Core cybersecurity knowlege and skills

- Introduction to Linux, SQL, and Python
- Use tools to protect business operations
- Glossary terms from week 4

Introduction to Linux, SQL, and Python

As we discussed previously, organizations use a variety of tools, such as SIEMs, playbooks, and packet sniffers to better manage, monitor, and analyze security threats. But those aren't the only tools in an analyst's toolkit. Analysts also use programming languages and operating systems to accomplish essential tasks.

In this video, we'll introduce you to Python and SQL programming, and the Linux operating system. All of which you'll have an opportunity to practice using later in the certificate program.

Organizations can use programming to create a specific set of instructions for a computer to execute tasks. Programming allows analysts to complete repetitive tasks and processes with a high degree of accuracy and efficiency. It also helps reduce the risk of human error, and can save hours or days compared to performing the work manually. Now that you're aware of what programming languages are used for, let's discuss a specific and related operating system called Linux, and two programming languages: SQL and Python.

Linux is an open-source, or publicly available, operating system. Unlike other operating systems you may be familiar with, for example MacOS or Windows, Linux relies on a command line as the primary user interface. Linux itself is not a programming language, but it does allow for the use of text-based commands between the user and the operating system. You'll learn more about Linux later in the program.

A common use of Linux for entry-level security analysts is examining logs to better understand what's occurring in a system. For example, you might find yourself using commands to review an error log when investigating uncommonly high network traffic.

Next, let's discuss SQL. SQL stands for Structured Query Language. SQL is a programming language used to create, interact with, and request information from a database. A database is an organized collection of information or data. There may be millions of data points in a database. So an entry-level security analyst would use SQL to filter through the data points to retrieve specific information.

The last programming language we'll introduce is Python. Security professionals can use Python to perform tasks that are repetitive and time-consuming and that require a high level of detail and accuracy.

As a future analyst, it's important to understand that every organization's toolkit may be somewhat different based on their security needs. The main point is that you're familiar with some industry standard tools because that will show employers that you have the ability to learn how to use their

tools to protect the organization and the people it serves.
You're doing great! Later in the course, you'll learn more about Linux and programming languages, and you'll practice using these tools in security-related scenarios.

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.

Glossary terms from week 4

Terms and definitions from the certificate

Terms and definitions from Course 1, Week 4

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Database: An organized collection of information or data

Data point: A specific piece of information

Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions

Linux: An open-source operating system

Log: A record of events that occur within an organization’s systems

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network

Order of volatility: A sequence outlining the order of data that must be preserved from first to last

Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks

Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

SQL (Structured Query Language): A programming language used to create, interact with, and request information from a database