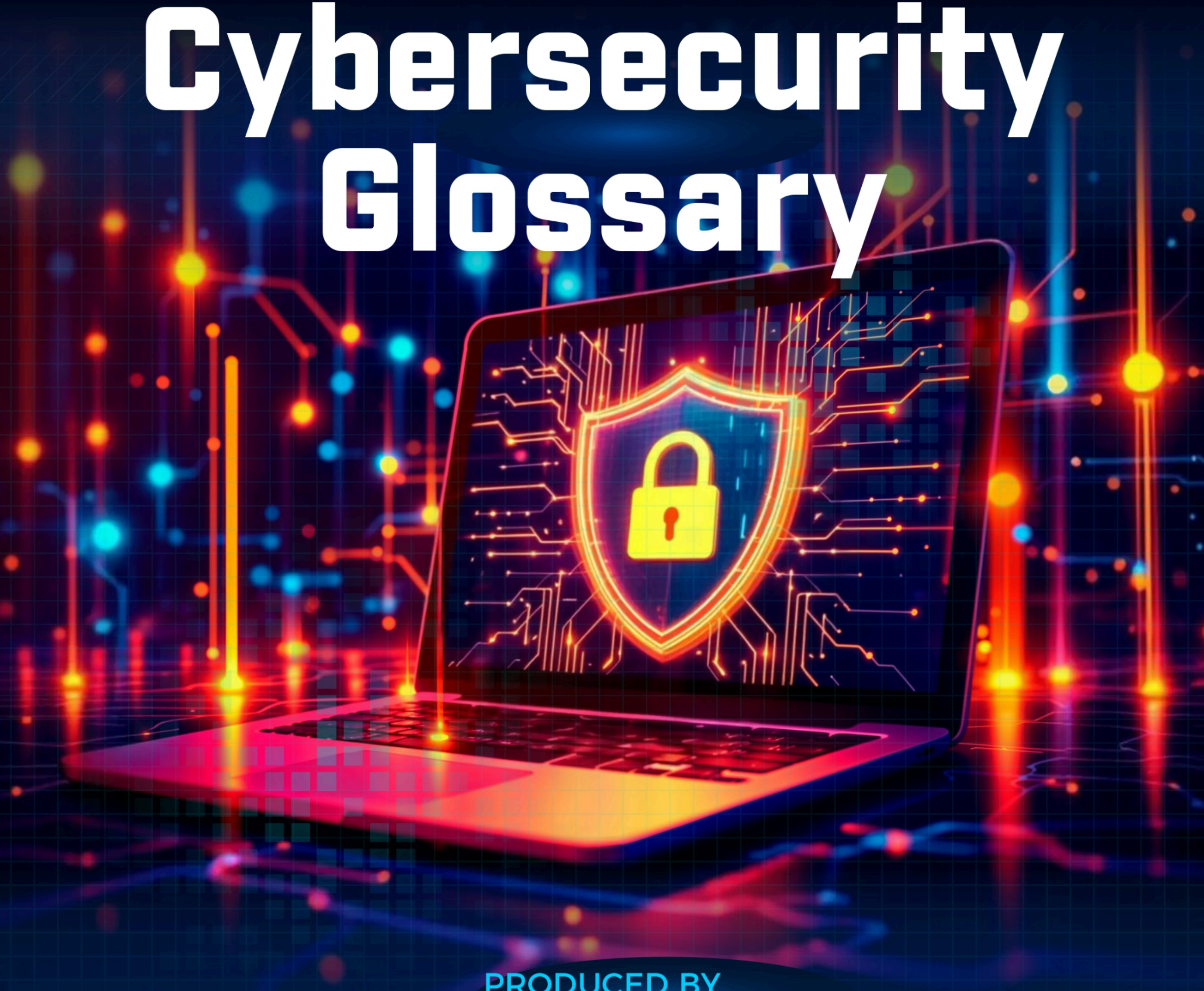
Cybersecurity Glossary



PRODUCED BY

Cyber Gear

www.cyber-gear.ai

A

ACCESS CONTROL

A security technique that regulates who or what can view, use, or change resources in a computing environment. It is a fundamental concept designed to minimize risk by enforcing policies.

ADVANCED PERSISTENT THREAT (APT)

A prolonged and targeted cyberattack in which an intruder gains unauthorized access to a network and remains undetected for an extended period. The goal is typically data theft or espionage rather than causing immediate damage.

ADVERSARY

An entity or individual that attacks or is a threat to a system. Also commonly known as a Threat Actor.

ADWARE

Software designed to display unwanted advertising on a device. While not always malicious, it can be a privacy concern and sometimes acts as a vector for more harmful malware.

ANTIVIRUS

A type of software designed to detect, prevent, and remove malicious software, such as viruses, worms, and trojans, from computers and networks.

ASSET

Any data, device, or other component of the environment that supports information-related activities. In cybersecurity, assets are what must be protected.

ATTACK SURFACE

The sum of all possible points (or "attack vectors") where an unauthorized user can try to enter data into or extract data from an environment.

AUDIT TRAIL

A chronological record of system activities that enables the reconstruction and examination of the sequence of events and/or changes in an event. It's used for security analysis, accountability, and diagnostics.

AUTHENTICATION

The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Common methods include passwords, biometrics, and security tokens.

AUTHORIZATION

The process of granting or denying specific permissions to an authenticated user. While authentication confirms who you are, authorization determines what you are allowed to do.

B

BACKDOOR

A covert method of bypassing normal authentication or encryption in a computer, product, or embedded device. It may be built-in for legitimate purposes, but can also be created by attackers for unauthorized access.

BACKUP

A copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Regular backups are a critical defense against ransomware.

BASELINE

A standardized level of performance or security configuration for a system or network. Baselines are used as a reference point to measure and detect deviations or changes that could indicate a security incident.

BIOMETRICS

Authentication techniques that rely on measurable physical or behavioral characteristics that are unique to an individual. Examples include fingerprints, facial recognition, iris scans, and voice patterns.

BLACKLIST

A list of entities (such as IP addresses, email addresses, or applications) that are explicitly denied access or permission to a system or network. The opposite of a whitelist.

BLUE TEAM

The group responsible for defending an enterprise's information systems against attack. They are tasked with maintaining the defensive security posture and responding to security incidents.

BOTNET

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, for example, to send spam or conduct Distributed Denial-of-Service (DDoS) attacks.

BRUTE-FORCE ATTACK

A trial-and-error method used to obtain information such as a user password or PIN. In an exhaustive search, automated software runs through all possible combinations until the correct one is found.

BUFFER OVERFLOW

A type of software vulnerability that occurs when a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This can be exploited by attackers to execute arbitrary code.

BUG

An error, flaw, or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. Security bugs can lead to vulnerabilities.

BUSINESS CONTINUITY PLAN (BCP)

A comprehensive plan that outlines the procedures and instructions an organization must follow in the face of a disaster, whether man-made or natural. It covers business processes, assets, human resources, and business partners to ensure operations can continue.

C

CERTIFICATE (DIGITAL)

An electronic document used to prove the ownership of a public key. It includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct.

CIA TRIAD

A foundational model in information security representing its three core goals: Confidentiality (preventing unauthorized disclosure), Integrity (preventing unauthorized modification), and Availability (ensuring access when needed).

CLOUD SECURITY

A sub-domain of cybersecurity dedicated to securing cloud computing systems. This includes protecting data, applications, and infrastructure involved in cloud computing.

COMPLIANCE

The act of adhering to, and being able to demonstrate adherence to, mandated requirements defined by laws, regulations, standards, or policies.

CRACKER

An individual who attempts to break into computer systems, typically with malicious intent. Unlike a hacker, the term "cracker" is used exclusively for malicious actors.

CRYPTOGRAPHY

The practice and study of techniques for secure communication in the presence of third parties, called adversaries. It involves creating and analyzing protocols that prevent malicious third parties from reading private messages.

CROSS-SITE SCRIPTING (XSS)

A type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users.

CYBERCRIME

Criminal activity that either targets or uses a computer, a computer network, or a networked device.

CYBERSECURITY

The practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

CIPHER

An algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.

CRITICAL INFRASTRUCTURE

The assets, systems, and networks, whether physical or virtual, that are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economy, public health, or safety.

D

DATA BREACH

An incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.

DATA LOSS PREVENTION (DLP)

A set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

DECRYPTION

The process of converting encrypted data (ciphertext) back into its original, readable form (plaintext).

DENIAL-OF-SERVICE (DOS) ATTACK

A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

A DoS attack where the incoming traffic flooding the victim originates from many different sources, making it more difficult to stop the attack by simply blocking a single source.

DIGITAL SIGNATURE

A mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient very strong reason to believe that the message was created by a known sender (authentication) and that the message was not altered in transit (integrity).

DIGITAL FORENSICS

The branch of forensic science encompassing the recovery and investigation of material found in digital devices, often concerning computer crime.

DNS SPOOFING

A type of cyberattack whereby a malicious actor redirects traffic from a legitimate website to a fake one by corrupting the Domain Name System (DNS) records.

DRIVE-BY DOWNLOAD

The unintentional download of software to a computer or mobile device. A user can be visiting a legitimate but compromised website, and malware is downloaded without their knowledge or consent.

DWELL TIME

The period between when a cyberattack first infiltrates a network and when it is detected. Reducing dwell time is a key objective for security teams.

E

ENCRYPTION

The process of converting information or data (plaintext) into a code (ciphertext), especially to prevent unauthorized access.

ENDPOINT SECURITY

The practice of securing endpoints or entry points of end-user devices, such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns.

ETHICAL HACKING

The practice of intentionally penetrating a computer system or network to find security vulnerabilities that a malicious attacker could potentially exploit. The ethical hacker has permission from the asset owner.

EVENT LOG

A file that contains a record of events that occur on a computer system. Security event logs are used to track user activities and diagnose operational problems.

EXPLOIT

A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

EXPLOIT KIT

A software kit designed to run on web servers, to identify software vulnerabilities in client machines communicating with it, and exploiting discovered vulnerabilities to upload and execute malicious code on the client.

EAVESDROPPING

The act of secretly listening to the private communication of others without their consent. In cybersecurity, this refers to intercepting data packets as they travel across a network.

EXPOSURE

A state in a computing system in which a vulnerability is known or used by an adversary.

F

FIREWALL

A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

FILE INTEGRITY MONITORING (FIM)

A security process that tests and checks operating system, database, and application software files to determine if they have been tampered with or corrupted.

FALSE POSITIVE

An alert that incorrectly indicates that a particular condition or attribute is present. In cybersecurity, it's a security alert that is triggered when there is no actual threat.

FALSE NEGATIVE

A result that incorrectly indicates that a particular condition or attribute is absent. In cybersecurity, it is the failure of a security system to detect a real, active threat.

FIRMWARE

Permanent software programmed into a read-only memory. It is a specific class of computer software that provides the low-level control for a device's specific hardware.

FUZZING

An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions.

FINGERPRINTING

The process of collecting detailed information about a remote computer system to identify its operating system, software versions, and network configuration.

G

GOVERNANCE

The set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

GRAY HAT

A computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

GUEST NETWORK

A separate network access point provided for temporary visitors or non-employees. It provides internet access but restricts access to the organization's primary internal network.

GUIDELINE

A recommendation or suggestion that indicates a specific course of action is advisable, but not mandatory.

H

HACKER

An individual who uses computer, networking, or other skills to overcome a technical problem. The term also may refer to a person with an advanced understanding of computers and computer networks. The term is often used in a negative context, but can also refer to ethical hackers.

HASH FUNCTION

A function that converts an input of letters and numbers into an encrypted output of a fixed length. Hashing is a one-way function used to ensure data integrity.

HONEYPOT

A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. It is a decoy system designed to be an attractive target for attackers.

HARDENING

The process of securing a system by reducing its surface of vulnerability. This involves removing unnecessary software, changing default passwords, and applying security patches.

HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)

An intrusion detection system that is installed on a specific computer or device (a "host") to monitor its internal activity for signs of malicious behavior.

I

INCIDENT RESPONSE (IR)

An organized approach to addressing and managing the aftermath of a security breach or cyberattack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

INFORMATION SECURITY

The practice of protecting information by mitigating information risks. It is part of the broader field of cybersecurity but focuses specifically on protecting data assets, regardless of their form.

INTEGRITY

A core principle of the CIA Triad. It refers to maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

INTRUSION DETECTION SYSTEM (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

IP SPOOFING

The creation of Internet Protocol (IP) packets with a forged source IP address, to conceal the identity of the sender or impersonate another computing system.

IDENTITY AND ACCESS MANAGEMENT (IAM)

A framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities. It ensures the right individuals access the right resources at the right times for the right reasons.

INDICATOR OF COMPROMISE (IOC)

A piece of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.

J

JAILBREAKING

The process of removing software restrictions imposed by the manufacturer on devices running the iOS operating system. It allows users to install applications and customizations not available through the official Apple App Store.

JITTER

The variation in the time delay of received packets in a network. In security, analyzing network jitter can sometimes be used to infer the presence of network congestion or certain types of attacks.

JAVASCRIPT INJECTION

A type of attack where malicious JavaScript code is injected into a website's client-side to be executed by the victim's browser. This is a common method for achieving Cross-Site Scripting (XSS).

K

KEY

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. It is used in conjunction with an algorithm to encrypt and decrypt data.

KEYLOGGER

A type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. It can be used by employers to monitor employee activity or by malicious actors to steal passwords and other sensitive information.

KEY MANAGEMENT

The management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys.

KERBEROS

A computer network authentication protocol that works based on 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

(CYBER) KILL CHAIN

A model developed by Lockheed Martin that describes the stages of a cyberattack, from early reconnaissance to the final goal of data exfiltration or system damage. The stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives.

L

LEAST PRIVILEGE

A security concept requiring that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose.

LOG ANALYSIS

The process of reviewing, interpreting, and understanding computer-generated records called logs. In security, log analysis is crucial for detecting security incidents, troubleshooting issues, and conducting forensic investigations.

LATERAL MOVEMENT

The techniques that a cyber attacker uses to progressively move through a network as they search for key assets and data. After gaining initial access, an attacker moves laterally to expand their foothold and escalate their privileges.

LOGIC BOMB

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer might hide a piece of code that starts deleting files if they are ever terminated from the company.

M

MALWARE

Malicious software specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It is a collective term for viruses, worms, trojans, ransomware, spyware, etc.

MAN-IN-THE-MIDDLE (MITM) ATTACK

An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

MULTI-FACTOR AUTHENTICATION (MFA)

A security process that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

METASPLOIT

A popular and powerful penetration testing framework that makes hacking simpler for attackers and defenders alike. It provides information about security vulnerabilities and aids in developing and executing exploit code.

MOBILE SECURITY

The protection of smartphones, tablets, and other portable devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

MITIGATION

The action of reducing the severity, seriousness, or painfulness of something. In cybersecurity, mitigation refers to the steps taken to reduce the impact of a security incident or the severity of a vulnerability.

N

NETWORK SECURITY

A broad term that covers a multitude of technologies, devices, and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies.

NETWORK ADDRESS TRANSLATION (NAT)

A method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. It can provide a layer of security by hiding internal IP addresses from the public internet.

NETWORK ACCESS CONTROL (NAC)

An approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement.

NMAP (NETWORK MAPPER)

A free and open-source utility for network discovery and security auditing. It is used by network administrators and security professionals to identify what devices are running on their systems, discovering hosts and services, and detecting security vulnerabilities.

NON-REPUDIATION

The assurance that someone cannot deny the validity of something. In digital security, non-repudiation provides proof of the origin, integrity, and delivery of data, making it difficult for a sender to later deny having sent the message.

O

OPEN SOURCE INTELLIGENCE (OSINT)

Intelligence collected from publicly available sources. In the cybersecurity context, OSINT is used by both attackers for reconnaissance and defenders for threat intelligence.

OFFENSIVE SECURITY

The practice of proactively finding security vulnerabilities by simulating the methods of an attacker. It includes disciplines like penetration testing and red teaming.

ON-PREMISES

Software and technology that is located within the physical confines of an enterprise—often in the company's own data center—as opposed to running remotely on hosted servers or in the cloud.

OWASP TOP 10

The Open Web Application Security Project's (OWASP) Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

P

PATCH

A piece of software code designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs.

PENETRATION TESTING (PEN TEST)

An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

PHISHING

A type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

POLICY (SECURITY)

A document that outlines the rules, expectations, and procedures for security within an organization. It defines what is and is not allowed.

PORT SCANNING

An attack that sends client requests to a range of server port addresses on a host, to find an active port and exploit a known vulnerability of that service.

PROXY SERVER

A server application that acts as an intermediary between a client requesting a resource and the server providing that resource. It can be used for security, logging, and caching.

PURPLE TEAM

A collaborative function where an organization's red team (offensive) and blue team (defensive) work together to maximize the effectiveness of security testing and improve overall security posture.

PRIVILEGE ESCALATION

The act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Q

QUARANTINE

The process of isolating a file or program that is suspected of being infected with a virus in a specific area of a disk to prevent it from contaminating other files. It is a common feature of antivirus software.

R

RANSOMWARE

A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

RED TEAM

The group that plays the role of an adversary, attempting to penetrate an organization's defenses to identify vulnerabilities. Their work is a key part of offensive security.

RESILIENCE

The ability of an organization to prepare for, respond to, and recover from cyberattacks. It goes beyond simple prevention to ensure business continuity.

RISK ASSESSMENT

The process of identifying, analyzing, and evaluating risks. In cybersecurity, this involves identifying assets, threats, and vulnerabilities to determine the likelihood and impact of a security incident.

ROOTKIT

A clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence.

REMOTE ACCESS TROJAN (RAT)

A type of malware that allows a remote attacker to have full control over a victim's machine.

S

SANDBOX

A security mechanism for separating running programs, usually to mitigate system failures or software vulnerabilities from spreading. It is often used to safely execute and analyze suspicious code.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

A solution that provides real-time analysis of security alerts generated by applications and network hardware. It collects, aggregates, and analyzes log data to identify security threats.

SNIFFING T

The process of capturing and monitoring traffic flowing on a network. Attackers use sniffers to capture data packets containing sensitive information like passwords.

SOCIAL ENGINEERING

The art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick you into giving them your passwords or bank information.

SPEAR PHISHING

A highly targeted phishing attack that uses personalized information about the victim to make the fraudulent email or message appear more legitimate.

SPOOFING

An attack in which a person or program successfully masquerades as another by falsifying data to gain an illegitimate advantage.

SPYWARE

Malware that secretly observes the computer user's activities without permission and reports it to the software's author.

SQL INJECTION (SQLI)

A code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g., to dump the database contents to the attacker).

SSL/TLS (SECURE SOCKETS LAYER/TRANSPORT LAYER SECURITY)

Cryptographic protocols designed to provide communications security over a computer network. They are widely used for securing web traffic (HTTPS).

SYMMETRIC ENCRYPTION

A type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information.

T

THREAT ACTOR

An entity that is partially or wholly responsible for an incident that impacts or has the potential to impact an organization's security. Also known as an Adversary.

THREAT INTELLIGENCE

Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

TOKENIZATION

The process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a "token," that has no extrinsic or exploitable meaning or value.

TROJAN HORSE

A type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.

TUNNELING

A protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network through a process called encapsulation. VPNs use tunneling.

TWO-FACTOR AUTHENTICATION (2FA)

A type, or subset, of multi-factor authentication. It is a method

U

UNPATCHED

Refers to a system or software that has not had a necessary security patch applied, leaving it vulnerable to known exploits.

USER ACCOUNT CONTROL (UAC)

A mandatory access control enforcement feature introduced with Microsoft's Windows Vista and Windows Server 2008 operating systems. It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation.

URL FILTERING

A security feature used to restrict or control the content a user is permitted to access on the web. It is commonly used by organizations to prevent employees from accessing malicious or inappropriate websites.

USB BAITING

A social engineering attack where an attacker leaves a malware-infected USB drive in a public place, hoping a curious individual will pick it up and plug it into their computer.

V

VIRUS

A type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros to execute its code.

VULNERABILITY

A weakness which can be exploited by a threat actor to perform unauthorized actions within a computer system.

VIRTUAL PRIVATE NETWORK (VPN)

A technology that creates a safe and encrypted connection over a less secure network, such as the public internet. A VPN is a way to extend a private network across a public network.

VULNERABILITY ASSESSMENT

The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

W

WEB APPLICATION FIREWALL (WAF)

A firewall that monitors, filters, or blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that it can filter the content of specific web applications while regular firewalls serve as a safety gate between servers.

WHALING

A specific type of phishing attack that targets high-profile employees, such as the CEO or CFO, to steal sensitive information from a company, as they have access to more sensitive data than lower-level employees.

WHITELIST

A list of entities, such as applications or IP addresses, that are explicitly allowed access to a system or network. Any entity not on the list is blocked.

WI-FI SECURITY

The protection of devices and networks connected via Wi-Fi. This includes protocols like WPA2 and WPA3 that encrypt traffic between devices and the wireless router.

WORM

A standalone malware computer program that replicates itself to spread to other computers. It often uses a computer network to spread itself, relying on security failings on the target computer to access it.

WIRESHARK

A free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Y

YARA

A tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA, you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

Z

ZERO-DAY EXPLOIT

An attack that exploits a previously unknown security vulnerability in a computer application or operating system. It is called "zero-day" because the developer has had zero days to create a patch to fix the flaw.

ZERO TRUST ARCHITECTURE

A security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter. It requires verification of every person and device trying to access resources.

ZOMBIE

A computer connected to the Internet that has been compromised by a hacker, computer virus, or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets are often networks of zombie computers.

Cyber Gear

www.cyber-gear.ai