Operating System for CyberSecurity

List of OS’s used for the CyberSecurity purpose are :

1)Kali Linux:

- The most widely used ethical hacking OS, Kali Linux, is a Debian-based Linux-based operating system.
- It is developed for digital forensics and penetration testing and is financed and maintained by Offensive Security Ltd.
- The Kali Linux for hacking includes the first Nexus device open-source Android penetration test.
- The forensic mode is another outstanding feature of the Kali Linux operating system.

2)BackBox:

- BackBox is a free, open-source community project. It aims to improve and secure the IT environment by fostering a security culture.
- This hacker's OS is more than just an operating system for ethical hacking.
- All this while it was utilizing only free, open-source software, showcasing the community's strength and promise.

3)BlackArch:

- BlackArch is an Arch Linux-based best distro for penetration testers, hacking, and security researchers.
- It is considered the best OS for hacking distribution for security researchers to undertake application-based and web security testing.
- This is because it comes with over 1,600 tools and is a serious rival to Kali Linux and Backbox regarding tool diversity and usability.

4)DEFT Linux:

- Digital Evidence and Forensic Toolkit is an open-source Linux distribution constructed around the DART (Digital Advanced Response Toolkit) software.
- It is based on Ubuntu and includes numerous well-known forensic tools and files useful to ethical hackers, penetration testers, IT security experts, etc.

5) NodeZero Linux:

- NodeZero is a free and open-source Linux distribution for penetration testing.
- This advanced operating system for hacking uses the Ubuntu repositories for updates.
- It includes a collection of fundamental services necessary for performing various tasks and more than 300 penetration testing tools.
- The dual-arch live DVD ISO image of the Linux distribution, which supports 32-bit and 64-bit computing architectures, is available for download.

6)Linux Kodachi:

- Linux Kodachi operating system , which is based on Ubuntu 18.04.6 will give a private, non-forensic, and anonymous operating system that includes all the characteristics that someone who cares about privacy would need to be secure.
- Kodachi is incredibly simple to use- all you need to do is boot it up on your computer using a USB drive.

7)Samurai Web Testing Framework:

- Samurai Web Testing framework is a live Linux system already set up to function as a platform for web pen testing.
- The framework includes various open-source and free hacking tools for finding website weaknesses. For web penetration testing, it is an ideal operating system.

8) Parrot OS:

- Parrot Security OS is built on Debian GNU/Linux. It is integrated with the Frozen Box OS and Kali Linux.
- Additionally, the Frozen Box team intends to use it to offer vulnerability evaluation and mitigation, computer forensics, and anonymous Web browsing.
- Parrot Security OS uses Kali repositories for a variety of package updates and to include new tools.

9) BugTraq:

- BugTraq is a clarification mailing list for in-depth analysis and notification of software security vulnerabilities.
- The foundation of the global security community on the Internet is BugTraq, the best OS for penetration testing.
- A wide range of pen-testing tools are available on Bugtraq, including mobile forensic devices, virus testing labs, tools created by the Bugtraq-Community.

10)Network Security Toolkit(NST) :

- Network Security Toolkit Linux distribution is based on Fedora.
- This bootable live CD aims to access the top open-source network security tools for penetration testing.
- Moreover, this user-friendly hacking distribution turns x86 PCs through an ethical hacking tool used for network traffic sniffing, intrusion detection, network packet creation, network/host scanning, etc.