Day 1 - Explore the different OS used for Cybersecurity (02/08/2024)

What is Cybersecurity?

- Cybersecurity is the **protection** of devices and their associated data from coming into the possession of unauthorized individuals.
- When hackers develop new tactics for circumventing antiviral software or cybersecurity programs, professionals **analyze the tactics** and update the programs to **defend** against the new tactic.
- They even find themselves engaging in **counter-hacking attempts** when the stolen information is sensitive enough to warrant further investigation.

What is Linux?

- Linux is a collection of **open-source,** modular operating systems with a vast array of versions and distributions.
- The Linux family of operating systems is UNIX-like, meaning that they function similarly to the UNIX operating system, which was capable of advanced multitasking.
- It was targeted as software that could power personal devices with the added benefit of serving as an open-source option, making it free for all, amid more prominent and expensive options like the early builds of Windows and Apple's OS.
- Linux was built on the **Intel x86** software architecture concept and remains the most prominent example of general-purpose software. Contemporarily, Linux can be found on computers, mobile devices, and smart devices like televisions.
- While Linux is only used by about 2.3% of all desktop computer users, it remains a viable option for specific tasks, including cybersecurity. In fact, there are even specific Linux distros that are engineered as cybersecurity platforms. Some of those are included 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.
- Unlike other variations of the Linux operating system, Kali Linux's developer is a world-class provider of information security and penetration training.
- When BackTrack was initially released, it was based on the Knoppix distribution of Linux and **focused on security**. When Kali Linux went up, it was with a whole new suite of tools and code.
- The main tools found with Kali Linux are:
    - ➢ **Burp Suite**: A tool for web application penetration testing.
    - ➢ **Wireshark**: A network protocol analysis tool.
    - ➢ **Aircrack-ng**: A wireless cracking tool.
    - ➢ **Hydra**: A tool for online brute force password hacking.
    - ➢ **Maltego**: A tool for intelligence gathering.
    - ➢ **John**: An offline equivalent for Hydra's password cracking.
    - ➢ **Metasploit Framework**: A tool to exploit security weaknesses.
    - ➢ **Owasp-zap**: A tool to find vulnerabilities in applications.
    - ➢ **Nmap**: A network scanner.
    - ➢ **Sqlmap**: A tool to exploit vulnerabilities in SQL injections.

2) NodeZero -

- While the information on who made the NodeZero distribution of Linux is unavailable, it is known that the operating system was originally released on October 6th, 2010.
- NodeZero was built around the **Ubuntu distribution** of the original Linux software as a complete system designed with **penetration testing** in mind. Penetration testing, or ethical hacking, is a key responsibility for those in the cybersecurity industry.
- NodeZero comes with over three hundred tools for penetration testing and security. It also comes with the THC IPV6 Attack Toolkit, which features tools such as live6, dnsdict6, and toobig6 for penetration and security testing.
- Unlike Kali Linux, NodeZero is more of a source code style, making it more difficult to work with if you are not an established user of Linux software

3) Parrot Security OS -

- Another **Debian-based** Linux distribution, Parrot Security (ParrotSec) is a Linux distribution released on the 10th of April in 2013. Parrot Security was created by Lorenzo “Palinuro” Faletra and the Frozenbox team with the goal of creating an operating system for **penetration testing, vulnerability assessment and mitigation, computer forensics, and anonymous browsing**.
- Unlike other Linux operating systems, ParrotSec **combines features** from **Frozenbox** (Another Linux distribution) and **Kali Linux** to create a new operating system.
- One benefit that Parrot Security OS has over Kali Linux is the **anonymity tools**. ParrotSec allows the user to completely **hide their identities** when surfing the Internet and therefore remain relatively **undetectable** when engaging in cybersecurity counterattacks against hack attempts.

4) BlackArch -

- Another **penetration-testing-oriented** distribution of the Linux operating software, BlackArch is functionally like the previously mentioned Parrot Security and Kali Linux distributions.
- Unlike the others, however, BlackArch does **not offer desktop functionality**. Instead, the operating system opts for preconfigured windows in which to process commands.
- Developed by a small group of cybersecurity specialists, the BlackArch software offers over two thousand tools dedicated to penetration testing.
- BlackArch is one of the better interfaces for devices that will only serve a purpose for cybersecurity tools.

5) CAINE Linux -

- An **Ubuntu-based** variation of the Linux software, the Computer-Aided Investigative Environment (CAINE) began development under Giovanni Bassetti in 2008.
- CAINE was created as part of a project for **digital forensics** software, organizing cyber forensic tools with a user-friendly graphical interface.
- CAINE offers several tools to aid in the forensic analysis needed for cybersecurity professionals:

    - ➢ **The Sleuth Kit**: A tool for inputting open-source command lines to execute commands to analyze file systems and disk volume.
    - ➢ **Autopsy**: Serving as the graphical interface for the Sleuth Kit, the Autopsy tool is designed to execute forensic analysis of files and search for specific keywords and web artifacts.
    - ➢ **RegRipper**: A tool that extracts and parses information from files stored in a device.
    - ➢ **Tinfoleak**: A tool dedicated to the analysis of Twitter posts and accounts.
    - ➢ **Wireshark**: This tool collates network traffic, and analyzes data packet captures.
    - ➢ **PhotoRec**: An especially useful tool that facilitates the recovery of deleted files and documents directly from the hard drive.
    - ➢ **Fsstat**: This tool displays the statistical data for images and storage devices.
- As a forensics tool, CAINE is the sort of operating system that would likely see more use among cybersecurity professionals employed by law enforcement agencies.
- Its toolset is dedicated to extracting incriminating information stored on a suspect's personal device. However, the tool can also be useful for those seeking to understand how information is retrieved to develop countermeasures to protect privacy. While CAINE is more likely to be used by professionals, its **user-friendly graphical interface** makes it worthy of consideration for even students looking into this niche sect of cybersecurity.

Installation of Kali Linux