## Terms and definitions from Course 5

A

**Access controls:** Security controls that manage access, authorization, and accountability of information

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

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

**Algorithm:** A set of rules used to solve a problem

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

**Application programming interface (API) token:** A small block of encrypted code that contains information about a user

**Asset:** An item perceived as having value to an organization

**Asset classification:** The practice of labeling assets based on sensitivity and importance to an organization

**Asset inventory:** A catalog of assets that need to be protected

**Asset management:** The process of tracking assets and the risks that affect them

**Asymmetric encryption:** The use of a public and private key pair for encryption and decryption of data

**Attack surface:** The characteristics and features of the areas where an attack can come from

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

**Attack vector:** The pathways attackers use to penetrate security defenses

B

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

**Basic auth:** The technology used to establish a user’s request to access a server

**Bit:** The smallest unit of data measurement on a computer

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

**Brute force attack:** The trial and error process of discovering private information

**Bug bounty:** Programs that encourage freelance hackers to find and report vulnerabilities

C

**Cipher:** An algorithm that encrypts information

**Common Vulnerabilities and Exposures (CVE®) list:** An openly accessible dictionary of known vulnerabilities and exposures

**Common Vulnerability Scoring System (CVSS):** A measurement system that scores the severity of a vulnerability

**Compliance:** The process of adhering to internal standards and external regulations

**Computer virus:** see “virus”

**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

**Cryptographic key:** A mechanism that decrypts ciphertext

**Cryptography:** The process of transforming information into a form that unintended readers can’t understand

**CVE Numbering Authority (CNA):** An organization that volunteers to analyze and distribute information on eligible CVEs

D

**Data:** Information that is translated, processed, or stored by a computer

**Data at rest:** Data not currently being accessed

**Data in transit:** Data traveling from one point to another

**Data in use:** Data being accessed by one or more users

**Data custodian:** Anyone or anything that’s responsible for the safe handling, transport, and storage of information

**Data owner:** The person that decides who can access, edit, use, or destroy their information

**Defense in depth:** A layered approach to vulnerability management that reduces risk

**Digital certificate:** A file that verifies the identity of a public key holder

**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

E

**Encryption:** The process of converting data from a readable format to an encoded format

**Exploit:** A way of taking advantage of a vulnerability

**Exposure:** A mistake that can be exploited by a threat

F

**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

H

**Hacker:** Any person who uses computers to gain access to computer systems, networks, or data

**Hash collision:** An instance when different inputs produce the same hash value

**Hash function:** An algorithm that produces a code that can’t be decrypted

**Hash table:** A data structure that's used to store and reference hash values

I

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

**Information privacy:** The protection of unauthorized access and distribution of data

**Information security (InfoSec):** The practice of keeping data in all states away from unauthorized users

**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

L

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

M

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

**MITRE:** A collection of non-profit research and development centers

**Multi-factor authentication (MFA):** A technology that requires at least two distinct forms of identification

N

**National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

**Non-repudiation:** The concept that the authenticity of information can’t be denied

O

**OAuth:** An open-standard authorization protocol that shares designated access between applications

P

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

**Payment Card Industry Data Security Standards (PCI DSS):** A set of security standards formed by major organizations in the financial industry

**Personally identifiable information (PII):** Any information used to infer an individual's identity

**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

**Policy:** A set of rules that reduce risk and protect information

**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.( legitimate free Program(freeware) display adds and benefit from these adds, the attacker mix the PUA in the legitimate program and take the benefits to himself and display adds even user refuse)

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

**Principle of least privilege:** The concept of granting only the minimal access and authorization required to complete a task or function

**Procedures:** Step-by-step instructions to perform a specific security task

**Protected health information (PHI):** Information that relates to the past, present, or future physical or mental health or condition of an individual

**Public key infrastructure (PKI):** An an encryption framework that secures the exchange of online information

Q

**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

R

**Rainbow table:** A file of pre-generated hash values and their associated plaintext

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

**Regulations:** Rules set by a government or other authority to control the way something is done

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

**Risk**: Anything that can impact confidentiality, integrity, or availability of an asset

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

S

**Salting:** An additional safeguard that’s used to strengthen hash functions

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

**Security assessment:** A check to determined how resilient current security implementations against threats

**Security audit**: A review of an organization's security controls, policies, and procedures against a set of expectations

**Security controls:** Safeguards designed to reduce specific security risks

**Security hardening:** The process of strengthening a system to reduce its vulnerability and attack surface

**Separation of duties:** The principle that users should not be given levels of authorization that would allow them to misuse a system

**Session:** A sequence of network HTTP basic auth requests and responses associated with the same user

**Session cookie:** A token that websites use to validate a session and determine how long that session should last

**Session hijacking:** An event when attackers obtain a legitimate user’s session ID

**Session ID:** A unique token that identifies a user and their device while accessing a system

**Single sign-on (SSO):** A technology that combines several different logins into one

**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

**Standards:** References that inform how to set policies

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

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

**Symmetric encryption:** The use of a single secret key to exchange information

T

**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

U

**User provisioning:** The process of creating and maintaining a user's digital identity

V

**Virus**: Malicious code written to interfere with computer operations and cause damage to data and software

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

**Vulnerability:** A weakness that can be exploited by a threat

**Vulnerability scanner:** Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network

**Vulnerability assessment:** The internal review process of a company’s security systems

**Vulnerability management:** The process of finding and patching vulnerabilities

W

**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

**Worm:** Malware that can duplicate and spread itself across systems on its own

Z

**Zero-day:** An exploit that was previously unknown