**DAY-1 LOS Assignment**

**Name: Hymha N Raj**

**Program: M.E in Cyber Security**

**Subject: Linux Operating and Scripting**

**Roll No: 241059052**

**Definition of operating system**

Operating system is an intermediate between people and the machine, making available a user interface and supporting running of programs. It manages hardware and software resources on a computer or other devices

**Operating systems used in Cyber Security**

1. **Kali Linux**:

* **What It Does**: It's like a toolbox for security experts.
* **Why It’s Used**: Comes with everything you need for testing and fixing security issues—kind of like having all the right tools for a job right in one place.
* **Purpose**: Penetration testing and security research.
* **Features**: Built with a wide range of tools for security testing including Metasploit, Nmap, and WiresharK

1. **Parrot Security OS**:

* **What It Does**: It's like Kali’s laid-back sibling.
* **Why It’s Used**: Offers similar security tools but also focuses on keeping your privacy and doing forensic investigations—like having a multi-purpose gadget that’s great for various tasks.
* **Purpose**: Penetration testing, digital forensics, and development.
* **Features**: It has similar tools to Kali Linux but also emphasizes on privacy, anonymity and software development.

1. **BackBox**:

* **What It Does**: It’s a straightforward security assessment tool.
* **Why It’s Used**: User-friendly and designed for easy network and vulnerability checking—think of it as a no-fuss option for keeping your system secure.
* **Purpose**: Security assessment and vulnerability analysis.
* **Features**: A collection of network analysis tools, vulnerability assessment etc.

1. **Tails**:

* **What It Does**: Acts as a cloak of invisibility for your online activities.
* **Why It’s Used**: Helps you browse the web without leaving traces and keeps your identity anonymous—perfect for when you need to stay under the radar.
* **Purpose**: Privacy and anonymity.
* **Features**: A live OS that ensures privacy and anonymity while using the internet; it routes traffic through Tor without leaving any trace on the machine.

1. **Whonix**:

* **What It Does**: Provides double protection for your online actions.
* **Why It’s Used**: Uses two virtual machines to keep you safe and anonymous—one handles your internet connection through Tor, and the other takes care of your activities.

1. **Qubes OS**:

* **What It Does**: Keeps different tasks and apps separated to boost security.
* **Why It’s Used**: Like having separate rooms for different activities; if one room gets compromised, the others stay safe.

1. **Ubuntu Server**:

* **What It Does**: A reliable server platform you can customize.
* **Why It’s Used**: It’s stable and widely used, and you can enhance its security for managing server operations—like having a dependable workhorse that you can tweak for extra security.

1. **Windows Server**:

* **What It Does**: Manages and secures large IT environments.
* **Why It’s Used**: Comes with built-in security tools and is commonly used in big businesses to handle everything from user permissions to network security.

1. **OpenBSD**:

* **What It Does**: Focuses on being super secure and reliable.
* **Why It’s Used**: Known for its strong security measures and stable performance—like having a meticulous guardian to keep your systems safe.

1. **Fedora Security Lab**:

* **What It Does**: A playground for security researchers.
* **Why It’s Used**: Packed with tools for testing and exploring security issues—think of it as a specialized workshop for diving into cybersecurity challenges.

**Installation Process of Ubuntu**

**Prerequisites:**

* A computer with virtualization support (Intel VT-x/AMD-V)
* A laptop or PC with at least 25GB of storage space.
* A flash drive (12GB or above recommended).
* At least 4GB of RAM (8GB or more recommended)
* 30GB of free disk space
* Internet access

**Step 1:** **Install VirtualBox**

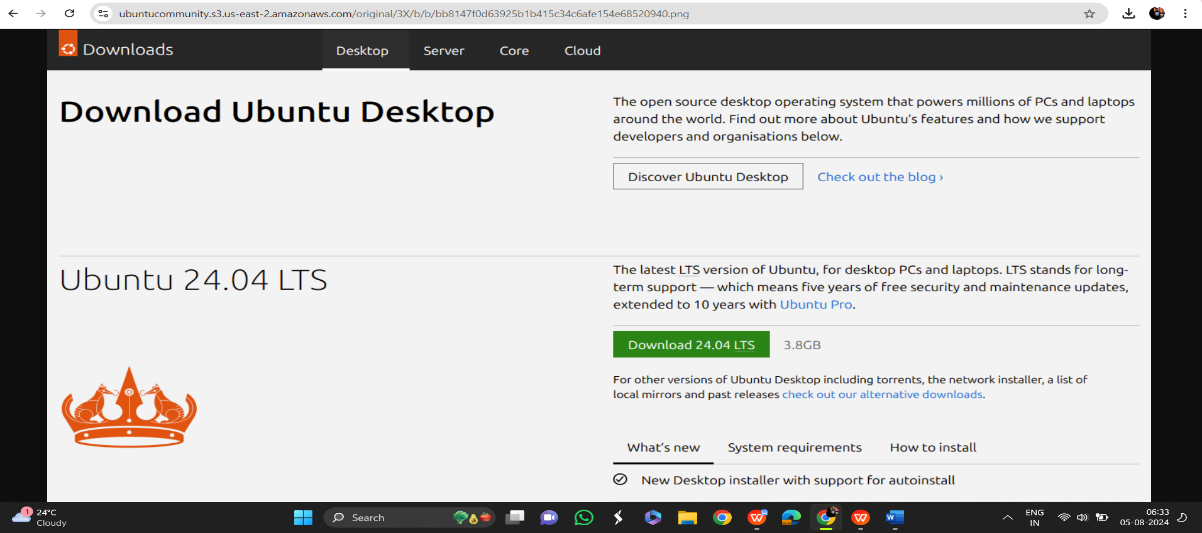
Visit the official VirtualBox website ([https://www.virtualbox.org](https://www.virtualbox.org/?ref=techiemike.com)) and download the latest version compatible with your operating system.

Run the installer and follow the on-screen instructions to complete the installation.

**Step 2:** **Download Ubuntu**

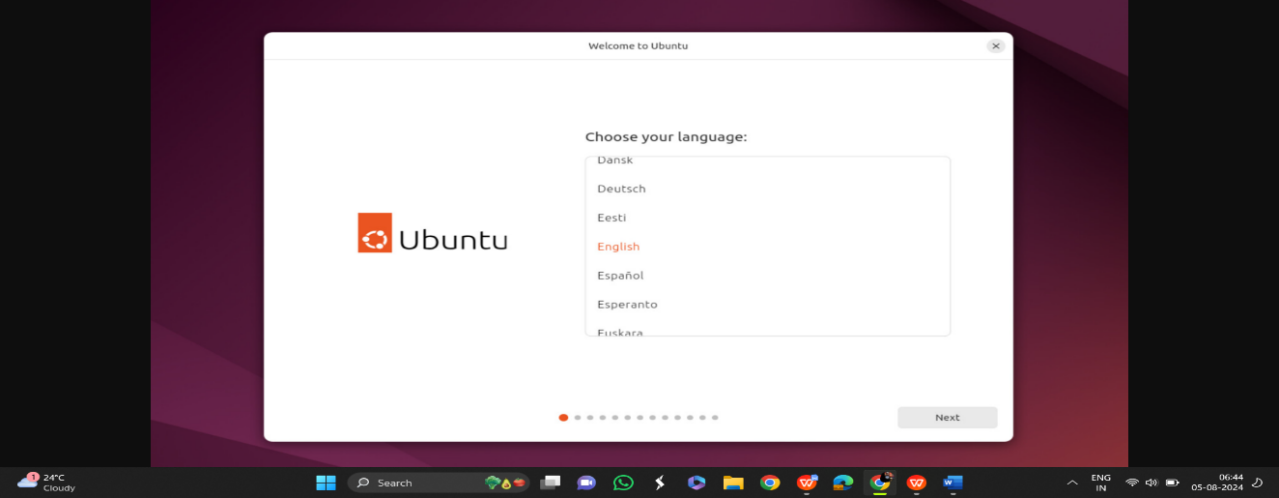
Visit the official Ubuntu website (https://ubuntu.com/) and navigate to the "Download" section.

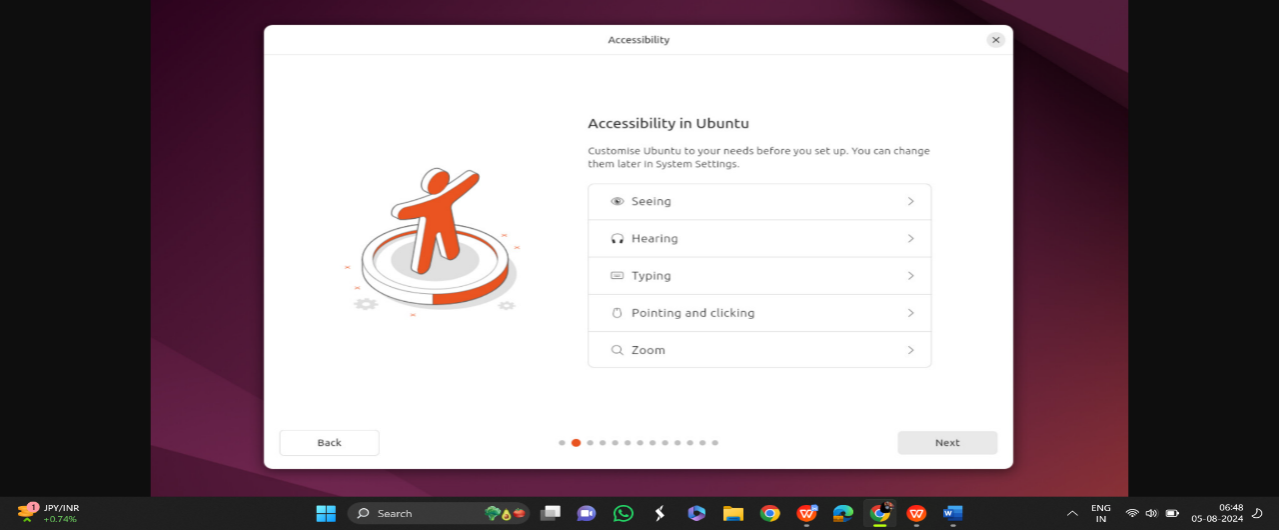
Download the Ubuntu Gateway and Ubuntu Workstation virtual machine images (OVAs) to a location of your choice.

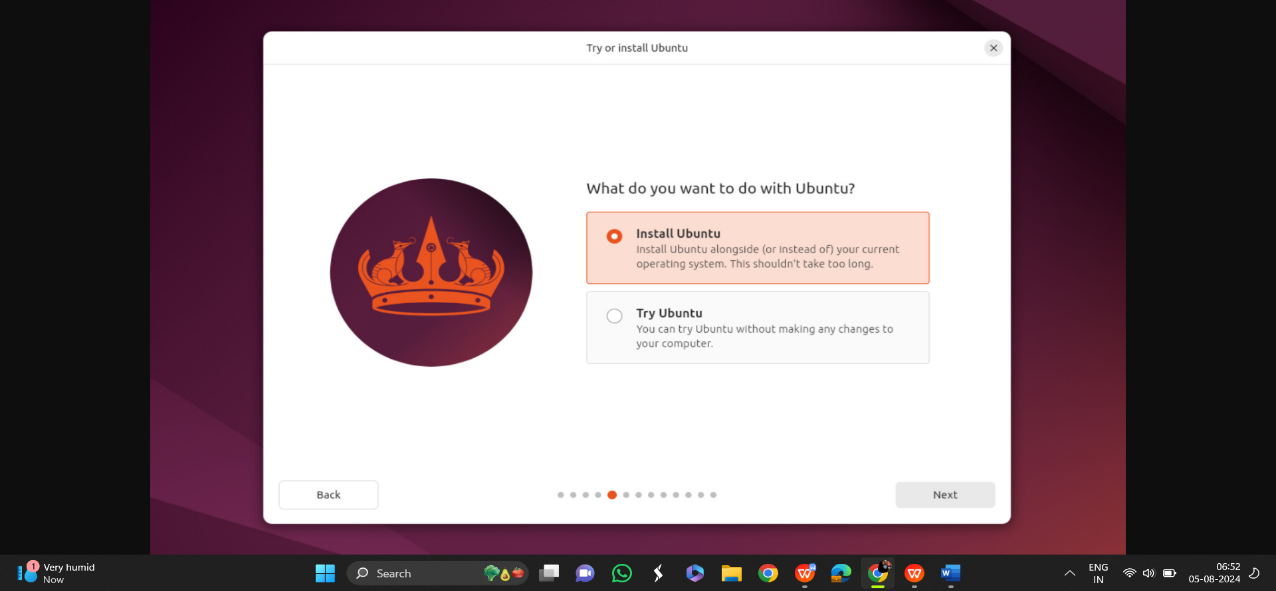


**Step 3:** **Boot from USB flash drive**

Insert the USB flash drive into the laptop or PC you want to use to install Ubuntu and boot or restart the device. It should recognise the installation media automatically. If not, try holding F12 during startup and selecting the USB device from the system-specific boot menu.

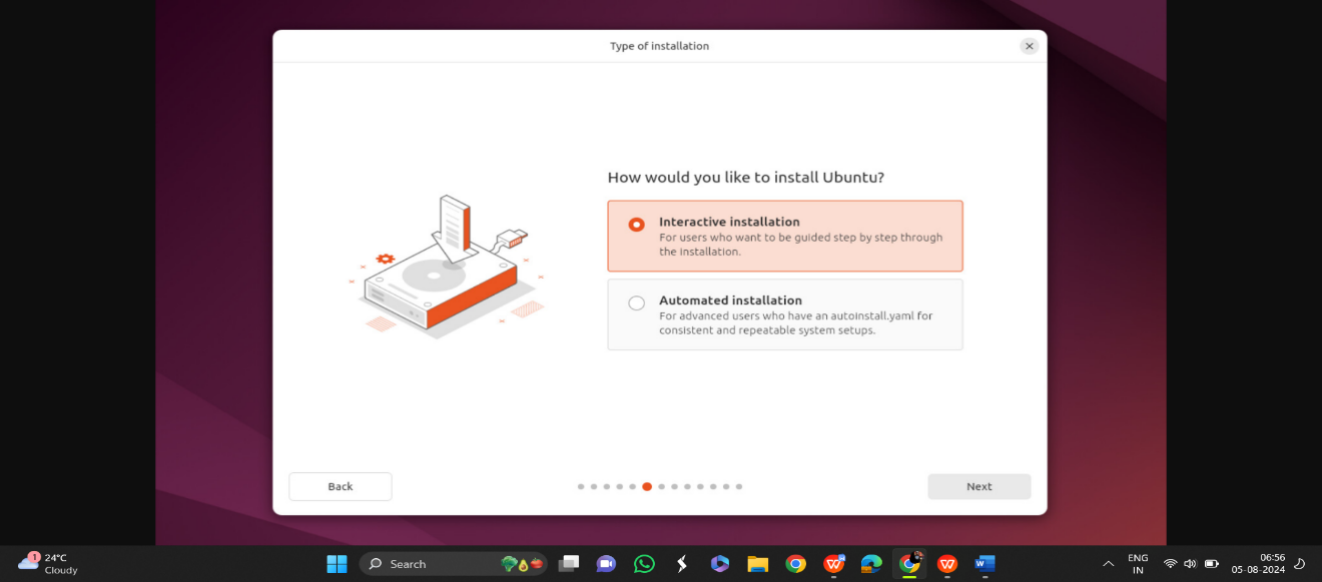






**Step 4:** **Installation Setup**

You will be prompted to choose between **Interactive installation** and **Automated Installation**. The interactive option is the standard route, but more advanced users can use the automated installation option to import a configuration file from a web server to standardise multiple installs and add further customisations. 

****

**Step 5: Configure Ubuntu Workstation**

Select the imported Ubuntu Workstation virtual machine from the VirtualBox Manager.

Click on "Settings" and navigate to the "Network" section.

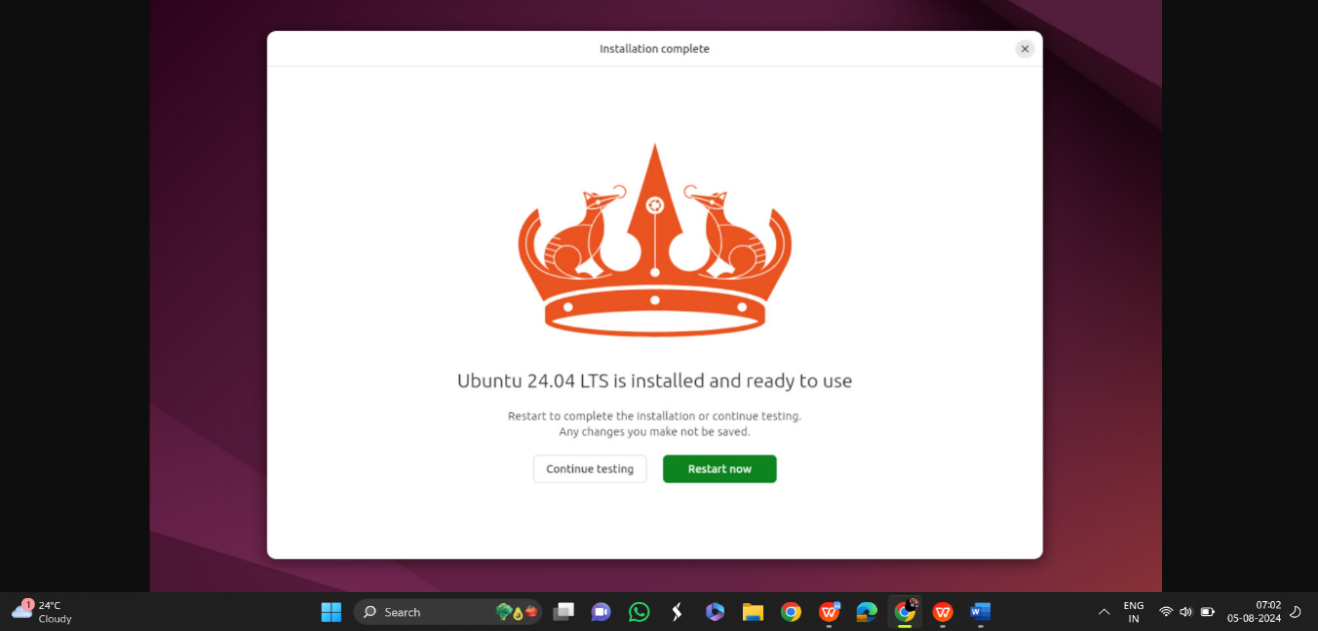
In the "Adapter 1" tab, select "Internal Network" from the "Attached to" dropdown menu. Enter the same internal network name used in the previous step ("Ubuntu-intnet").

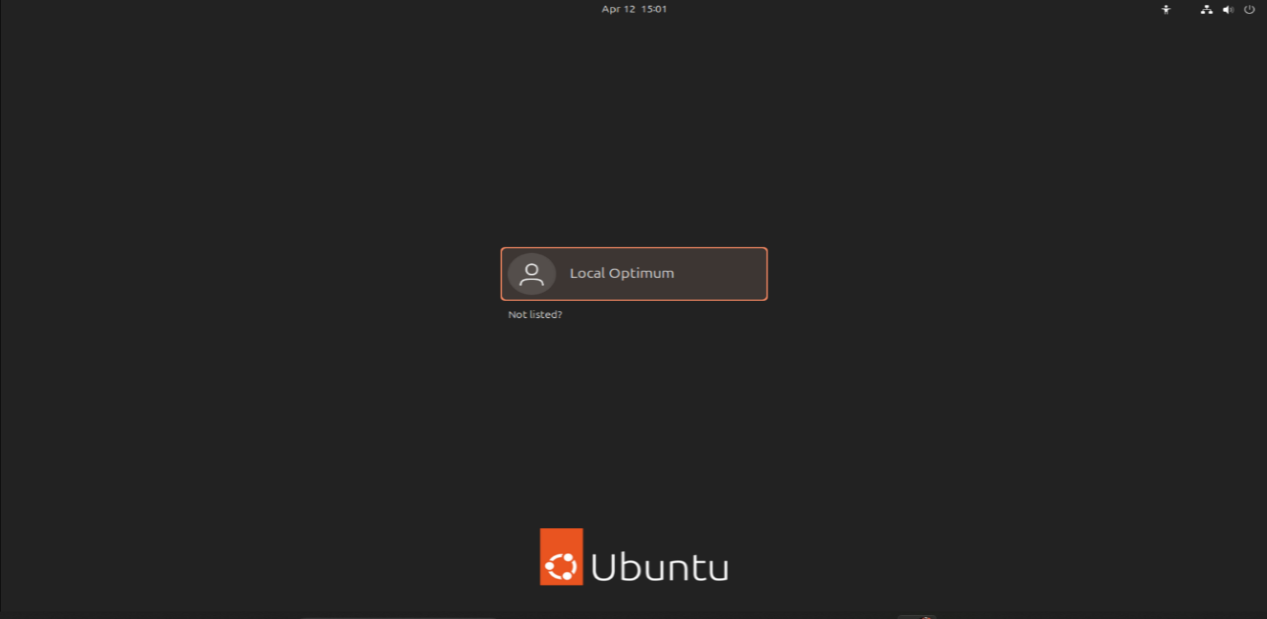
Click "OK" to save the changes.

**Step 6:** **Start Ubuntu**

Start the Ubuntu Gateway virtual machine first by selecting it and clicking on the "Start" button.

Once the Ubuntu Gateway is running, start the Ubuntu Workstation by selecting it and clicking on the "Start" button.





A screenshot of a computer

Description automatically generated

**Conclusion:**  
Setting up Ubuntu provides an effective way to enhance your internet privacy and maintain anonymity while browsing the web. By following the step-by-step instructions outlined in this guide, you can establish a secure environment that routes all network traffic through the Tor network. Remember to exercise caution and adhere to best privacy practices to maximize your online privacy and security. Stay informed and stay safe!