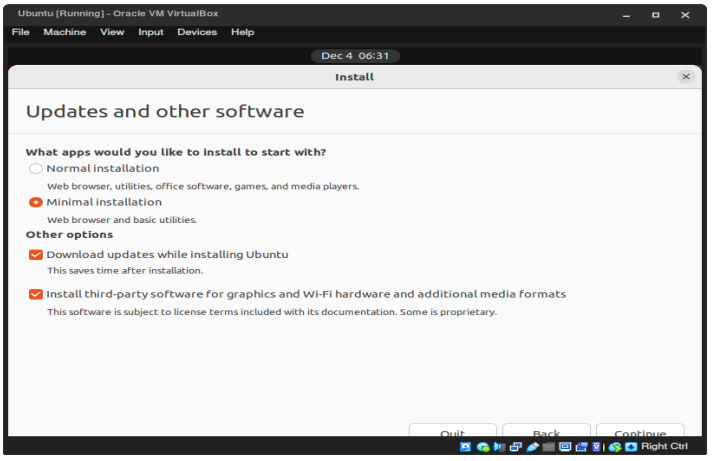
INDEX

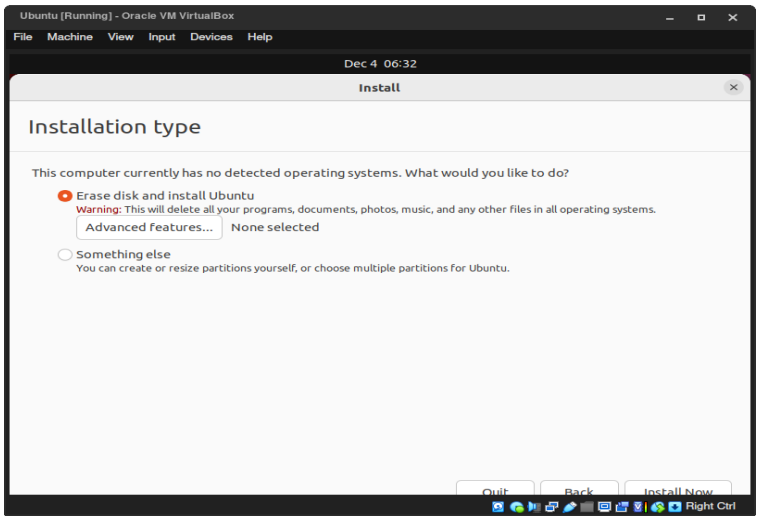
1. Installation of operating system (LINUX)

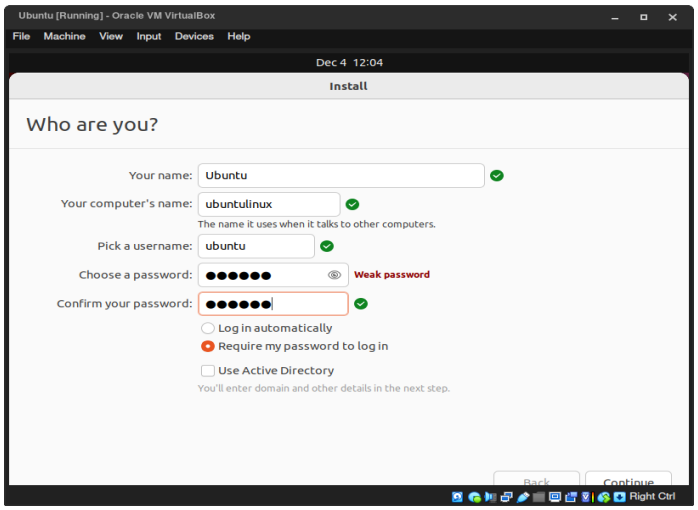












ASHISH BIBYAN
196301016

2. Installing openoffice in Linux

Install openoffice .deb file from its official site

Go to downloads folder and extract .tar file

```
virtual@virtualbox:~/Downloads$ tar -xvf Apache_OpenOffice_4.1.7_Linux_x86-64_install-deb_en-US.tar.gz
en-US/
en-US/DEBS/
en-US/DEBS/openoffice-brand-math_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-base_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-draw_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-calc_4.1.7-1_amd64.deb
en-US/DEBS/openoffice_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-writer_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-ooolinguistic_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-core04_4.1.7-1_amd64.deb
en-US/DEBS/desktop-integration/
en-US/DEBS/desktop-integration/openoffice4.1-debian-menus_4.1.7-9800_all.deb
en-US/DEBS/openoffice-en-us_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-calc_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-en-us_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-gnome-integration_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-pyuno_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-math_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-impress_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-res_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-images_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-help_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-impress_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-base_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-math_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-brand-draw_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-en-us-calc_4.1.7-1_amd64.deb
en-US/DEBS/openoffice-ure_4.1.7-1_amd64.deb
```

Go to en-US/DEBS and install .deb file

```
virtual@virtualbox:~/Downloads$ cd en-US/DEBS/
virtual@virtualbox:~/Downloads/en-US/DEBS$ sudo dpkg -i *.deb
Selecting previously unselected package openoffice.
(Reading database ... 192881 files and directories currently installed.)
Preparing to unpack openoffice_4.1.7-1_amd64.deb ...
Unpacking openoffice (4.1.7-1) ...
Selecting previously unselected package openoffice-base.
```

Also install desktop integration to get an icon in menu

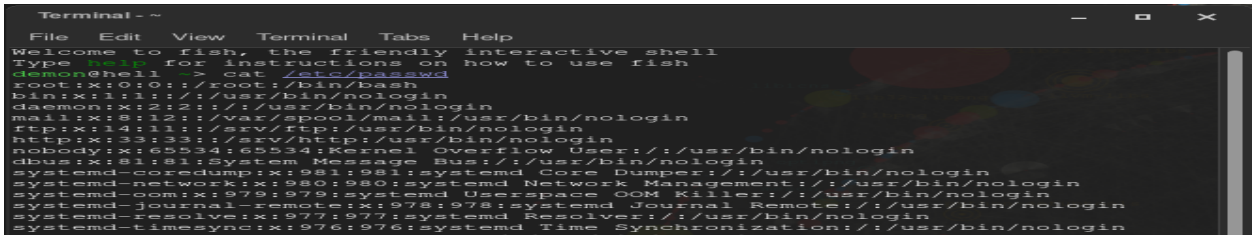
```
virtual@virtualbox:~/Downloads/en-US/DEBS$ cd desktop-integration/
virtual@virtualbox:~/Downloads/en-US/DEBS/desktop-integration$ sudo dpkg -i *.deb
(Reading database ... 184495 files and directories currently installed.)
Preparing to unpack openoffice4.1-debian-menus_4.1.7-9800_all.deb ...
Unpacking openoffice-debian-menus (4.1.7-9800) ...
Setting up openoffice-debian-menus (4.1.7-9800) ...
```

Openoffice is now installed in your system

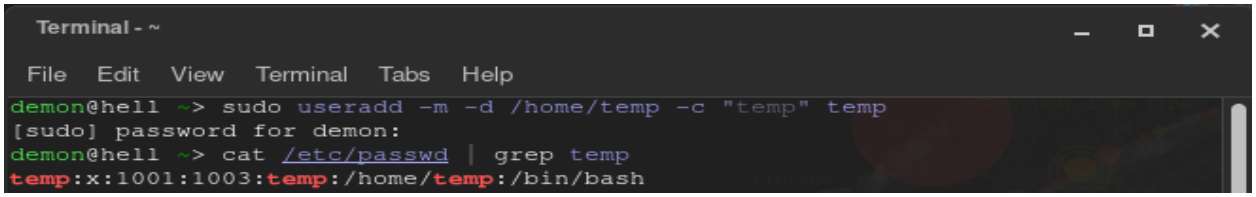
ASHISH BIBYAN
196301016

3. User Management

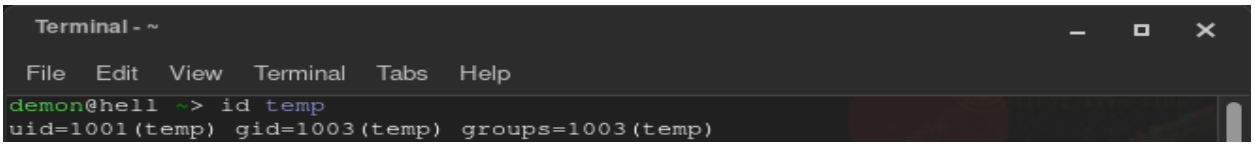
List users



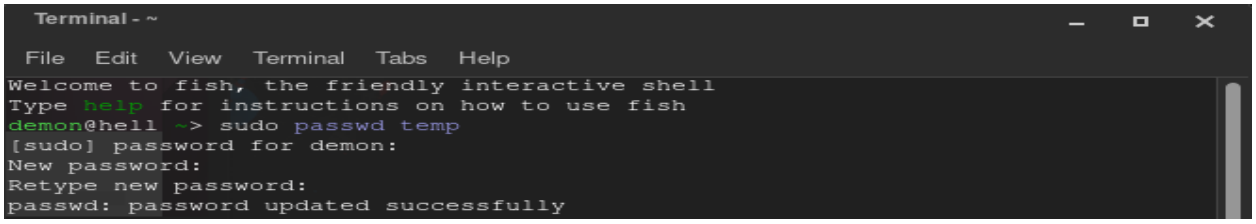
Add user



Get id of user



User password



Add user to group

Delete user

4. Security Management

Security management has evolved since the turn of the 20th century. Today's security managers must constantly adapt to keep up with a myriad of potential threats. They must be able to identify security vulnerabilities in an organization's network that could lead to a data breach, as well as facility vulnerabilities that could be exploited by thieves or vandals. These professionals must also develop a plan to protect a company's employees and assets in the event of a natural disaster, such as a wildfire, tornado or flood.
Corporate security managers identify and mitigate potential threats to a company. For example, they assess safety and security policies to ensure that an organization's employees, products, buildings and data are safeguarded. Security managers also make sure an organization fully complies with state and federal regulations, such as the Americans with Disabilities Act, and that safety procedures follow Occupational Safety and Health Administration (OSHA) guidelines. They may also be asked to develop safety manuals and training materials to ensure that current and future staff members are informed of a company's policies.
The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy. The information and procedures developed as part of security management processes will be used for data classification, risk management, and threat detection and response.These procedures enable an organization to effectively identify potential threats to the organization's assets, classify and categorize assets based on their importance to the organization, and to rate vulnerabilities based on their probability of exploitation and the potential impact to the organization.

Types of Security Management

Security management can come in various different forms. Three common types of security management strategies include information, network, and cyber security management.

Information Security Management: Information security management includes implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/IEC 27000 family of standards. Information security management programs should ensure the confidentiality, integrity, and availability of data. For example, healthcare organizations are governed by the Health Insurance Portability and Accessibility Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) protects payment card information.

Network Security Management: Network security management is a vital component of a network management strategy. The network is the vector by which most cyberattacks reach an organization's systems and its first line of defense against cyber threats. Network security management includes deploying network monitoring and defense solutions, implementing network segmentation, and controlling access to the network and the devices connected to it.

Cybersecurity Management: Cybersecurity management refers to a more general approach to protecting an organization and its IT assets against cyber threats. This form of security management includes protecting all aspects of an organization's IT

infrastructure, including the network, cloud infrastructure, mobile devices, Internet of Things (IoT) devices, and applications and APIs.

Security Management with Check Point

Security Automation into CI/CD Pipelines: Integrating security into CI/CD pipelines via automation reduces configuration errors, makes rapid deployments possible, and allows operational processes to be orchestrated.

Security Consolidation: Consolidated security improves efficiency, reduces capital and operational expenditure (CAPEX and OPEX), and achieves improved visibility and context by integrating security policy and events management within a single solution.

Solution Agility: Security management solutions must be agile and dynamic to keep up with the evolving cyber threat landscape. An example is an object in the security policy that defines private or public cloud addresses or users. As these external entities change, so does the security policy.

Efficient Operations: Security should be a business enabler, not a roadblock. Security management solutions must be efficient to not inhibit security innovation. For example, easy to use management that unifies security and event management and enables delegated access to multiple admins at the same time enables security staff to do more in less time.

Examples of security management tasks include:

- Adding rules and objects to a security policy to complete a new project.
- Responding to a security incident by validating threat indicators, mitigating the threat by isolating the infected host, and searching logs for other infected hosts using Indicators of Compromise (IoC) returned from the security incident analysis.
- Provisioning new cloud infrastructures, including the firewalls and the security policy for the firewalls protecting the new infrastructure.
- Cloud applications of DevSecOps include container image scanning, code scanning, Infrastructure as a Code (IaC) scanning, and scanning for credential exposure.

5. How to execute a script at startup and shutdown

- To execute a script at startup of Ubuntu, simply edit

```
/etc/rc.local
```

- And add your commands.
- Note that the script must always end with

```
exit 0
```

How to execute a script upon rebooting?

- To execute a script upon rebooting an Ubuntu system, you must write your script in

```
/etc/rc0.d
```

- Be sure to make the script executable by using

```
sudo chmod +x myscript
```

- Note that the scripts in this directory will be executed in alphabetical order. The name of your script must begin with K99 to run at the right time.

How to execute a script at shutdown?

- In order to execute a script at shutdown, you must put your script in

```
/etc/rc6.d
```

- And make it executable through

```
sudo chmod +x myscript
```

Please note that the scripts in this directory are executed in alphabetical order. Similar to the rebooting script, the name of your rebooting script must begin with K99

6. Network planning - subnet creation

In TCP/IP, the DARPA Internet support includes the concept of the subnet, sometimes called a subnetwork. This is a mechanism that enables several local networks to appear as a single Internet network to off-site hosts. You should consider using subnets in the following instances:

- When you want to hide the local network topology to the outside world. Using subnets requires only a single route to external gateways.
- When you want the ability to administer IP addresses locally. For example, a company may have an engineering subnet, a product marketing subnet, and a sales subnet, each administered by a different administrator who has control of IP addresses in a given range.
- When network bandwidth is limited due to cabling constraints. Setting up subnets, each separated by a gateway host, limits local subnet packets to those that are either destined for or sent from a local host. In this way, the overall network traffic each host on the subnet sees is lessened.

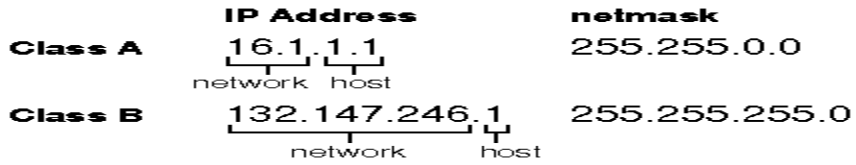
Setting up a subnet consists of:

- determining the appropriate IP addresses for your subnets.
- configuring subnet hosts with the correct IP addresses and netmasks.
- configuring gateway hosts between subnets.

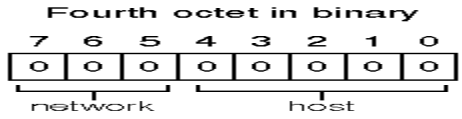
To set up subnet addresses, you must use a segment of the host portion of the IP address to use as the subnet address. For example, consider the following IP addresses and netmasks:

For class A and B networks, you can create subnets by converting the second and third octets, respectively, from host addresses to subnet addresses. Notice how the netmask changes accordingly:

The class A network *16* can now have up to 254 subnets (*16.1 - 16.254*). The class B network *10.0* can also have up to 254 subnets (*10.0.1 - 10.0.254*). While the netmask masks the network portion of the address, the broadcast address exposes the network address and hides the host portion. For example, the broadcast address for the subnet *10.0.246*, with a netmask of *255.255.255.0*, is *10.0.246.255*.



Partitioning a class C address is slightly more complex, as you must take a portion of the fourth octet as the subnetwork. For example, you might partition the first three (high order) bits of the fourth octet to represent the subnetwork, with the last five bits representing the host:



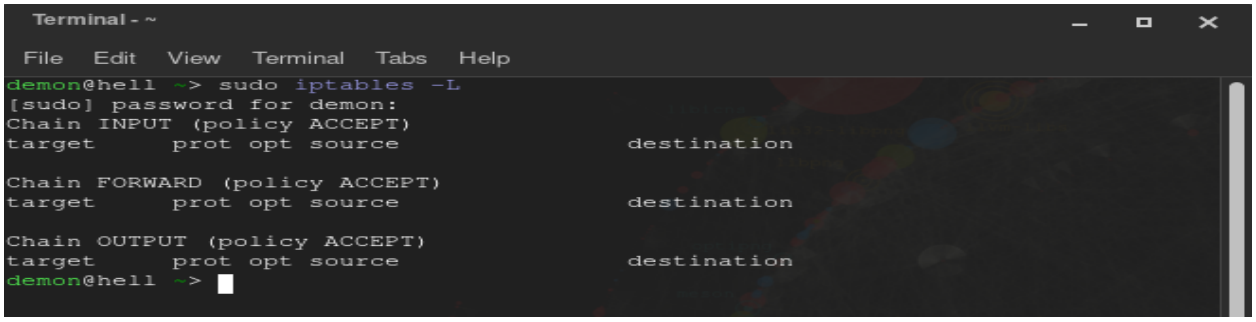
This scheme allows for up to 6 subnets of 30 hosts each, for a total of 180 hosts. The netmask for the hosts on these subnets is *255.255.255.224*; *224* is a decimal representation of the binary octet 11100000, which masks the subnet portion of the IP address.Possible subnets for the class C network *221.138.62.0*, with associated broadcast addresses, are:

Subnet	Hosts	Broadcast address
221.138.62.32	.33-.62	221.138.62.63
221.138.62.64	.65-.94	221.138.62.95
221.138.62.96	.97-.126	221.138.62.127
221.138.62.128	.129-.158	221.138.62.159
221.138.62.160	.161-.190	221.138.62.191
221.138.62.192	.193-.222	221.138.62.223

After you determine the new addresses for your hosts, you must configure them with the **Network Configuration Manager** or by editing */etc/tcp*. In addition, we must configure gateways between your subnets: these are hosts with multiple networking cards that serve more than one network. In linux you can assign subnet ip by editing /etc/network/interfaces

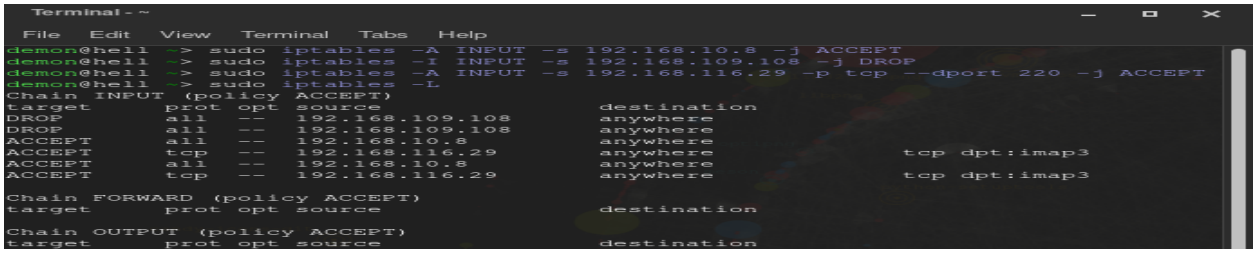
7. Firewall Configuration

List all the rules

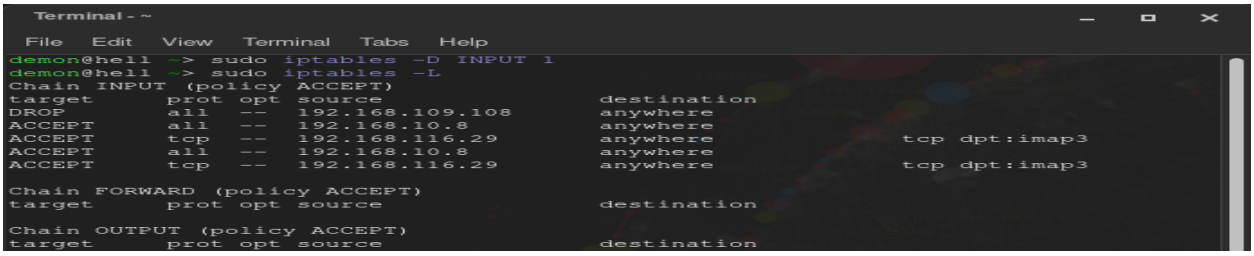


Set default rule

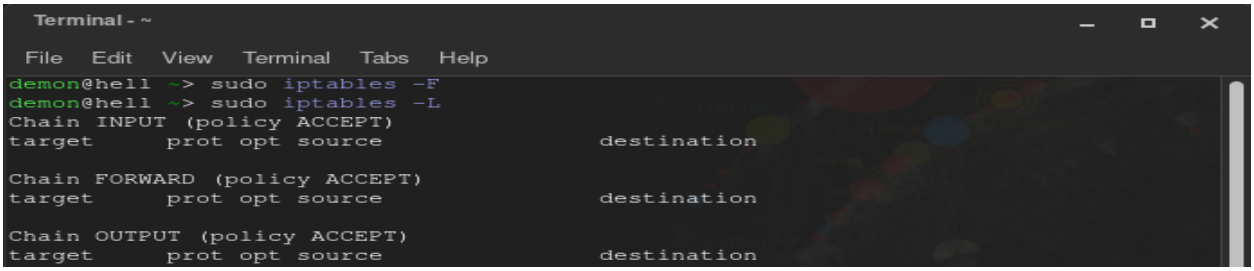
Insert Rules



Delete rules



Flush all rules

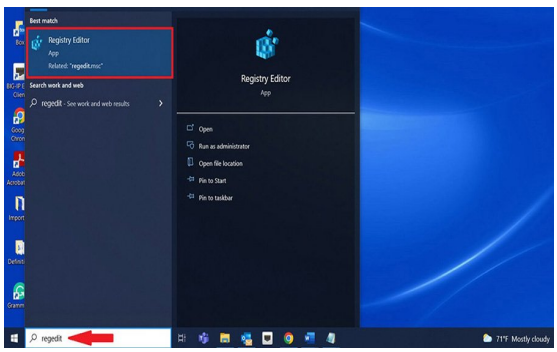


8. Basic properties of Windows Registry

The Windows registry is a hierarchically structured database that is used to store data related to configuration settings, software and user preferences in a Microsoft Windows operating system (OS). It contains entries and values that control the behavior of certain configurations and user preferences, as well as information for OS components and applications that operate at a low level.
Windows registry features and advantages are as follows:

- All low-level and third-party OS components and applications, like device drivers and kernels, can access the registry.
- To profile system performance, it facilitates access to the necessary counters.
- It stores and reflects user changes to configurations, preferences, policies and applications.
- Depending on the Windows version, it stores physical registry files in different locations.
- It contains two elements: keys, which are similar in concept to Windows folders, and values, which are similar to files.

The following properties have several use cases for the Windows Registry:
System performance. If registry entries or the keys inside a registry become corrupt or faulty, they can cause the system to crash or other performance issues. By using the Windows Registry Editor's intuitive display, users can edit or update the malfunctioning entries.
Configuration settings. The automatic startup programs, display or desktop settings inside the registry aren't always configured according to the user's preferences. The Windows Registry Editor can be used to change these configuration settings.
Registry cleaning. Items or entries inside a registry can sometimes break, though it is a rare occurrence with modern versions of Windows registries. To fix broken entries, a registry cleaner is required, but unlike standard configuration files, entries inside a Windows registry cannot be opened or cleaned via standard text editors. While there are many third-party registry cleaners available, the Windows Registry Editor tool works well for removing unwanted data in the registry.
Registry errors. Certain events can disrupt the hierarchy of the registry and cause errors. For example, a power outage can prevent the registry from saving, or worse, a malware intrusion into the system can take over a computer's registry. After addressing the root cause of the disruption -- for example, using antimalware software to find and eradicate the malware -- the Windows Registry Editor tool can be used to fix the hierarchical structure of the registry.
Finding strings. The Registry Editor can be helpful when searching for specific strings in key names, value names and value data.



ASHISH BIBYAN
196301016

9. Study of Important Windows Services

Windows Services are a core component of the Microsoft Windows operating system and enable the creation and management of long-running processes.Unlike regular software that is launched by the end user and only runs when the user is logged on, Windows Services can start without user intervention and may continue to run long after the user has logged off. The services run in the background and will usually kick in when the machine is booted. Developers can create Services by creating applications that are installed as a Service, an option ideal for use on servers when long-running functionality is needed without interference with other users on the same system.Some of the important services of Windows are Listed below:

Active Directory Service – Active Directory is a service Microsoft developed for Windows networks. It is included by default in most Microsoft Windows Server systems. Active Directory oversees centralized domain management and identity-related functions.

Prefetch and Superfetch Service – Speeds up operating system and application startup by caching to RAM frequently used files, libraries and application components. It does this by monitoring application usage and behavior.

Background Intelligent Transfer Service – This service facilitates throttled, prioritized and asynchronous file transfer between machines via idle bandwidth. It plays a key role in the delivery of software updates from servers to clients as well as in the transfer of files on Microsoft's instant messaging applications.

DNS Client Service – This service resolves domain names to IP addresses and locally caches this data.

Computer Browser Service – It allows users to easily locate shared resources on neighboring computers. All information is aggregated on one of the computers (referred to as the Master Browser) and other computers contact this machine for information on shared resources.

Internet Connection Sharing (ICS) Service – ICS enables the use of one device connected to the internet as an access point for other devices. Access could be through Ethernet broadband, cellular service or other gateway.

Routing and Remote Access Service – This service makes it possible to create applications that manage the remote access and routing capabilities of the Windows operating system. It allows the machine to act as a network router.

10. Study of Important LINUX Services

Some of the important services of Linux are Listed below:

Service Name	Description	Comments
crond	Periodic Command Scheduler	The task scheduling tool.
cups	Common Unix Printing System	A must have to enable printing
dm	Display Manager	The core of the x-server, required for using any GUI.
gpm	Mouse	Console mode mouse driver
iptables	kernel based Packet Filtering firewall	All good Linux firewalls are based on this service.
keytable	keyboard map	This tells the system exactly which keyboard you are using.
messagebus	Event monitoring service	This one sends broadcast messages to all users when needed, like the server is going down for reboot.
mon	System Monitoring daemon	A lot of system services require this in order to function
network	Networking	This turns the network card on, or powers the modem.
partmon	Partition Monitoring	This service keeps track on free space on mounted partitions.
shorwall	Firewall	A very good IPTables based firewall.
syslog	System Logging	It controls system logging.
Init	System init service	the first process started during booting of the computer system