**OS INSTALLATION**

**Xubuntu:**

Xubuntu is a Linux distribution based on the Ubuntu operating system and designed to be lightweight, fast and efficient. It uses the Xfce desktop environment, which is known for its simplicity and resource efficiency. Xubuntu is suitable for both older hardware and modern systems, providing a balance between performance and a user-friendly experience.

**System Requirements:**

* Minimum 2 GB RAM or more for a smoother experience
* 1 GHz dual-core processor or better.
* Minimum 25 GB of free disk space for installation

**Installation Process:**

Installing Xubuntu Linux as a single operating system using a USB drive involves a series of steps.

**1)Preparing the USB drive:**

* **Downloading Xubuntu ISO:** Visiting the official Xubuntu website and download the ISO file for the latest version.
* **Creating a Bootable USB Drive:** Using tool Rufus to create a bootable USB drive. Following the instructions provided by the tool.

**2)Boot from the USB Drive:**

* **Insert USB Drive:** Plug the USB drive into a USB port on the target system.
* **Restarting the target system:** Restart the target system and during the boot process, pressing the esc key continuously to access the boot menu and F9 key to booting process.
* **Selecting USB drive:** In the boot menu, select the USB drive as the device to boot from which is San disk.

**3) Launch the Xubuntu Installer:**

* **Launch Installer:** On the Xubuntu desktop, there is an icon to install Xubuntu. Double-click that icon to launch the installer.
* **Follow the Installer Wizard:** The Xubuntu installer will guide through the installation process. Choose the language, keyboard layout and other regional settings.

**4)Partitioning and Installation:**

* **Select Installation Type:** Choose the installation type. Since you want to use Xubuntu as the sole operating system. Select the option to “Erase disk and install Xubuntu”.
* **Configure Time Zone:** Setting the time zone
* **Creating User Account:** Creating a user account by providing a username and password.
* **Wait for Installation:** Allow the installer to copy files and complete the installation.

**5) Complete the Installation:**

* **Restarting the system:** Once the installation is complete, the installer will prompt to remove the installation media (USB drive) and press Enter.
* **Boot into Xubuntu:** The system now boot into Xubuntu. If all work is done successfully it will prompt to log in with the user account that is created during the installation.

**6) Post-Installation:**

* **Update system:** Using the following commands to update and upgrade the system.

**“sudo apt update”**

**“sudo apt upgrade”**

Xubuntu uses the Xfce desktop environment which is a lightweight, fast and efficient desktop environment that is known for its simplicity and resource efficiency. It is designed to prove a user-friendly experience without consuming excessive system resources, making it an excellent choice for older or less powerful hardware.

**Installing GNOME in Xubuntu:**

**Step 1:** Install the GNOME desktop environment by using the following command

“sudo apt install ubuntu-desktop”

This command installs the “ubuntu-desktop” package, which includes the GNOME desktop environment along with various default applications.

**Step 2:** During the installation, you might be prompted to choose a display manager. The display manager is responsible for starting the graphical session. You can choose between ‘gdm3’ (GNOME Display Manager) and ‘lightdm’ (Xubuntu’s default display manager). If you want a consistent look, you might want to choose ‘lightdm’.

**Step 3:** After the installation is complete, you need to configure the default session.

**Step 4:** Restart the system to apply the changes. After restarting, it should be able to log in to a GNOME session.

**Anti-Virus:**

Anti-Virus is designed to detect, prevent and remove malicious software (malware) from computer systems.

**Key Points:**

* **Detection Methods:** Antivirus programs use various methods to detect and identify malware. These methods include signature-based detection, behavioral analysis, and cloud-based detection.
* **Signature-Based detection:** This is the traditional method where antivirus software identifies known malware based on specific patterns (signatures). When a file matches a known signature, the antivirus program can quarantine or delete it.
* **Behaviroal Analysis:** Some antivirus programs monitor the behavior of programs in real-time. If a program behaves in a way that is characteristic of malware, the antivirus software may take action to stop or quarantine it.
* **Real Time Protection:** Many antivirus programs offer real-time protection, constantly monitoring the system for potential threats and blocking them as they occur.
* **Firewall integration:** Some antivirus solutions include a firewall to provide an additional layer of protection against unauthorized access and network-based attacks.

**Clam Anti-Virus:**

Clam Anti-Virus known as ClamAV, a popular open-source antivirus toolkit available for multiple platforms, including Linux, Windows and macOS,

**Features:**

* Command-line scanner
* Milter interface for sendmail
* Virus database updated multiple times per day
* Built-in support for all standard mail file formats

**Pros:**

* Open-source and free
* Regular updates
* Lightweight and versatile
* Multi-platform support

**Cons:**

* Limited for zero-day threats and novel malware.
* Limited real-time protection
* Lack of advanced features

**Installing ClamAV:**

**Step 1**: Install the ClamAV utilities by running the following command:

**“sudo apt install clamav clamav-daemon”**

**Step 2:** After the installation , check the version of ClamAV installed by running the following command:

**“clamscan --version”**

**Step 3:** To update the signature database need to stop the freshclam service.

**“sudo systemctl stop clamav-freshclam”**

**Step 4**: Update the signature database by running the freshclam command:

**“sudo freshclam”**

**Step 5:** After the signature database has been updated start the freshclam service

**“sudo systemctl start clamav-freshclam”**

**Scanning with ClamAV:**

1) To scan the /etc/ directory for infected files

**“sudo clamscan -i -r –remove /etc”**

\* -i – prints only infected files

\* --remove – removes infected files

\* --r – recursive scan , all the subdirectories in the directory are scanned

2) To scan the entire system,

**“sudo clamscan -i -r –remove”**

Day – 3

29/12/2023

Friday