







Important cybersecurity tools

Core cybersecurity knowledge and skills

-  **Video:** Introduction to Linux, SQL, and Python
3 min
-  **Reading:** Use tools to protect business operations
20 min
-  **Practice Quiz:** Test your knowledge: Core cybersecurity knowledge and skills
4 questions
-  **Reading:** Create a cybersecurity portfolio
20 min
-  **Quiz:** Portfolio Activity: Draft a professional statement
5 questions
-  **Reading:** Portfolio Activity Exemplar: Draft a professional statement
10 min

Review: Cybersecurity tools and programming languages

Congratulations on completing Course 1!

Use tools to protect business operations

Previously, you were introduced to programming, operating systems, and tools commonly used by cybersecurity professionals. In this reading, you'll learn more about programming and operating systems, as well as other tools that entry-level analysts use to help protect organizations and the people they serve.

Tools and their purposes

Programming

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. Security analysts use programming languages, such as Python, to execute automation. **Automation** is the use of technology to reduce human and manual effort in performing common and repetitive tasks. Automation also helps reduce the risk of human error.

Another programming language used by analysts is called Structured Query Language (SQL). **SQL** is used to create, interact with, and request information from a database. A **database** is an organized collection of information or data. There can be millions of data points in a database. A **data point** is a specific piece of information.

Operating systems

An **operating system** is the interface between computer hardware and the user. Linux®, macOS®, and Windows are operating systems. They each offer different functionality and user experiences.

Previously, you were introduced to **Linux** as an open-source operating system. Open source means that the code is available to the public and allows people to make contributions to improve the software. Linux is not a programming language; however, it does involve the use of a command line within the operating system. A **command** is an instruction telling the computer to do something. A **command-line** interface is a text-based user interface that uses commands to interact with the computer. You will learn more about Linux, including the Linux kernel and GNU, in a later course.

Web vulnerability

A **web vulnerability** is malicious code or behavior that's used to take advantage of coding flaws in a web application. Vulnerable web applications can be exploited by threat actors, allowing unauthorized access, data theft, and malware deployment.

To stay up-to-date on the most critical risks to web applications, review the [Open Web Application Security Project \(OWASP\) Top 10](#).

Antivirus software

Antivirus software is a software program used to prevent, detect, and eliminate malware and viruses. It is also called anti-malware. Depending on the type of antivirus software, it can scan the memory of a device to find patterns that indicate the presence of malware.

Intrusion detection system

An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. The system scans and analyzes network packets, which carry small amounts of data through a network. The small amount of data makes the detection process easier for an IDS to identify potential threats to sensitive data. Other occurrences an IDS might detect can include theft and unauthorized access.

Encryption

Encryption is the process of converting data from a readable format to a cryptographically encoded format. **Cryptographic encoding** means converting plaintext into secure ciphertext. **Plaintext** is unencrypted information and **secure ciphertext** is the result of encryption. A cryptographic form of code is used to communicate in secret and prevent unauthorized, unapproved access to data, programs, or devices.

Note: Encoding and encryption serve different purposes. Encoding uses a public conversion algorithm to enable systems that use different data representations to share information. Encryption makes data unreadable and difficult to decode for an unauthorized user; its main goal is to ensure confidentiality of private data.

Penetration testing

Penetration testing, also called pen testing, is the act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. It is a thorough risk assessment that can evaluate and identify external and internal threats as well as weaknesses.

Key takeaways

In this reading, you learned more about programming and operating systems. You were also introduced to several new tools and processes. Every organization selects their own set of tools. Therefore, the more tools you know, the more valuable you are to an organization. Tools help security analysts complete their tasks more efficiently and effectively.

Mark as completed

 Like  Dislike  Report an issue