Different OS used for Cybersecurity:

Operating System:

The operating system is a kind of system software. It essentially manages every aspect of the computer's resources. An operating system serves as an interface between software and various computer components or hardware.

Different OS used for Cybersecurity:

The best OS for cybersecurity can be determined by understanding the OS systems:

1. Kali Linux

It is referred to as a Debian-based Linux system designed for penetration testing techniques and digital forensics. Most frequently, hackers use it. Whole disc encryption is supported by the OS of the system. Forensic work can also be performed with it. It has 20GB of disc space and 2GB of RAM. It is regarded as one of the top operating systems for hacking and cybersecurity.

Features:

- **Live USB Boot:** This is essential for any forensics job since it enables you to install Kali on a USB drive and boot it without touching the host operating system. You can choose the file system Kali uses at startup by using optional persistence volume(s), which enables you to store files between sessions and create various profiles. The ability to encrypt each persistent volume is a crucial component required in our sector.
- **Kali NetHunter:** Kali on your smart watch and Android phone. This includes the NetHunter App, the NetHunter App Store, and a ROM overlay for many devices. In addition, you can boot into the "Kali NetHunter Desktop Experience (KeX)" and a "full desktop" via chroot and containers.
- **Full customisation of Kali ISOs**: A readily accessible ISO customization method and the usage of metapackages tailored to security professional’s specific need sets make it simple to build an optimum version of Kali for your needs.

- **Win-KeX**: With seamless windows, clipboard sharing, audio support, and more, this offers a Kali Desktop Experience for Windows Subsystem for Linux (WSL).
- **Kali Everywhere**: It doesn't matter where you need it—a version of Kali is always with you. Whatever the case, there are several options accessible, such as Bare-Metal (single and multi-boot), Containers (Docker, Podman & LXD), ARM (SBC) (including Raspberry Pis), Virtual Machines (VMware, VirtualBox, Hyper-V, Parallels, Cloud (AWS, Azure, Digital Ocean & Linode), Proxmox & Vagrant), DVD/USB, WSL, and more.
- **Kali Undercover:** Since Kali Undercover blends in with a widely used operating system, most people can use it to prevent shoulder surfing and avoid standing out in a crowd.
- **The Industry Standard**: The indisputable open-source penetration testing platform industry standard is Kali Linux.

2. Parrot Security OS

Another OS, Parrot Security, is based on Debian GNU/Linux and is compatible with Kali Linux and the Frozen Box OS. This operating system facilitates anonymous web browsing, vulnerability assessment, and remediation. It is a lightweight program, and its source code is modifiable, needs 16GB of hard drive space and 320MB of RAM.

Features:

- **Customizable Desktop:** They offer the option to choose between MATE, which is pre-installed by default, and KDE, two distinct desktop environments. For those who are not familiar with Linux jargon, desktop environments can be thought of as the primary user interface (UI) for a Linux distribution.
- **Custom Kernel**: Parrot Security has its own hardened Linux kernel, specifically customized to offer maximum security and resistance to hackers as the initial line of defense, in addition to the extensive library of scripts.

- **Lightweight**: The fact that Parrot OS is comparatively lighter than Kali Linux is one of its main advantages. This indicates that it requires as little as 320MB of RAM to operate properly, requiring a lot less disc space and processing power.
- **Variety of Apps**: Parrot Security has every tool found in Kali Linux, a popular operating system for penetration testing, plus a few more just for good measure. This has been accomplished while maintaining the exact same operating system size across the two operating systems.

3. Cyborg Linux

A security distribution based on Ubuntu called Cyborg is intended for forensic analysis and penetration testing. It is primarily meant for experts and hobbyists who are interested in security, although any Linux user can use it as a desktop system for daily computing needs. A custom-built Linux kernel 3.13.0-40-generic, more than 700 open-source penetration testing tools, and GNOME metacity and compiz Desktop Environment are all pre-installed on Cyborg-Linux in addition to normal Ubuntu software.

Under the code name "Cyborg-Hawk," Cyborg was first made available on December 4, 2014, and it was the most sophisticated, potent, and elegant penetration testing distribution ever made. matched with the best selection of tools available for experts in cyber security and ethical hacking.

Use Cyborg to streamline security in your IT infrastructure. Its true strength comes from the understanding, that a tester needs a robust and effective system that is combined with a stable Linux environment and a robust tool selection.

It offers more than 700 utilities, compared to more than 300 in other well-known distros, plus a menu with specific tools for malware analysis and mobile protection.

Distro Features:-

1. **Forensics**: Identify the digital proof. Look into them and analyse digital information for use in court.

2. **Exploitation Toolkit**: A set of tools for examining your IT infrastructure's consistency. Optimal use of for optimal outcomes.

3. **Reverse Engineering**: Tracing backwards through the development cycle to reverse the analysis's core code.

4. **Mobile Security:** Identify and address any weaknesses in the mobile security system. Mobile Security protects all known smartphone platforms.

5**. Stress Testing**: Find out how much strain your application, device, network, or computer can withstand.

6. **Wifi Security:** Keep your wifi environment safe. Cyborg has advanced tools for assessing your security.

4. BlackArch Linux:

Based on Arch Linux, BlackArch is a penetration testing distro that comes with a ton of security tools. It is an open-source distribution designed with security researchers and penetration testers in mind. More than 2900 tools are available in the repository and can be installed alone or in groups. Installs of Arch Linux that already exist are compatible with BlackArch Linux.

Features of BlackArch

Based on Arch Linux, BlackArch OS is a Linux system made especially for ethical hacking and penetration testing. These are BlackArch OS's five main characteristics:

- **Lightweight**: BlackArch OS is a distribution that is easy to operate on outdated computers or laptops due to its low system requirements.
- **Large Software Repository**: Over 3700 tools for cybersecurity and penetration testing are included in the large software repository that comes with BlackArch OS. To guarantee that users have access to the most recent security tools, the repository is updated on a regular basis.

- **Live ISO**: BlackArch OS may be launched from a live ISO, which eliminates the need to install the program on the host computer and makes it perfect for testing and demonstrations.
- **Community-Driven:** With a committed group of developers and contributors, BlackArch OS is a community-driven project. The community provides free online help to its members and hosts activities on a regular basis.
- **Highly configurable**: BlackArch OS lets users customize the system to meet their own requirements. Numerous desktop environments are available to users, such as Fluxbox, Awesome, Openbox, and more.

5. DEFT Linux

An Ubuntu live Linux CD distribution that has been customized is called DEFT (Digital Evidence & Forensic Toolkit). It's a user-friendly system with some of the greatest open-source incident response and computer forensics programs together with great hardware detection.

DEFT Linux Features:

1. **Open Source Software:** The foundation of DEFT Linux is open source software, which is available for free usage, alteration, and distribution. Because of this, it's a simple option for people and businesses without the funds for expensive software**.**
2. **Security Features:** Numerous security measures in DEFT Linux assist users in safeguarding and securing their data. Data encryption, network scanning and analysis tools, and hardening tools are some of these features.
3. **Digital Forensics Focus:** A Linux distribution created especially for forensics and forensics is called DEFT Linux. It is perfect for professionals working in law enforcement or the cybersecurity industry because it has many of the capabilities and tools required for these duties.

4. **User-Friendly Interface:** DEFT Linux boasts an intuitive interface that is meant to be used by both inexperienced and experienced users, even with its distinct purpose. Users can select the command line interface or the graphical user interface that best suits their needs by using both included in the package.

5. **Live Environment:** Because DEFT Linux operates in a fully live environment, the host cannot alter it. By doing this, malware and other potential security risks on the host will be less likely to exist. Furthermore, Linux is the ideal platform for searching digital evidence because of DEFT, which enables people to examine evidence without altering or properly processing it.

6. BackBox

BackBox is an Ubuntu-based Linux distribution focused on security assessments and penetration tests that offers a toolbox for network and informatic systems investigation. It comes with every tool needed for security testing and ethical hacking.

Backbox Features:

Rich Repository: It comes with a large selection of tools for forensic investigation, vulnerability assessment, penetration testing, and exploitation.

Regular Updates: To guarantee that users have access to the most recent versions, the distribution is updated frequently to incorporate the newest security tools and patches.

User-Friendly Interface: Because of its user-friendly interface, security experts with varying levels of experience can utilize it.

Network Analysis: To assist users in monitoring and analyzing network traffic, tools for network analysis are supplied, such as Wireshark, tcpdump, and others.

Exploitation Tools: Metasploit, Armitage, and other frameworks that assist users in testing and exploiting vulnerabilities are among the many exploitation tools that come with BackBox.

Forensics Tools: Digital forensics tools including Autopsy, Sleuth Kit, and other forensic analysis tools are also included in the download.

Reporting Tools: With BackBox's reporting capabilities, users may create thorough reports of their security evaluations and testing.

Anonymous Testing: Included are features and resources for preserving privacy and anonymity when testing, such as Tor and other anonymization tools.