Cyber Security Glossary

A

**Access Control**

The means and mechanisms of managing access to and use of resources by users.

**Active Directory**

Microsoft's proprietary directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources

**Arbitrary code execution**

An attacker’s ability to /execute arbitrary commands/ or /code/ on a target machine or in a target process

**Authentication**

The process of proving an individual is a claimed identity.

**Authorization**

The security mechanism determining and enforcing what authenticated users are authorized to do within a computer system

**Automated code review**

Software that /check source code for compliance within a predefined set of rules/ and/or best practices

**Availability**

Authorized users that can freely access the systems, networks, and data needed to perform their daily tasks

B

**Backup**

A duplicate copy of data on a separate physical storage device or online/cloud storage solution

**Biometrics**

A method of user authentication that uses biological features such as fingerprints, facial structure or voice profiles.

**Brute force attack**

An attack based on repeated attempts with variating inputs to break into a secured system

**Business Email Compromise (BEC)**

A type of scam targeting companies who conduct wire transfers and have suppliers abroad

C

**Countermeasure**

An action taken to counteract a potential or imminent danger / threat

**Cracking**

An unauthorised attack on computers, networks and technology

**Client**

The user’s end of a network request

**Cyclic Redundancy Check (CRC)**

A method to ensure data has not been altered after being sent through a communication channel

**Cross Site Scripting (XSS)**

Cross-Site Scripting is a security flaw found in some Web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the Web application.

**Credentials**

Verification of identity or tools for authentication.

This bit needs to be reduced T-T

**Confidentiality, Integrity and Availability (CIA) \_*TRIAD\_***

*Confidentiality*

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

*Integrity*

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

*Availability*

Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

High availability systems are the computing resources that have architectures that are specifically designed to improve availability. Based on the specific HA system design, this may target hardware failures, upgrades or power outages to help improve availability, or it may manage several network connections to route around various network outages.

D

**Data Protection**

A process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets.

**Data Integrity**

The assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so

**Distributed Denial of Service (DDoS) Attack**

An attack that floods an active service with bogus requests from multiple locations

**Dictionary Attack**

An attack that uses a predefined list of commonly used or previously captured passwords to attempt access to a secured device or file

**Domain Name System (DNS)**

The system used to derive IP addresses from Domain Names.

It’s basically the phonebook of the internet :D

E

**Encryption**

A mathematical calculation used to encode and secure data

F

**Flooding**

A type of DDoS where a SYN is sent however the ACK is not thus wasting the server’s resources

**Firewall**

Hardware or software designed to prevent unauthorised access to a computer or network

G

**Gap Analysis**

The comparison of actual performance against expected or required performance

H

**Hacking**

The method of gaining unauthorised access to hardware of software

**Handshakes**

**Hash**

A mathematical calculation used to get a quasi-unique string from the input

**Hosts**

Devices connected to a system

**Host Intrusion Detection System (HIDS)**

An intrusion detection system that is installed and running on a host system rather than or in conjunction with the network

**HyperText Transfer Protocol (HTTP)**

The protocol used to transfer data over a network

**HyperText Markup Language (HTML)**

The language used to write websites

**Hybrid Attack**

An attack that uses a predefined dictionary that also tests permutations of the provided data such as replacing letters and numbers or adding numbers where commonly used

I

**Internet Protocol (IP)**

A connectionless protocol, which means that each unit of data is individually addressed and routed from the source device to the target device, and the target does not send an acknowledgement back to the source.

**Intellectual Property (IP)**

Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights.

**Internet of Things (IoT)**

Devices connected to the internet

**Intrusion Detection System (IDS)**

A system in place to detect unusual or attacks on a network.

**Integrity of Data**

See *data integrity*

J

K

L

**Linux**

An open source kernel developed by Linus Torvalds that is POSIX compliant used in the majority of servers and low power devices

M

**Man in the Middle Attack**

A method of intercepting trust from a source and guest by acting as a 3rd party brokering the connection.

**Manual code review**

The act of a human checking code written by a developer

**Malware**

Short for malicious software

N

**National Cyber Security Centre (NCSC)**

An organisation of the United Kingdom Government that provides advice and support in how to avoid computer security threats.

**National Security**

The security and defence of a nation state, including its citizens, economy, and institutions, which is regarded as a duty of government.

**Network Intrusion Detection System (NIDS)**

An intrusion detection system that is installed on network management devices such as a switch, router or firewall.

**Non-repudiation**

Associating actions or changes with a unique individual.

(e.g.: Giving another person your password to perform actions on your behalf is a breach of ToS)

O

**Operating system security**

Systems in place to prevent privilege escalation and only provide authorised access to the system resources.

**Operational Security (OPSec)**

A risk management process that encourages managers to view  operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands.

P

**Penetration Testing (Pen Testing)**

**Phishing Attack**

A social engineering attack used to steal user data where the attacker poses as a trusted entity to acquire information.

**Privacy of Data**

Ensuring only authorised users have access to their content

**Privilege escalation**

Gaining more privileges to a system beyond what you should have

Q

R

**Reusable password**

Passwords that are fixed until changed by the user

**Risk Management**

The process of performing a risk assessment and evaluating the responses to risk in order to mitigate or otherwise handle the identified risks

**Ransomware**

A form of malware that holds a victim's data hostage on their computer typically through robust encryption

**Round Trip Time (RTT)**

S

**Secure coding techniques / standards**

Secure coding is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities

**Security Information and Event Management System (SIEM)**

A formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security violating events

**Security threat**

A malicious act that seeks to damage data, steal data, or disrupt digital life in general

**Security Patches**

An update or change or an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities

**Social engineering attack**

An attempt to gain sensitive information or gain access to a system by manipulating people. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information

**Software security**

**Spoofing**

**Secure Socket Layer (SSL)**

**Single Point of Failure**

**Sliding Window Technique**

**Static Packet FIltering**

**Stateful Packet Inspection**

**Super Account / Super User (root)**

**Supplicant**

T

**Transport Connection Protocol (TCP)**

**Timeout**

**Two-factor Authentication**

U

V

**Virtual Private Network (VPN)**

**Verifier**

W

X

Y

Z

END OF SECTION