Day 1 - Explore the different OS used for Cybersecurity

What is Cybersecurity?

- Cybersecurity focuses on safeguarding computers, networks, and information from unauthorized access or harm. It's similar to securing your home with locks to prevent unwanted visitors, but it's for digital systems.
- **Preventing Unauthorized Access:** Cybersecurity works to block hackers and harmful software from accessing confidential information or systems. This is achieved through methods like firewalls, encryption, and robust passwords to ensure data remains safe.
- **Response and Recovery:** When a security breach occurs, cybersecurity involves having strategies ready to promptly handle and recover from the incident. This process includes identifying the breach, limiting its impact, and restoring affected systems and data.

What is Linux?

- Linux is a free and open-source operating system used as the core for various computer systems. Unlike Windows or macOS, Linux is created and supported by a worldwide network of volunteers and organizations. It is renowned for its flexibility, security, and performance, and it runs on a diverse array of devices, including servers, desktops, smartphones, and embedded systems.
- Linux was developed based on the Intel x86 software architecture and is a leading example of general-purpose software. Today, it is widely used across various devices, including computers, mobile devices, and smart gadgets like televisions.
- Although only about 2.3% of desktop computer users utilize Linux, it is still a valuable choice for particular applications, such as cybersecurity. In fact, there are specialized Linux distributions designed specifically for cybersecurity tasks, as mentioned below.

1) Kali Linux –

- Released on March 13th, 2013, the Kali Linux, formerly known as **Backtrack,** distribution of the Linux operating system was developed by Offensive Security and is derived from the **Debian** distribution of Linux.
- Kali Linux is a tailored Linux distribution aimed at cybersecurity experts and ethical hackers. It includes an extensive array of tools for activities like penetration testing, vulnerability assessment, and digital forensics. Professionals often use Kali Linux to evaluate and protect networks and systems by discovering and mitigating potential security vulnerabilities.

Kali Linux includes several key tools, such as:

- **Nmap**: A tool for scanning networks to identify hosts and services.
- **Metasploit Framework**: A system for creating and running exploit code against target systems.
- **Wireshark**: A network protocol analyser that captures and inspects network traffic.
- **Air crack-ng**: A collection of tools designed for evaluating the security of wireless networks.
- **Burp Suite**: A tool for scanning web applications and identifying security vulnerabilities.
- **John the Ripper**: A tool used for cracking passwords, supporting various encryption formats.
- **Hydra**: A versatile and rapid password cracking tool that works with many different protocols.
- **Nikto**: A scanner that detects security issues and vulnerabilities in web servers.
- **Sql map**: An automated tool for finding and exploiting SQL injection vulnerabilities.
- **Autopsy**: A platform for digital forensics, used for analysing disk images and recovering data.

2) Node Zero -

- Node Zero is a Linux distribution created for penetration testing and security auditing. It offers a suite of tools and utilities to assist security professionals in detecting and resolving vulnerabilities within systems and networks. Node Zero combines both open-source and proprietary tools to support activities like network scanning, vulnerability evaluation, and exploit development. Its objective is to provide a thorough platform for performing security assessments and safeguarding against potential threats.

3) Parrot Security OS –

- Parrot Security OS is a Linux distribution specifically designed for cybersecurity professionals and ethical hackers. It offers a diverse range of tools for activities like penetration testing, vulnerability assessment, digital forensics, and privacy enhancement. By incorporating both open-source and proprietary software, Parrot Security OS helps in securing and analyzing networks and systems. Its goal is to deliver a powerful and adaptable platform for thorough security assessments and effective threat management.

6) Black Arch -

- Black Arch is a Linux distribution tailored for security researchers and penetration testers. Based on Arch Linux, it features an extensive collection of security tools for activities such as vulnerability assessment, network scanning, and exploitation. Black Arch incorporates a wide range of open-source utilities to aid in thorough security evaluations and system analysis. Its aim is to offer a broad and adaptable platform for advanced cybersecurity tasks.

7) CAINE Linux -

CAINE Linux is a Linux distribution specialized in digital forensics and incident response. It comes equipped with an extensive array of tools for forensic analysis, data recovery, and evidence collection. By combining both open-source and proprietary software, CAINE Linux aids in investigating digital evidence and retrieving information from compromised systems. Its goal is to provide a powerful and intuitive platform for performing thorough forensic examinations and handling digital investigations.

Installation of Kali Linux