

# Glossary

## Cybersecurity



---

### Terms and definitions from Course 3

#### A

**Active packet sniffing:** A type of attack where data packets are manipulated in transit

**Address Resolution Protocol (ARP):** Used to determine the MAC address of the next router or device to traverse

#### B

**Bandwidth:** The maximum data transmission capacity over a network, measured by bits per second

**Baseline configuration:** A documented set of specifications within a system that is used as a basis for future builds, releases, and updates

**Bluetooth:** Used for wireless communication with nearby physical devices

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

#### C

**Cloud-based firewalls:** Software firewalls that are hosted by the cloud service provider

**Cloud computing:** The practice of using remote servers, application, and network services that are hosted on the internet instead of on local physical devices

**Cloud network:** A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet

**Controlled zone:** A subnet that protects the internal network from the uncontrolled zone

## D

**Data packet:** A basic unit of information that travels from one device to another within a network

**Denial of service (DoS) attack:** An attack that targets a network or server and floods it with network traffic

**Distributed denial of service (DDoS) attack:** A type of denial of service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic

**Domain Name System (DNS):** A networking protocol that translates internet domain names into IP addresses

## E

**Encapsulation:** A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

## F

**File Transfer Protocol (FTP):** Used to transfer files from one device to another over a network

**Firewall:** A network security device that monitors traffic to or from your network

**Forward proxy server:** A server that regulates and restricts a person's access to the internet

## H

**Hardware:** The physical components of a computer

**Hub:** A network device that broadcasts information to every device on the network

**Hypertext Transfer Protocol (HTTP):** An application layer protocol that provides a method of communication between clients and website servers

**Hypertext Transfer Protocol Secure (HTTPS):** A network protocol that provides a secure method of communication between clients and servers

## I

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

**IEEE 802.11 (Wi-Fi):** A set of standards that define communication for wireless LANs

**Internet Control Message Protocol (ICMP):** An internet protocol used by devices to tell each other about data transmission errors across the network

**Internet Control Message Protocol (ICMP) flood:** A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server

**Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network

**Internet Protocol (IP) address:** A unique string of characters that identifies the location of a device on the internet

**IP spoofing:** A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network

## L

**Local area network (LAN):** A network that spans small areas like an office building, a school, or a home

## M

**Media Access Control (MAC) address:** A unique alphanumeric identifier that is assigned to each physical device on a network

**Modem:** A device that connects your router to the internet and brings internet access to the LAN

**Multi-factor authentication (MFA):** A security measure that requires a user to verify their identity in two or more ways to access a system or network

## N

**Network:** A group of connected devices

**Network log analysis:** The process of examining network logs to identify events of interest

**Network protocols:** A set of rules used by two or more devices on a network to describe the order of delivery of data and the structure of data

**Network segmentation:** A security technique that divides the network into segments

## O

**Operating system (OS):** The interface between computer hardware and the user

**Open systems interconnection (OSI) model:** A standardized concept that describes the seven layers computers use to communicate and send data over the network

**On-path attack:** An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit

## P

**Packet sniffing:** The practice of capturing and inspecting data packets across a network

**Passive packet sniffing:** A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network

**Patch update:** A software and operating system update that addresses security vulnerabilities within a program or product

**Penetration testing:** A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes

**Ping of death:** A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB

**Port:** A software-based location that organizes the sending and receiving of data between devices on a network

**Port filtering:** A firewall function that blocks or allows certain port numbers to limit unwanted communication

**Proxy server:** A server that fulfills the requests of its clients by forwarding them to other servers

## R

**Replay attack:** A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time

**Reverse proxy server:** A server that regulates and restricts the Internet's access to an internal server

**Router:** A network device that connects multiple networks together

## S

**Secure File Transfer Protocol (SFTP):** A secure protocol used to transfer files from one device to another over a network

**Secure shell (SSH):** A security protocol used to create a shell with a remote system

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

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

**Security zone:** A segment of a company's network that protects the internal network from the internet

**Simple Network Management Protocol (SNMP):** A network protocol used for monitoring and managing devices on a network

**Smurf attack:** A network attack performed when an attacker sniffs an authorized user's IP address and floods it with ICMP packets

**Speed:** The rate at which a device sends and receives data, measured by bits per second

**Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats

**Stateless:** A class of firewall that operates based on predefined rules and that does not keep track of information from data packets

**Subnetting:** The subdivision of a network into logical groups called subnets

**Switch:** A device that makes connections between specific devices on a network by sending and receiving data between them

**Synchronize (SYN) flood attack:** A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

## T

**TCP/IP model:** A framework used to visualize how data is organized and transmitted across a network

**Transmission Control Protocol (TCP):** An internet communication protocol that allows two devices to form a connection and stream data

**Transmission control protocol (TCP) 3-way handshake:** A three-step process used to establish an authenticated connection between two devices on a network

## U

**Uncontrolled zone:** The portion of the network outside the organization

**User Datagram Protocol (UDP):** A connectionless protocol that does not establish a connection between devices before transmissions

## V

**Virtual Private Network (VPN):** A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet

## W

**Wide Area Network (WAN):** A network that spans a large geographic area like a city, state, or country

**Wi-Fi Protected Access (WPA):** A wireless security protocol for devices to connect to the internet

---