GenCyber Teacher Camp 2022
Cybersecurity Terminology Glossary

(see https://niccs.cisa.gov/about-niccs/cybersecurity-glossary)

access control

Definition: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Adversary

Definition: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

antispyware software

Definition: A program that specializes in detecting and blocking or removing forms of spyware.

antivirus software

Definition: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

Attack

Definition: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Authentication

Definition: The process of verifying the identity or other attributes of an entity (user, process, or device).

Authorization

Definition: A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.

blue Team

Definition: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Bot

Definition: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator.

Botnet

Definition: A collection of computers compromised by malicious code and controlled across a network.

Bug

Definition: An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

Cipher

Synonym(s): cryptographic algorithm

cloud computing

Definition: A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

computer network defense

Definition: The actions taken to defend against unauthorized activity within computer networks.

Confidentiality

Definition: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

critical infrastructure

Definition: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cryptography

Definition: The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cybersecurity

Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

cyber operations

Definition: In the NICE Framework, cybersecurity work where a person: Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

data breach

Definition: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

data integrity

Definition: The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Decryption

Definition: The process of transforming ciphertext into its original plaintext.

- Extended Definition: The process of converting encrypted data back into its original form, so it can be understood.
- Synonym(s): decode, decrypt, decipher

denial of service

Definition: An attack that prevents or impairs the authorized use of information system resources or services.

digital forensics

Definition: The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

electronic signature

Definition: Any mark in electronic form associated with an electronic document, applied with the intent to sign the document.

Encryption

- Definition: The process of transforming plaintext into ciphertext.

- Extended Definition: Converting data into a form that cannot be easily understood by unauthorized people.
- Synonym(s): encode, encrypt, encipher

Exploit

Definition: A technique to breach the security of a network or information system in violation of security policy.

Firewall

Definition: A capability to limit network traffic between networks and/or information systems.

Hacker

Definition: An unauthorized user who attempts to or gains access to an information system.

information assurance

Definition: The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.

information security policy

Definition: An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

information technology

Definition: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Intrusion

Definition: An unauthorized act of bypassing the security mechanisms of a network or information system.

IP Address

Definition: an internet protocol address which is associated with a specific computer or computer network and uniquely identifies it. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

malicious code

Definition: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malware

Definition: Software that compromises the operation of a system by performing an unauthorized function or process.

Synonym(s): malicious code, malicious applet, malicious logic

passive attack

Definition: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Password

Definition: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

penetration testing

Definition: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing

Definition: A digital form of social engineering to deceive individuals into providing sensitive information.

Plaintext

Definition: Unencrypted information.

private key

Definition: A cryptographic key that must be kept confidential and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

public key

Definition: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

public key infrastructure

Definition: A framework consisting of standards and services to enable secure, encrypted communication and authentication over potentially insecure networks such as the Internet.

Rootkit

Definition: A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges, and conceal the activities conducted by the tools.

security policy

Definition: A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets.

software assurance

Definition: The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

Spam

Definition: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spoofing

Definition: Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.

Extended Definition: The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

Spyware

Definition: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

symmetric cryptography

Definition: A branch of cryptography in which a cryptographic system or algorithms use the same secret key (a shared secret key).

system administration

Definition: In the NICE Framework, cybersecurity work where a person: Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability; also manages accounts, firewalls, and patches; responsible for access control, passwords, and account creation and administration.

threat assessment

Definition: The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

trojan horse

Definition: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus

Definition: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Worm

Definition: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

VPN (virtual private network)

Definition: an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.