**JEEVAN S U**

**241059038**

**LINUX OS & SCRIPTING**

**M.E – CYBER SECURITY**

**Operating systems used in Cyber Security**

1. **Kali Linux**:

* **It’s Purpose**: It's like a toolbox for security experts.
* **It’s Use**: 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.

1. **Parrot Security OS**:

* **It’s Purpose**: It's like Kali’s laid-back sibling.
* **It’s Use**: 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.

1. **BackBox**:

* **It’s Purpose**: It’s a straightforward security assessment tool.
* **It’s Use**: User-friendly and designed for easy network and vulnerability checking—think of it as a no-fuss option for keeping your system secure.

1. **Tails**:

* **It’s Purpose**: Acts as a cloak of invisibility for your online activities.
* **It’s Use**: Helps you browse the web without leaving traces and keeps your identity anonymous—perfect for when you need to stay under the radar.

1. **Whonix**:

* **It’s Purpose**: Provides double protection for your online actions.
* **It’s Use**: 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**:

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

1. **Ubuntu Server**:

* **It’s Purpose**: A reliable server platform you can customize.
* **It’s Use**: 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**:

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

1. **OpenBSD**:

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

1. **Fedora Security Lab**:

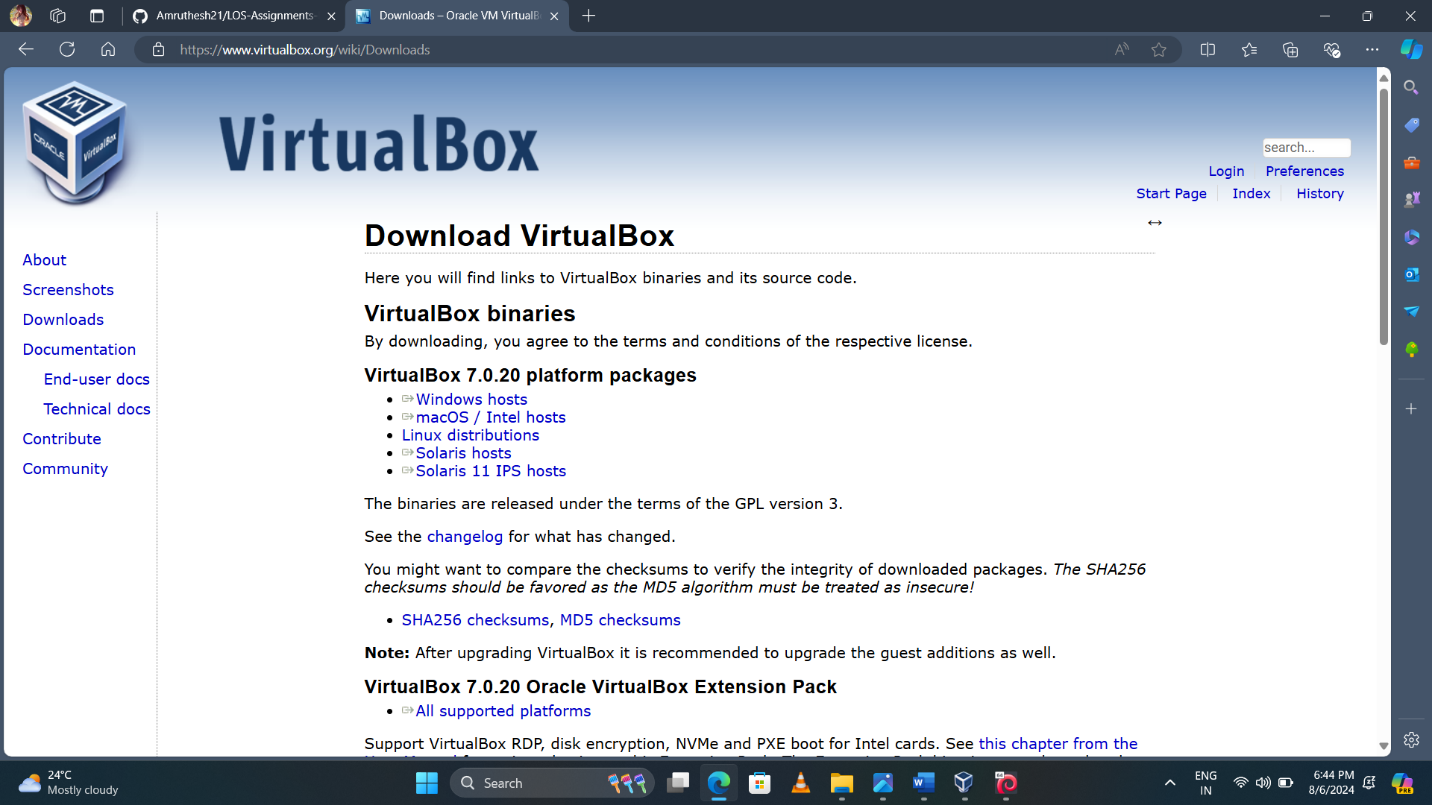
* **It’s Purpose**: A playground for security researchers.
* **It’s Use**: Packed with tools for testing and exploring security issues—think of it as a specialized workshop for diving into cybersecurity challenges.

**Installation Process of Whonix**

**Introduction:**  
In an era where online privacy is increasingly important, Whonix stands out as a powerful tool for maintaining anonymity and securing your online activities. Whonix is an operating system specifically designed to run in a virtual machine and route all network traffic through the Tor network. This tutorial will provide you with a step-by-step guide on how to set up Whonix and enjoy enhanced internet privacy.

**Prerequisites:**

* A computer with virtualization support (Intel VT-x/AMD-V)
* 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.

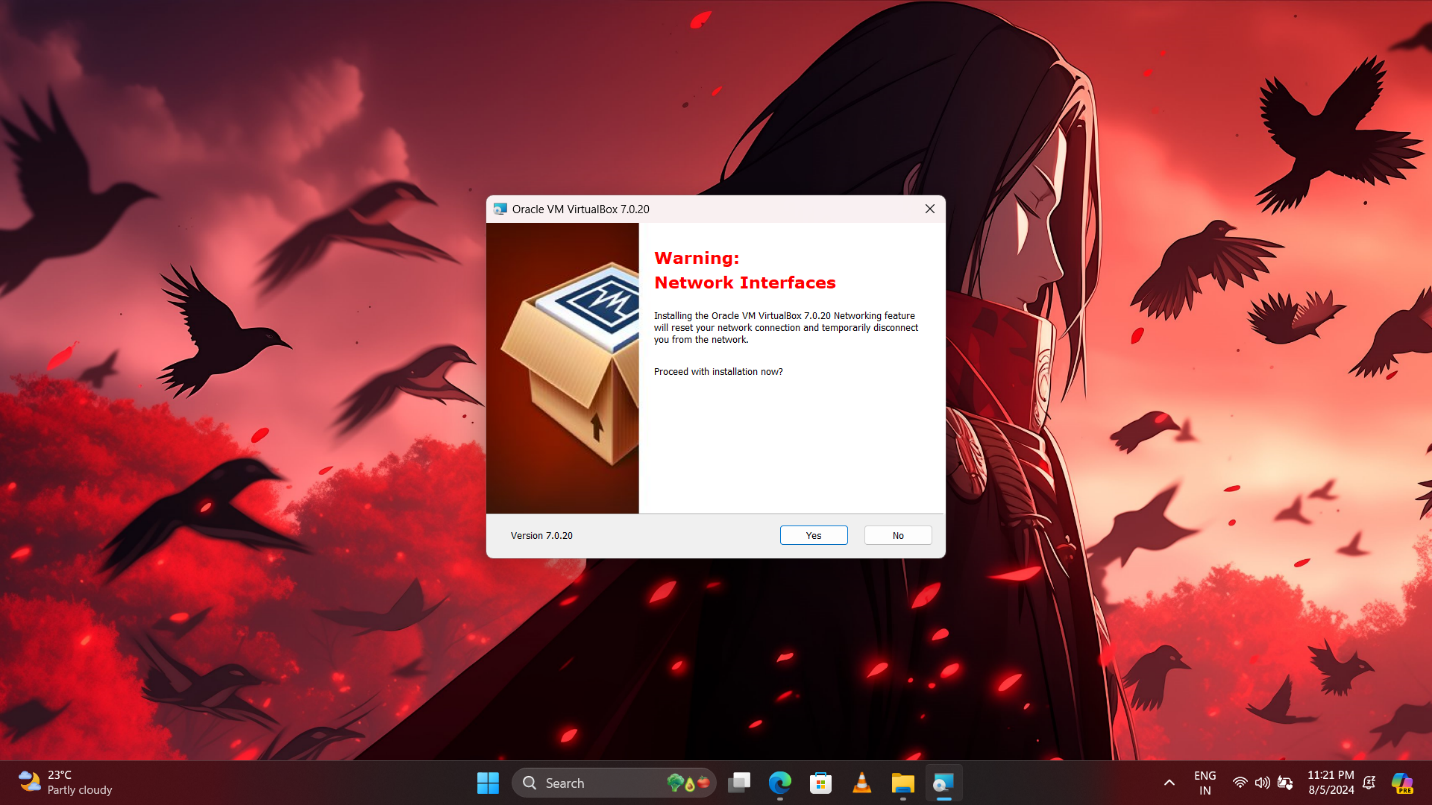
Run the installer and follow the on-screen instructions to complete the installation.



**Step 2:** **Download Whonix**

Visit the official Whonix website ([https://www.whonix.org](https://www.whonix.org/?ref=techiemike.com)) and navigate to the "Download" section.

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



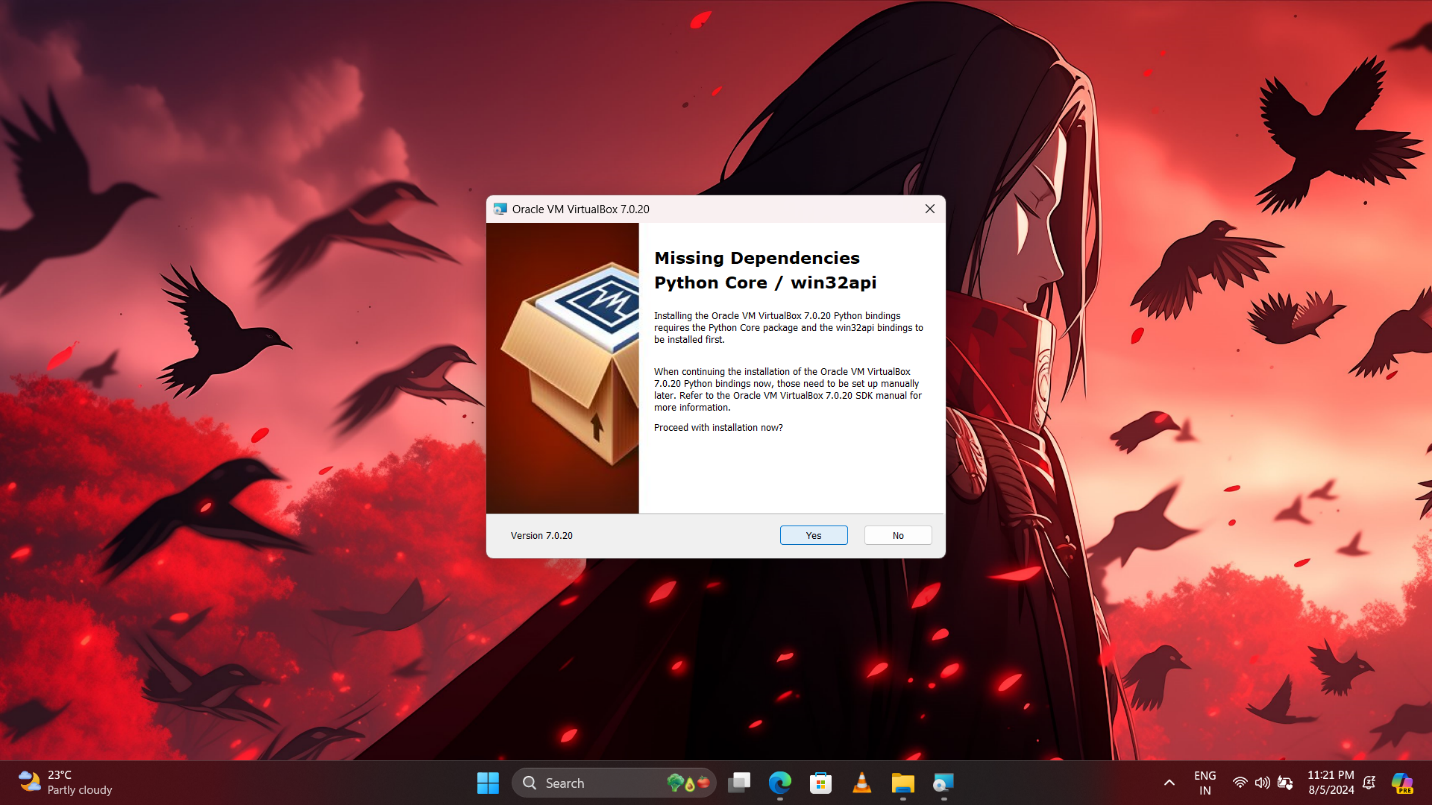
**Step 3:** **Import Whonix into VirtualBox**

Open VirtualBox and click on "File" in the menu bar, then select "Import Appliance."

Choose the Whonix Gateway OVA file you downloaded earlier and click "Next."

Review the import settings and click "Import" to start the process.

Repeat the same steps to import the Whonix Workstation OVA file.



**Step 4:** **Configure Whonix Gateway**

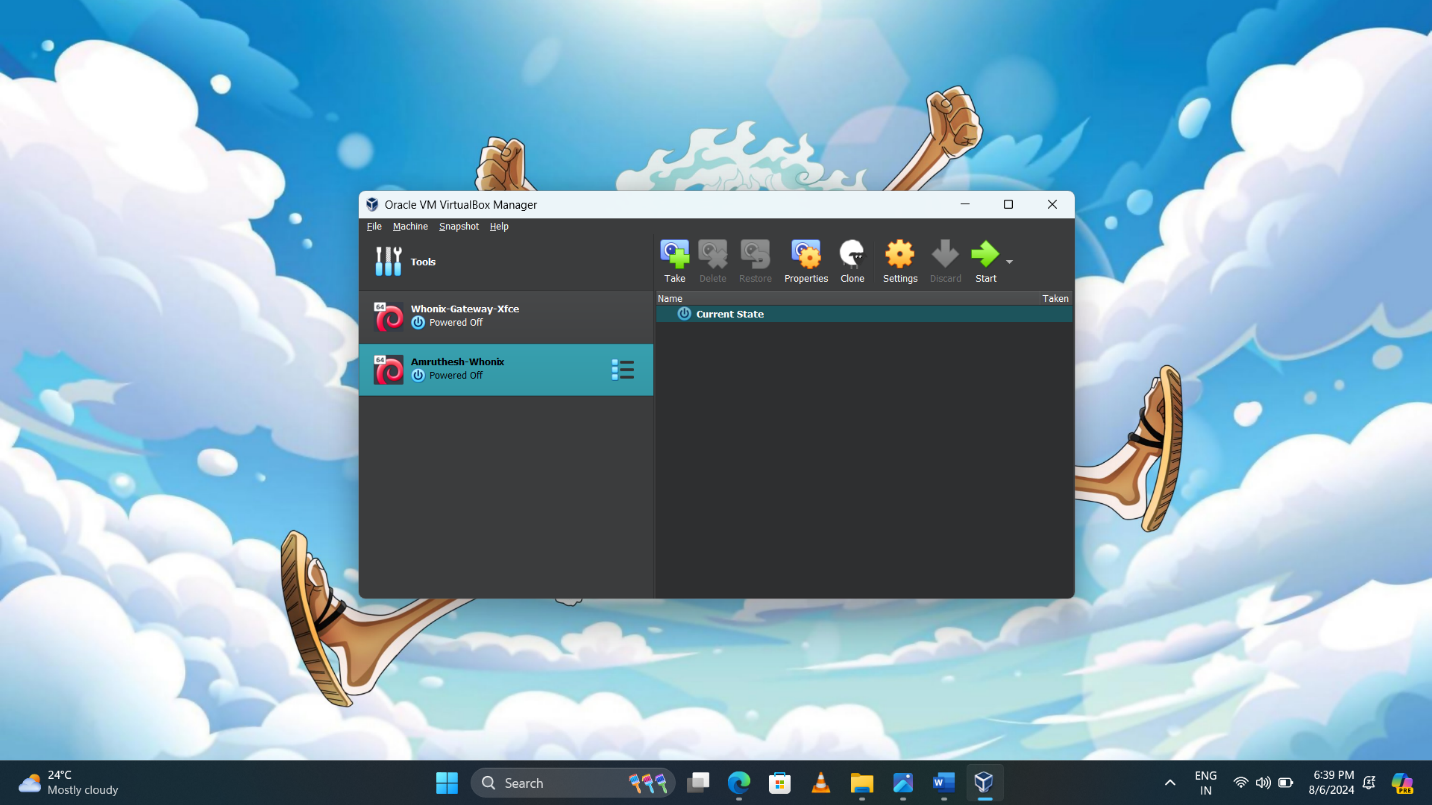
Select the imported Whonix Gateway virtual machine from the VirtualBox Manager.

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

In the "Adapter 1" tab, select "NAT" from the "Attached to" dropdown menu.

In the "Adapter 2" tab, select "Internal Network" from the "Attached to" dropdown menu. Provide a name for the internal network (e.g., "whonix-intnet").

Click "OK" to save the changes.



**Step 5: Configure Whonix Workstation**

Select the imported Whonix 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 ("whonix-intnet").

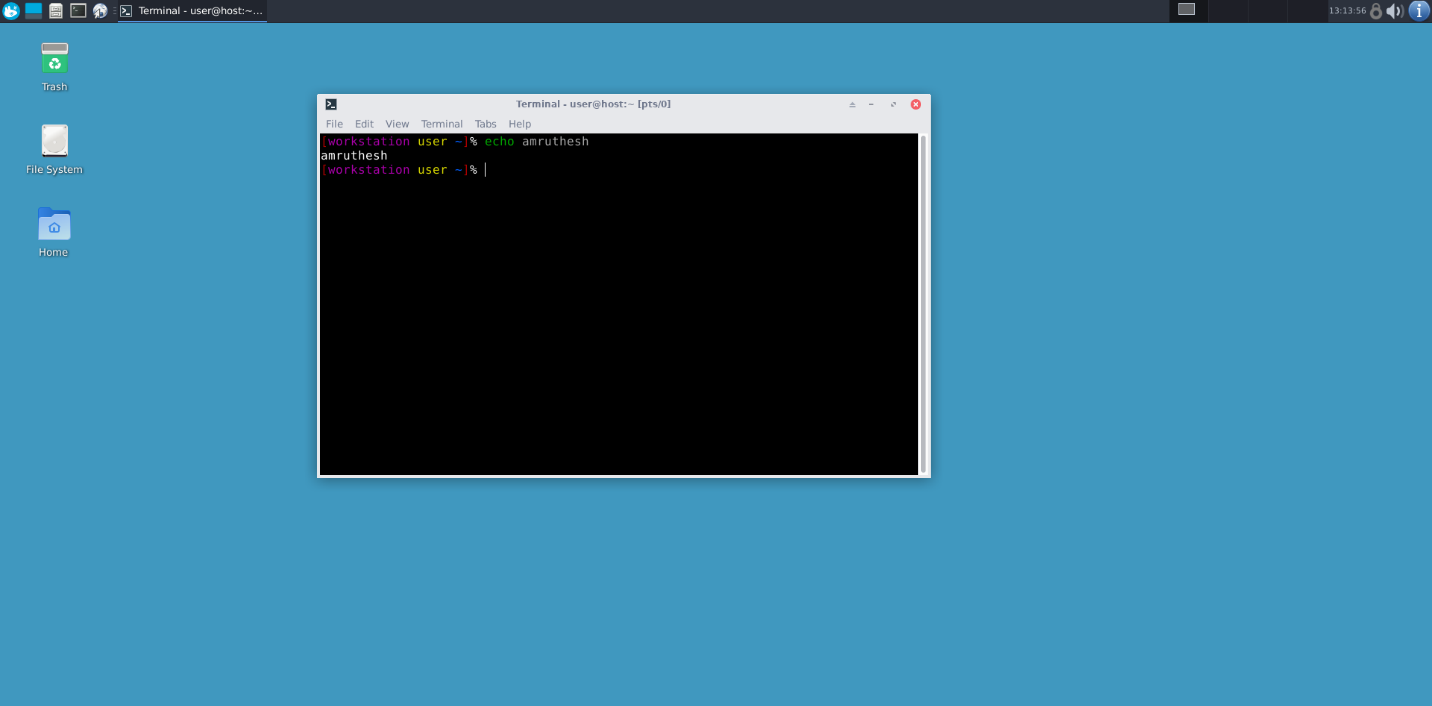
Click "OK" to save the changes.



**Step 6:** **Start Whonix**

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

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



**Step 7:** **Configure Whonix Network Settings**

In the Whonix Workstation, go to the "Applications" menu and click on "Settings."

Open the "Networking" section and ensure that "sys-whonix" is selected as the NetVM.

Verify that "sys-whonix" is connected to the Whonix Gateway by clicking on the "Qubes VM Manager" icon in the system tray.

Confirm that the Whonix Gateway and Whonix Workstation are connected and functioning correctly.

**Conclusion:**  
Setting up Whonix 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!