Determine the type of attack

Previously, you learned about the eight Certified Information Systems Security Professional (CISSP) security domains. The domains can help you better understand how a security analyst's job duties can be organized into categories. Additionally, the domains can help establish an understanding of how to manage risk. In this reading, you will learn about additional methods of attack. You'll also be able to recognize the types of risk these attacks present.

Attack types

Password attack

A **password attack** is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Some forms of social engineering attacks that you will continue to learn about throughout the program are:

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB (Universal Serial Bus) baiting
- Physical social engineering

Social engineering attacks are related to the security and risk management domain.

Physical attack

A **physical attack** is a security incident that affects not only digital but also physical environments where the incident is deployed. Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

Physical attacks fall under the asset security domain.

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learning technology to conduct attacks more efficiently. Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

Supply-chain attack

A **supply-chain attack** targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them. Supply-chain attacks can fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.

Cryptographic attack

A **cryptographic attack** affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

Cryptographic attacks fall under the communication and network security domain.

Key takeaways

The eight CISSP security domains can help an organization and its security team fortify against and prepare for a data breach. Data breaches range from simple to complex and fall under one or more domains. Note that the methods of attack discussed are only a few of many. These and other types of attacks will be discussed throughout the certificate program.

Resources for more information

To view detailed information and definitions of terms covered in this reading, visit the National Institute of Standards and Technology (NIST) glossary.

Pro tip: If you cannot find a term in the NIST glossary, enter the appropriate search term (e.g., “cybersecurity birthday attack”) into your preferred search engine to locate the definition in another reliable source such as a .edu or .gov site.