

# Wrap-up; terms and definitions from course 5, week 4

Managing threats is a major part of what security professionals do.

In this part of the course, we've explored some common types of cyber threats that you'll likely encounter in the field. Let's review.

We started off discussing social engineering.

You learned that attackers have a variety of ways to trick their targets into sharing private information.

Social engineering techniques rely on exploiting people's trust and willingness to help.

Phishing attacks are one of the most common ways that attackers go about manipulating their targets.

Next, we explored malware.

Here, we discussed the major classes of malware, like viruses, trojans, and worms.

You learned how to spot signs of infection.

You also learned how malware has evolved and become more sophisticated over the years.

After that, we turned our attention to web-based exploits, specifically injection attacks.

You learned about cross-site scripting and SQL injection, two of the most common types of attacks facing organizations online.

We discussed how each of these attacks are carried out.

You also learned about how web applications can be protected from malicious code.

Finally, we explored the threat modeling process.

You learned the process that security teams use to perform these exercises.

Unfortunately, cyberattacks and security breaches are a reality that we're challenged with on a regular basis.

However, being aware of the type of threats that exist and the threat modeling process provides an important foundation for your work as a security analyst.

---

## Glossary terms from week 4

**Angler phishing:** A technique where attackers impersonate customer service representatives on social media

**Advanced persistent threat (APT):** Instances when a threat actor maintains unauthorized access to a system for an extended period of time

**Adware:** A type of legitimate software that is sometimes used to display digital advertisements in applications

**Attack tree:** A diagram that maps threats to assets

**Baiting:** A social engineering tactic that tempts people into compromising their security

**Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder"

**Cross-site scripting (XSS):** An injection attack that inserts code into a vulnerable website or web application

**Cryptojacking:** A form of malware that installs software to illegally mine cryptocurrencies

**DOM-based XSS attack:** An instance when malicious script exists in the webpage a browser loads

**Dropper:** A type of malware that comes packed with malicious code which is delivered and installed onto a target system

**Fileless malware:** Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer

**Hacker:** Any person or group who uses computers to gain unauthorized access to data

**Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment

**Injection attack:** Malicious code inserted into a vulnerable application

**Input validation:** Programming that validates inputs from users and other programs

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

**Loader:** A type of malware that downloads strains of malicious code from an external source and installs them onto a target system

**Malware:** Software designed to harm devices or networks

**Process of Attack Simulation and Threat Analysis (PASTA):** A popular threat modeling framework that's used across many industries

**Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software

**Phishing kit:** A collection of software tools needed to launch a phishing campaign

**Prepared statement:** A coding technique that executes SQL statements before passing them onto the database

**Potentially unwanted application (PUA):** A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software

**Quid pro quo:** A type of baiting used to trick someone into believing that they'll be rewarded in return for sharing access, information, or money

**Ransomware:** Type of malicious attack where attackers encrypt an organization's data and demand payment to restore access

**Reflected XSS attack:** An instance when malicious script is sent to a server and activated during the server's response

**Rootkit:** Malware that provides remote, administrative access to a computer

**Scareware:** Malware that employs tactics to frighten users into infecting their device

**Smishing:** The use of text messages to trick users to obtain sensitive information or to impersonate a known source

**Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables

**Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

**Spyware:** Malware that's used to gather and sell information without consent

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

**SQL injection:** An attack that executes unexpected queries on a database

**Stored XSS attack:** An instance when malicious script is injected directly on the server

**Tailgating:** A social engineering tactic in which unauthorized people follow an authorized person into a restricted area

**Threat:** Any circumstance or event that can negatively impact assets

**Threat actor:** Any person or group who presents a security risk

**Threat modeling:** The process of identifying assets, their vulnerabilities, and how each is exposed to threats

**Trojan horse:** Malware that looks like a legitimate file or program

**Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

**Watering hole attack:** A type of attack when a threat actor compromises a website frequently visited by a specific group of users

**Whaling:** A category of spear phishing attempts that are aimed at high-ranking executives in an organization

**Web-based exploits:** Malicious code or behavior that's used to take advantage of coding flaws in a web application

---

Revision #2

Created 28 August 2023 18:40:54 by naruzkurai

Updated 28 August 2023 18:43:10 by naruzkurai