- **Spoofing** – the act of falsifying or manipulating data, information, or communication to deceive or trick someone.
- **SPIM (Instant Messaging Spam)** – spam sent through instant messaging (WhatsApp).
- **SPIT (Spam over Internet Telephony or VoIP spam)** – transmission of spam messages over Voice over Internet Protocol (Skype).
- **Pharming** – involved the redirection of a website's traffic to a fake/malicious website without the user's knowledge.
- **Phishing** – revolves on Social Engineering to trick users to reveal sensitive information.
- **Elicitation** – The goal is to exploit human psychology, trust, and vulnerabilities to obtain confidential information that can be used as leverage for unauthorized access or malicious activities.
- **Typosquatting** – misspelled URL domain that sends you to a similar but malicious website of the website you are looking for.
- **Prepending** – adding data, characters, or information at the beginning of an existing piece of data.
- **Pretexting** – attacker creates a fake scenario or pretext to deceive someone into providing sensitive information or taking certain actions.
- **Watering Hole Attack** – attacker compromises a website that is likely to be visited by the targeted individuals or organization. The goal is to infect the device or gather sensitive information.
- **Trojan Horse (Trojan)** – Type of malware that disguises itself as legitimate to deceive users and gain unauthorized access to their computer systems.
- **Worm** – Standalone malicious program that spreads over a computer's network to affect system resources and network bandwidth.
- **Ransomware** – malware that encrypts files and locks the entire system until the user performs the requested action.
- **Malware** – harmful program that disrupts computer operation, gathers sensitive information, or gains unauthorized access to computer systems.
- **PUP (Potentially Unwanted Program)** – software applications that are not outright malicious but may exhibit behaviors or characteristics that users may find undesirable or unexpected.
- **Fileless Malware/Virus** – Only found in RAM (Random Access Memory).
- **Command and Control (C2) Server** – serves as a central communication hub for a cyber-attack, allowing for maintaining

control over compromised systems, receive information, and issue commands.

- **Botnet Control** – C2 server that is used to manage and orchestrate a network of compromised computers or devices.
- **Botnet** – used in DDoS (Distributed Denial of Service) attacks.
- **Keylogger** – software or hardware device used to record and monitor the keystroke types on a computer or mobile device. (Type of Spyware)
- **Rootkit** – malicious software designed to conceal/masks the existence of programs or certain processes on a computer.
- **Logic Bomb** – malicious code that is intentionally inserted with the purpose of executing harmful action when certain conditions are met/activated by a specific event.
- **RAT (Remote Access Trojan)** – designed to provide a backdoor into the infected system, allowing attackers to access and control the machine remotely.
- **Malware as a Service (MaaS)** – threat actors offer malware or hacking services to others, often on a subscription basis.
- **Software as a Service (SaaS)** – provides software applications over the internet on a subscription basis.
- **Everything as a Service (XaaS)** – an umbrella term that encompasses various "as a Service" models.
- **Platform as a Service (PaaS)** – provides a platform that includes tools and services for application development, testing, and deployment.
- **Infrastructure as a Service (IaaS)** – provides virtualized computing resources over the internet.
- **pfSense** – an open-source firewall and router software distributed based on FreeBSD, and an operating system derived from Unix.
- **PCAP (Packet Capture)** – file format and a set of tools used for capturing, strong, and analyzing network traffic.
- **Spraying Attack** – attacker attempts to gain access to user account by systematically trying a few commonly used passwords against many usernames and bypasses account-lockout policies.
- **Rainbow tables** – lookup tables used to speed up the process of password guessing. (contents are hash/password) Can be rendered ineffective by salting.
- **Pivoting** – technique of using an already compromised system as a stepping stone to attack other systems within the network.
- **Skimming** – unauthorized capture of sensitive information, such as credit cards details, by using a device known as a skimmer.
- **Cloning** – unauthorized copy of a payment card.

- **Replication** – copying and maintaining data in multiple locations to ensure redundancy, availability, and fault tolerance.
- **ML (Machine Learning)** – AI feature that accomplishes tasks based on training data without explicit human instructions.
- **Transmission Control Protocol (TCP)** - One of two main protocols of the Internet Protocol (IP) suite used to transmit data over an IP network. TCP provides error checking to ensure packets are not lost in transit.
- **User Datagram Protocol (UDP)** - The second main protocol in the IP suite that transmits datagrams in a best effort method. UDP does not include error checking.
- **Cross-Site Scripting (XSS)** – type of security vulnerability in web applications that allow an attacker to inject malicious scripts into web pages viewed by others.
- **SQL Injection** – type of security vulnerability that occurs in web applications when untrusted user input is incorporated into SQL queries without proper validation or sanitation. Countermeasures include stored procedures and input validation.
- **SQL Injection Attempt:** SELECT*FROM users WHERE username = 'input_username' AND password = 'input_password' OR '1'='1';
- **Dynamic Link Library (DLL)** – collection of precompiled functions designed to be used by more than one Microsoft Windows application simultaneously.
- **DLL Injections** – application attack that relies on executing a library of code.
- **LDAP** is an example of **Secure directory access protocol.**
- **LDAP Injection Attempt**: administrator)(&)) |search.aspx?name=username)(zone=*)
- **XML Injection Attempt**: … p@$$w0rd</password></user><user><name>attacker</name>...
- **Null-Pointer Dereference** – occurs when a program attempts to access or dereference a memory address that is set to null or uninitialized value.
- **Dot-dot-slash Attack A.K.A. Directory Traversal Attack**
- **On-Path Attack** – (A.K.A. Man-in-the-Middle (MitM) Attack) attacker positions themselves on the communication path between two parties, allowing them to intercept, manipulate, or eavesdrop on the communication.
- **Fuzzing (Fuzz test)** – software testing technique that involves providing invalid, unexpected, or random data as input to a computer program in order to uncover vulnerabilities, errors, or unexpected behavior.

- **Initialization Vector (IV)** – random or non-secret value that is used as an additional input to cryptographic algorithms, particularly in the context of symmetric-key encryption.
- **IV Attack** – an attack on a cryptographic system that exploits weaknesses in the initiation vector (IV) used with certain encryption algorithms, especially in block cipher modes of operation.
- **Buffer Overflow** – software vulnerability that occurs when a program writes more data to a block of memory, or buffer, that it was allocated to hold.
- **Memory Leak** – software defect where a program fails to release memory that it has allocated but is no longer in use.
- **Race Condition** – a malfunction in a preprogrammed sequential access to a shared resource.
- **Network Replay Attack** – occurs when an attacker intercepts sensitive user data and resends it to the receiver with the intent of gaining unauthorized access or tricking the receiver into unauthorized operations.
- **Characteristic Features of a session ID:** a unique identifier assigned by the website to a specific user, a piece of data that can be stored in a cookie or embedded as a URL parameter, & stored in a visitor's browser.
- **Session Replay Attack** – an attacker steals a vail session ID of a user and resends it to the server with the intent of gaining unauthorized access or tricking the server into authorized operations.
- **Server-Side Request Forgery (SSRF)** – exploit that allows an attacker to take control over a server and use it as a proxy for unauthorized actions.
- **Cross-Site Request Forgery (CSRF)** – attacker tricks a victim into performing unintended actions on a web application where the victim is authenticated.
- **SSL Stripping** – an attacker downgrades a secure HTTPS connection to an unencrypted HTTP connection (e.g. downgrade attack, on-path attack->); Attackers position themselves in the middle of the client and the server.
- **Refactoring** – restructuring or reorganizing existing code without changing its external behavior. Software/hardware driver manipulation.
- **Sideloading** – loading and running applications on a device without going through the official distribution channels.
- **Shimming** – inserting a small, intermediary piece of code or a "shim" between two incompatible components to enable them to work together without modifying the original components; Alters the external behavior of an application and at the same time does not

introduce any changes to the application's code. Software/hardware driver manipulation technique.

- **Pass The Hash** – technique that allows an attacker to authenticate to a remote server without extracting the cleartext password from a digest.
- **"Evil Twin"** – a rogue Wireless Access Point (WAP) that is set up with malicious intent, typically for eavesdropping or stealing sensitive user data.
- **Bluesnarfing** – describes a security vulnerability associated with Bluetooth-enabled devices.
- **Bluejacketing** – sending unsolicited messages or digital business cards (vCards) to Bluetooth-enabled devices within the range of the sender.
- **Wireless Disassociation Attack** – (A.K.A. deauthorization attack) involves sending forged deauthorization or disassociation frames to wireless devices on a Wi-Fi network.
- **Wireless Jamming Attack** is a type of DoS attack.
- **Salting** – technique used to enhance the security of hashed passwords or other sensitive data. This is done by adding a random and unique value, known as a "salt" to the data before it is hashed.
- **Salt** - provides better protection against brute-force, dictionary, and rainbow table attacks.
- **Address Resolution Protocol (ARP) Poisoning** – attacker sends malicious Address Resolution Protocol messages to associate their own MAC address with the IP address of a legitimate device on the network.
- **Media Access Control (MAC) Flooding** – network attack that compromises the security of a network switch by overflowing its memory used to store the MAC address table.
- **Network Interface Card (NIC)** – hardware component that allows computers to connect to a network.
- **MAC Spoofing/Cloning** – attacks that rely on altering the burned-in address of a NIC to assume the identity of a different network host.
- **Layer 2 Attacks:** MAC cloning, ARP poisoning, MAC flooding, & MAC spoofing.
- **Domain Hijacking** – situation in which domain registrants due to unlawful actions of third parties lose control over their domain names.
- **Domain Name System (DNS) Poisoning** – remapping a domain name to a rogue IP address.
- **hosts** – enables client-side URL redirection.
- **Distribution of** Spam – biggest impact on domain reputation.
- **Network-based** is the most common form of a DDoS attack.

- **Operational Technology** is the type of DDoS attack that targets industrial equipment and infrastructure.
- **.ps1** – filename extension of a Microsoft PowerShell script file.
- **.sh** – filename extension that denotes a shell script in Unix command.
- **.py** - filename extension used in cross-platform, general-purpose programming language.
- **.vbs** – filename extension used in a scripting language based on Microsoft's Visual Basic programming language.
- **Visual Basic for Applications (VBA)** – enables running macros in Microsoft Office applications.
- **Advanced Persistent Threat (APT):** high level of technical sophistication, extensive amount of resources/funding, & typically funded by governments/nation states.
- **Script Kiddie** – individuals who lack advanced hacking skills and rely on pre-written scripts or tools to carry out attacks.
- **Hacktivist** – individuals or groups who hack for ideological reasons, often to promote a political or social issue.
- **Insider Threat** – individual within an organization who misuse their legitimate access to company resources for malicious purposes.
- **Criminal Syndicates** – organized groups of criminals working together to achieve common goals, often for financial gain.
- **Competitors** – threat actors that engage in illegal activities to get the know-how and gain market advantage.
- **Gray Hat Hacker** – Individuals who fall between white hat and black hat, as they may engage in hacking activities without explicit authorization but no malicious intent.
- **Shadow IT** – describes software and hardware used within an organization, but outside of the organization's official IT infrastructure.
- **Wireless Threat Vector** – a specific path or method through which a wireless network or system could be vulnerable to security risks or attacks.
- **Rogue Access Point** – unauthorized wireless access points set up by the attackers to mimic legitimate networks and trick users into connecting without the knowledge or approval of the network administrator.
- **Penetration Testing:** bypasses security controls, actively tests security controls, & exploits vulnerabilities.
- **White-Box Testing** – authorized professional with full prior knowledge of how the system that is being tested works.
- **Black-Box Testing** – does not have prior knowledge of the system that is being tested.

- **Gray-Box Testing** – the person conducting the test has limited access to information on the internal workings of the targeted system.
- **War-Driving** – driving around with a Wi-Fi-enabled device to map and discover wireless networks. WAP antenna placement provides a countermeasure against this.
- **Open-Source Intelligence (OSINT)** – practice of collecting and analyzing information from publicly available sources to gather intelligence or insights.
- **Threat Vector** – method or path that a cyber threat takes to infilt4rate a system, network, or organization.
- **Incident Response Plan (IRP)** – documented set of procedures and guidelines for detecting, responding to, and mitigating security incidents.
- **Disaster Recovery Plan (DRP)** – documented and structured approach outlining the processes and procedures an organization should follow to recover and restore its IT systems and infrastructure in the event of a disaster.
- **Business Continuity Plan (BCP)** – process that involves creating systems of prevention and recovery to deal with potential threats to a company.
- **Common Vulnerabilities and Exposures (CVE)** – standardized list of common identifiers for publicly known cybersecurity vulnerabilities.
- **National Vulnerability Database (NVD)** – U.S. government repository of standard-based vulnerability management data; providing information on software vulnerabilities, security flaws, and misconfiguration.
- **Automated Indicator Sharing (AIS)** – U.S. government initiative that allows organizations to share real-time cybersecurity threat indicators and information automatically.
- **Indicator of Compromise (IoC)** – piece of evidence or artifact that suggests a computer system or network has been compromised or breached.
- **Structured Threat Information eXpression (STIX)** – a standardized language and format used for the exchange and sharing of cybersecurity threat intelligence.
- **Trusted Automated eXchange of Indicator Information (TAXII)** – a dedicated transport mechanism for cyber threat information.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)** – suite of communication protocols that form the foundation for the internet and many other networks.
- **Secure/Multipurpose Internet Mail Extensions (S/MIME)** – standard for securing email messages with cryptographic security

services.

- **GitHub** – a file/code repository with a collaboration platform for developers.
- **Request For Quotation** – document or formal process that invites suppliers to submit quotations for the supply of goods, services, or products.
- **Request for Comments** – formal document that defines various specifications of internet standards, protocols, procedures, and related issues.
- **Request for Information** – document or formal process used by organizations to gather information about products, services, or solutions from potential suppliers or vendors.
- **Request for Proposal** – formal document or process used by organizations to solicit proposals from potential suppliers, vendors, or service providers for the procurement of goods or services.
- **Personally Identifiable Information (PII)** – information that can be used to identify and distinguish an individual.
- **Tactics, Techniques, and Procedures (TTPs)** – describes the methods and behaviors that threat actors use to achieve their objectives.
- **Intrusion Prevention System (IPS)** – security technology that monitors networks and/or system activities for malicious exploits or security policy violations.
- **Intrusion Detection System (IDS)** – security tool or software that monitors network or system activities for malicious or suspicious behavior and alerts administrators or takes action to respond not potential incidents.
- **Secure Sockets Layer (SSL)** – a depreciated encryption protocol that was widely used to secure communication on the internet. Due to vulnerabilities, it was replaced by Transport Layer Security (TLS).
- **Common Vulnerability Scoring System (CVSS)** – industry standard for assessing the severity of computer system security vulnerabilities.
- **Security Information and Event Management (SIEM)** –provides real-time analysis of security alerts and is designed to detect anomalies in the log and event data collected from multiple network devices.
- **Proxy Server** – intermediate server that acts as a gateway between a user's device and the internet.
- **Syslog Server** – dedicated to collecting, storing, and analyzing log messages from networked devices.
- **Industrial Control System (ICS) Server** – associated with industrial control systems used in various industries, such as manufacturing and critical infrastructure.

- **Supervisory Control and Data Acquisition (SCADA)** – systems used for monitoring and controlling industrial processes and infrastructure.
- **Security Orchestration, Automation, and Response (SOAR)** – tool that enables automated response to security incidents.
- **Vulnerability Scanning** – identifies lack of security controls, identifies common misconfigurations, & passively tests security controls.
- **Physical and logical network diagrams** provide visual representation of network architecture.
- **A physical network diagram** contains information on hardware devices and physical links between them.
- **A logical network diagram** describes the actual traffic flow on a network and provides information related to IP addressing schemes, subnets, device roles, or protocols that are in use on the network.
- **Data Execution Prevention (DEP)** – security feature that helps prevent damage from viruses and other security threats by monitoring and preventing the execution of code in specific regions of memory.
- **Data Loss Prevention (DLP)** – set of technologies, strategies, and tools designed to prevent unauthorized access, use, and transmission of sensitive or confidential information outside an organization. Content inspection allows a DLP system to fulfill its role.
- **The state of digital data that requires it to be processed in an unencrypted form is "In processing".**
- **Tokenization** – the process of replacing sensitive data with non-sensitive information, known as a token.
- **Hashing** – process of converting sensitive data (such as passwords) into a fixed-size string of characters.
- **Hash Function** – designed to take an input and produce a fixed-size string of characters, known as the hash value or hash code.
- **Hot Site** – fully operational and ready-to-use duplicate of the original site.
- **Warm Site** – partially equipped duplicate of the original site.
- **Cold Site** – facility with basic infrastructure, such as power and space, but lacks the necessary computer systems and backups.
- **Honeypot** – security mechanism set up to attract and detect unauthorized users or attackers.
- **Honeynet** – network or honeypots designed to simulate a controlled environment that attracts and monitors malicious activity.
- **Fake Telemetry** – simulated or fabricated data sent by a system or device to mimic the behavior of legitimate telemetry.
- **DNS Sinkhole** – mechanism used in network security to redirect or

block undesirable or malicious domain names; an example of fake telemetry.

- **Cloud Access Security Broker (CASB)** – a security solution specifically designed to enforce security policies for data and applications in the cloud.
- **Unified Threat Management (UTM)** – comprehensive security solution, commonly in the form of a dedicated device, that integrates multiple security features into a single platform.
- **Next-Generation Firewall (NGFW)** – firewall with advanced capabilities that go beyond the traditional firewall.
- **Dynamic Multipoint Virtual Private Network (DMVPN)** – network technology that allows the creation of secure and scalable VPNs over the internet.
- **Cloud Security Alliance (CSA)** – nonprofit organization dedicated to promoting the use of best practices for providing security assurance within cloud computing.
- **Cybersecurity Framework (CSF)** – framework developed by the National Institute of Standards and Technology (NIST) to improve the cybersecurity posture of organizations.
- **Cloud Controls Matrix (CCM)** – framework developed by the Cloud Security Alliance (CSA) to provide security principles and guidelines for cloud service providers.
- **Center for Internet Security (CIS)** – nonprofit organization that focuses on providing cybersecurity best practices and standards to safeguard organizations against cyber threats.
- **Virtual Private Cloud (VPC)** – virtual network dedicated to a specific cloud account within a cloud service provider. Users can deploy and manage cloud resources within a VPC, and a transit gateway facilities connectivity between an on-premises network and the VPC.
- **Master Service Agreement (MSA)** – contractual agreement that outlines the terms and conditions between parties, often for establishing a long-term business relationship.
- **Managed Service Provider (MSP)** – companies that offer comprehensive IT services to clients on an ongoing basis.
- **Managed Security Service Provider (MSSP)** – specifically focus on providing managed security services.
- **Fog Computing** – a local network infrastructure between IoT devices and the cloud designed to speed up data transmission processing.
- **Edge Computing** – involves processing data closer to the source of data generation, typically at or near the edge of the network.
- **Thin Client** – a networked computer equipped with the minimum amount of hardware and software components; relies on network

resources provided by a remote server performing most of the data processing and storage functions.

- **Thick Client** – runs applications locally from its own hard drive.
- **Containerization** – lightweight form of virtualization that encapsulates an application and its dependencies into a container.
- **Microservice** – independent and self-contained code components that can be put together to form an application.
- **Software-Defined Networking (SDN)** – separates the control plane from the data plane in the networking devices.
- **Software-Defined Visibility (SDV)** – visualization combined with the capability to dynamically respond to events.
- **Virtual Machine (VM) Sprawl** – describes a situation in which a large number of virtual machines are deployed without proper administrative controls or management. Prevention with asset documentation and usage audit.
- **Virtual Machine (VM) Escape** – the process of breaking out of the boundaries of a guest operating system installation to access the primary hypervisor controlling all the virtual machines on the host machine. Prevention by sandboxing and patch management.
- **Library** – a collection of commonly used programming functions designed to speed up the software development process.
- **Open Web Application Security Project (OWASP)** – nonprofit organization dedicated to improving the security of software.
- **CSIRT** – Computer Security Incident Response Team
- **CERT** – Computer Emergency Response Team
- **Normalization** – process of removing redundant entries from a database.
- **Snapshot** – a file-based representation of the state of a virtual machine at a given point in time.
- **Snapshot backups** – commonly used with virtual machines.
- **Federation** – an authentication subsystem in which a single set of authentication credentials provides access to multiple systems across different organizations.
- **Time-Based One-Time Password (TOTP)** – Not vulnerable to replay attacks, based on a shared secret key and current time, & valid for only one login session.
- **HMAC-Based One-Time Password (HOTP)** – based on a cryptographic hash function and a secret cryptographic key, valid for only one login session, & not vulnerable to replay attacks.
- **Examples of hardware Authentication tokens**: key fob, RFID badge, & Smart card.
- **Example of a soft authentication token**: authenticator app

- **Static Authentication methods:** Personal Identification Number (PIN) & User-generated password
- **Example of a certificate-bases authentication:** Smart card
- **False Acceptance Rate (FAR)** – a measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorized user.
- **False Rejection Rate (FRR)** – likelihood of incorrectly rejecting an unauthorized user.
- **Cyclic Redundancy Check (CRC)** – a method for error-checking in data transmission.
- **Crossover Error Rate (CER)** – the point where FAR and FRR are equal in a biometric system; metric used for evaluation of a biometric security system's accuracy.
- **Multi-Factor Authentication (MFA) examples:** PIN, USB token, & Retina scan.
- **MFA attributes:** handwritten signature, gait analysis, GPS reading, & chain of trust.
- **Redundant Array of Independent Disks (RAID)** – a dedicated data storage solution that combines multiple disk drive components into a single logical unit to increase volume size, performance, or reliability.
- **RAID 0:** requires a minimum of 2 drives to implement, also known as disk striping, decreases reliability (failure of any disk in the array destroys the entire array, is suitable for systems where performance has higher priority than fault tolerance & DOES NOT offer fault tolerance.
- **Hardware RAID Level 1:** requires at least 2 drives to implement, offers improved reliability by creating identical data sets on each drive, & is also referred to as disk mirroring.
- **Hardware RAID Level 5:** requires at least 3 drives to implement & offers increased performance and fault tolerance.
- **Hardware RAID Level 6:** requires at least 4 drives to implement & offers increased performance and fault tolerance.
- **Hardware RAID Level 10:** requires a minimum of 4 drives to implement, is referred to as stripe of mirrors, i.e. a combination of RAID 1 and RAID 0, & offers increased performance and fault tolerance.
- **Multipath I/O** – a framework that improves fault tolerance and performance by enabling additional, alternate routes for data that is being transferred to and from storage devices.
- **Network Interface Card (NIC) teaming** – a technology that allows multiple NICs to work together as a single logical interface.
- **Uninterrupted Power Supply (UPS)** – a device that can provide

short-term emergency power during an unexpected main power source outage.

- **Backup Generator is best suited for providing long-term emergency power during an outage.**
- **Dual-Power Supply** – component that would add power redundancy on a server box.
- **Managed Power Distribution Unit (Managed PDU)** – device designed to distribute and monitor the quality of electric power to multiple outlets.
- **Storage Area Network (SAN)** – a dedicated local network consisting of devices providing data access.
- **To restore data from an incremental backup you would need:** copy of the last full backup & all copies of incremental backups made since the last full backup.
- **In a differential backup strategy:** restoring data from backup requires a working copy of the last full backup and the last differential backup.
- **Magnetic Tapes** – refers to a sequential-access backup media.
- **Network Attached Storage (NAS)** – a dedicated storage appliance that can be added to a local network.
- **System Image** – an exact copy of the entire state of a computer system.
- **Concept of non-persistence:** last known-good configuration, live boot media, & known state reversion.
- **Live-boot Media** – a type of removeable storage media that contains portable, non-persistent OS.
- **Scalability** – the capability of a hardware or software system to process increasing workload without the decrease in performance.
- **Examples of embedded systems:** Raspberry Pi, Arduino, & Field Programmable Gate Array (FPGA).
- **Internet of Things (IoT)** – an emerging field of innovative technologies, such as wearable tech or home automation.
- **Heating, Ventilation, and Air Conditioning (HVAC)** – refers to an environmental control system.
- **MFD** – Multi-Function Device
- **MFP** – Multi-Function Printer
- **Real-Time Operating System (RTOS)** – type of OS characterized by low delay between the execution of tasks required in specific applications, such as in military missile guidance systems or automotive braking systems.
- **System on a Chip (SoC)** – an integrated circuit combining components normally found in a standard computer system. Sensitive

data should not be stored in the register after opening, & a separate security verification tool should be used to check the design.

- **Zigbee** – an IoT technology designed to provide communication between appliances in a home automation network.
- **Mantrap** – a physical security access control system used to prevent unauthorized users from gaining access to restricted areas by following another person.
- **Proximity Card** – use RFID technology to communicate with card readers in a close range but is contactless.
- **Faraday Cage** – physical security control types, provides protection against Radio-Frequency Interference (RFI), & provides protection against Electromagnetic Interference (EMI).
- **Bollard** – a barricade used in many environments.
- **Screened Subnet** – a lightly protected subnet consisting of publicly available servers placed on the outside of the company's firewall.
- **Degaussing** – process used to reduce or eliminate unwanted magnetic field in objects, particularly in magnetic storage media such as hard drives and magnetic tapes.
- **Digital Signatures provide:** Integrity, Authentication, & Non-repudiation.
- **Key Stretching** – a mechanism for extending the length of a cryptographic key to make it more secure against brute-force attacks. (e.g. Bcrypt & PBKDF2 [Password-Based Key Derivation Function2])
- **Characteristic features of Elliptic Curve Cryptography (ECC)** – asymmetric encryption, low processing power requirements, & suitable for small wireless devices.
- **Perfect Forward Secrecy (PFS)** – a solution designed to strengthen the security of session keys.
- **Post-Quantum Cryptography** – it is predicted to be the most future-proof cryptographic solution.
- **Symmetric Encryption** – involves the use of a single key for both encryption and decryption, and is commonly referred to as secret-key encryption. Requires less processing power than asymmetric encryption. (e.g. AES)
- **Asymmetric Encryption** – involves the use of a pair of keys (public and private) for encryption and decryption. Requires more processing power than symmetric encryption. (e.g. RSA)
- **Ephemeral Key** – an asymmetric encryption key designed to be used only for a single session or transaction.
- **Session Key** – used during a single session and is part of the symmetric key.

- **Blockchain** – a decentralized digital ledger system (i.e. a specific type of distributed database) stored across multiple computers in a P2P network.
- **Stream Ciphers** – process data bit by bit or byte by byte.
- **Block Ciphers** – divide data into fixed-size blocks and encrypt each block separately.
- **Electronic Codebook (ECB)** – block cipher that is simple/weak.
- **Galois/Counter Mode (GCM)** – block cipher that provides both data integrity and confidentiality.
- **Security Through Obscurity Concept** – the practice of relying on the secrecy or obscurity of certain elements of a system as a means of providing security.
- **Steganography** – the purpose is to hide data within another piece of data.
- **Homomorphic Encryption** – technique that enables processing data in an encrypted form.
- **Encryption** applies to the concept of **confidentiality.**
- **Hashing** applies to the concept of **integrity.**
- **Security through Obscurity** applies to the concept of **obfuscation.**
- **Digital Certificate** applies to the concept of **non-repudiation.**
- **The lack of entropy in the process of generating cryptographic keys reduces the security of cryptographic algorithms.**
- **Domain Name System Security Extensions (DNSSEC)** – a suite of security extensions for an internet service that translates domain names into IP addresses.
- **Secure Shell (SSH) - a non**-proprietary cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services.
- **Telnet** – a protocol used for a remote command-line login, but does not provide encryption, making it insecure for transmitting sensitive information over the network.
- **Remote Access Service (RAS)** – service in Microsoft Windows that allows remote access to a network, but it is not a cryptographic protocol.
- **SSH File Transfer Protocol (SFTP)** – network protocol for secure file transfer over SSH.
- **SNMPv1 & SNMPv2 offer authentication based on community strings sent in an unencrypted form.**
- **SNMPv3** – provides packet encryption, authentication, and hashing mechanisms that allow for checking whether data has changed in transit (i.e. validation of data integrity).
- **Authentication Header (AH)** – part of the Internet Protocol Security

(IPsec) protocol suite that provides authentication and integrity.

- **Encapsulating Security Payload (ESP)** – part of the IPsec protocol suite that provides authentica5tion, integrity, and confidentiality.
- **Tunnel Mode** – IPsec mode that provides entire packet encryption.
- **Transport Mode** – IPsec mode that provides encryption only for the payload (the data part of the packet).
- **Post Office Protocol version 3 (POP3)** – used for email retrieval. Encrypted communication on TCP port 995 & Secure Socket Layer (SSL), & Transport Layer Security (TLS).
- **Internet Message Access Protocol (IMAP)** – offers improved functionality in comparison to POP3 & serves the same function as POP3. The secure version is on TCP port 993, SSL, and TLS.
- **Network Time Protocol Security (NTPsec)** – a secure implementation of a protocol used for synchronizing clocks over a computer network.
- **Dynamic Host Configuration Protocol (DHCP)** – a network protocol providing an alternative solution to the manual allocation of IP addresses.
- **DHCP Snooping** – security feature of a network switch that provides countermeasures against rogue DHCP servers.
- **Endpoint Detection and Response (EDR)** – an endpoint security solution that provides the capability for detection, analysis, response, and real-time monitoring of cyber threats.
- **Host-based Firewall & Software Firewalls are used for protecting a single computer.**
- **Hardware Firewall & Network-based Firewall are used for protecting an ingress/egress point of a corporate network.**
- **Unified Extensible Firmware Interface (UEFI)** – a firmware interface designed as a replacement for Basic Input/Output Systems (BIOS).
- **Measured Boot** – refers to a security mechanism first introduced by Microsoft in Windows 8.
- **Tokenization, Salting, & Hashing** can be used to **protect database contents.**
- **Secure Cookie** – a type of HTTP cookie that has a Secure attribute set.
- **Code Signing** – confirms the application's source of origin & validates the application's integrity.
- **Static Code Analysis** – the process of analyzing the source code of a program without executing it. An automated or manual code review process aimed at discovering logic and syntax errors.
- **Dynamic Code Analysis** – the process of executing application code

to observe its behavior, identify potential vulnerabilities, and detect flaws.

- **Hardening** – the process of securing a system, network, or software application by reducing its attack surface and strengthening its defenses against potential security threats.
- **Self-Encrypting Drive (SED)** – a data storage device equipped with hardware-level encryption functionality. A specification for SEDs is **Opal.**
- **Full Disk Encryption (FDE)** – a software technology designed to provide confidentiality for an entire data storage device.
- **Advanced Encryption Standard (AES)** – symmetric encryption algorithm used to secure data. Least vulnerable to attacks.
- **Encrypting File System (EFS)** – feature in Microsoft Windows for encrypting individual files and folders.
- **Hardware Security Module (HSM)** – physical device that provides secure key storage and cryptographic operations.
- **Trusted Platform Module (TPM)** – hardware component that provides a secure foundation for various security functions, such as generating and storing cryptographic keys, measuring system integrity, and supporting secure boot processes. Also, is an embedded crypto-processor found on the motherboards of newer PCs and laptops.
- **Root of Trust** – foundational concept that establishes a secure starting point for building and verifying the security of a system.
- **HSM & TPM are both examples of hardware root of trust.**
- **Sandboxing** – a mechanism for safe execution of untested code or untrusted application.
- **In active-active mode load balancers distribute network traffic across ALL SERVERS.**
- **In active-passive mode load balancers distribute network traffic across SERVERS MARKED AS ACTIVE.**
- **In a round-robin load balancing method, each consecutive request is handled by the NEXT SERVER IN A CLUSTER.**
- **In a weighted round-robin load balancing method, each consecutive request is still handled in a rotational fashion, but servers with higher specifications or capacities are designated to process more workload.**
- **Virtual IP Address (VIP or VIPA)** – an IP address that doesn't correspond to any actual physical network interface.
- **Session Affinity** – a method that ignores the load balancing algorithm by consistently passing requests from a given client to the same server.

- **Virtual Local Area Network (VLAN)** – a logical grouping of computers that allows computer hosts to act as if they were attached to the same broadcast domain regardless of their physical location.
- **East-west** – refers to the network traffic within a data center, A.K.A. server-to-server traffic.
- **Extranet** – a private network that allows controlled access to specific authorized external (third-party) users, such as business partners, customers, or suppliers.
- **Intranet** – type of private network for a corporation or organization accessible only to its employees or authorized members.
- **Zero Trust** – none of the devices operating within the boundaries of a given network can be trusted by default even if they were previously verified.
- **VPN Concentrator** – a dedicated device for managing encrypted connections established over an untrusted network, such as the internet.
- **Always-on VPN** – a type of persistent VPN connection that starts automatically as soon as the computer detects a network link.
- **Split Tunnel** – allows the VPN user to direct some of their internet traffic through the encrypted VPN tunnel, while other traffic is routed directly to the internet without passing through the VPN.
- **Full Tunnel** – directs all of the user's internet traffic through the encrypted VPN tunnel, regardless of whether it is destined for the corporate network or the general internet.
- **Tethering** – process of sharing a mobile device's internet connection with other devices.
- **VPN type used for connecting computers to a network**: Remote Access & Client-to-Site.
- **Site-to-Site** – type of VPN that enables connectivity between two networks.
- **Protocols used for implementing secure VPN tunnels are**: IPsec, TLS, & L2TP.
- **Layer 2 Tunneling Protocol** – protocol that allows the creation of VPNs.
- **Point-to-Point Tunnel Protocol (PPTP)** – a depreciated method for implementing VPNs.
- **HTML5 VPN portal is an example of clientless VPN implementation where HTML5-compliant web browser along with TLS encryption can be used instead of a dedicated VPN client software.**
- **Network Access Controls (NAC)** – define a set of rules enforced in a network that the clients attempting to access the network must

comply with.

- **Out-of-band Management** – refers to a network device management technique that enables device access through a dedicated communication channel separate from the network where a given device operates.
- **Spanning Tree Protocol (STP)** – a network protocol that ensures a loop-free topology for Ethernet networks by blocking redundant paths.
- **Rapid Spanning Tree Protocol (RSTP)** – an improvement over STP, designed to provide faster convergence in response to network topology changes.
- **Bridge Protocol Data Unit (BPDU)** – refers to an STP frame; STP uses BPDUs to exchange information between switches in a network to identify and eliminate loops in the network topology.
- **Media Access Control (MAC) Filtering** – a network security access control method in which a 48-bit physical address assigned to each network card is used to determine access to the network.
- **Jump Server** – a type of hardened server used as a secure gateway for remote administration of devices placed in a different security zone. An intermediary between an intranet and a screened subnet.
- **Functions of a forward proxy are that it acts on behalf of a client & hides the identity of a client.**
- **Functions of a reverse proxy are that it acts on behalf of a server & hides the identity of a server.**
- **Characteristics of a Transparent Proxy include:** it doesn't require client-side configurations, redirects client's requests and responses without modifying them, & clients might be unaware of the proxy service.
- **Nontransparent Proxy** – modifies client's requests and responses & requires client-side configuration.
- **Network Intrusion Detection System (NIDS) | Network Intrusion Prevention System (NIPS)**
- **Signature-based NIDS/NIPS** – are security technologies designed to monitor network traffic for signs of malicious activities and unauthorized access.
- **Heuristic -**
- **A NIDS/NIPS that detects intrusions by comparing network traffic against the previously established baseline can be classified as Anomaly-based, Heuristic, & Behavioral.**
- **Stateful Inspection** – the dynamic packet filtering concept.
- **Stateless Inspection** – a firewall technology that filters packets based solely on their source and destination information, without keeping track of the state of network connections.

- **Network Address Translation (NAT)** – used to hide the internal IP addresses by modifying IP address information in IP packet headers while in transit across a traffic routing device. Also, a solution that alleviates the problem of depleting IPv4 address space by allowing multiple hosts on the same private LAN to share a single public IP.
- **Access Control List (ACL)** – a set of rules specifying which users or systems processes are granted access to objects and what operations are allowed on a given object such as routers, switches, and firewalls.
- **Quality of Service (QoS)** – the solution used for controlling network resources and assigning priority to different types of traffic.
- **Port Mirroring** – feature that allows an administrator to inspect traffic passing through a network switch.
- **Tap** – a monitoring port on a network device.
- **Wi-Fi Protected Access 3 (WPA3)** – has the highest level of wireless encryption schemes.
- **Wired Equivalent Privacy (WEP)** – deprecated wireless security protocol in favor of newer standards.
- **Advanced Encryption Standard with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)** – the encryption scheme used in Wi-Fi Protected Access 2.
- **For the purpose of encryption, WPA3 takes advantage of:** AES-GCMP & AES-CCMP.
- **Pre-Shared Key (PSK)** – a client authentication method used in WPA2 Personal mode.
- **Simultaneous Authentication of Equals (SAE)** – a client authentication method used in WPA3 Personal mode.
- **Extensible Authentication Protocol (EAP)** – an authentication framework commonly used in wireless networks and point-to-point connections.
- **EAP-TLS** – EAP method that offers the highest level of security; relies on both client-side and server-side certificates for authentication.
- **IEEE 802.11X NOT 'x'**
- **For securing a small network that lacks an authentication server use: WPA3-SAE**
- **Characteristics of WPA2/WPA3 Enterprise mode:** suitable for large corporate networks, IEEE 802.1X, & requires RADIUS authentication server.
- **Wi-Fi Protected Setup (WPS)** – a solution that simplifies configuration of new wireless networks by allowing non-technical users to easily configure network security settings and add new devices to an existing network; deprecated as well.

- **Capital Portal** – security solution that allows administrators to block network access for users until they perform required action.
- **Heat Map** – identifies areas of low signal strength and optimizes the placement of multiple Access Points (APs).
- **Wi-Fi Analyzer** – diagnostic tool that can be used for measuring wireless signal strength.
- **Channel Overlapping** – situation where multiple channels share the frequency band causing interference and performance degradation for devices operating on channels that are too close to each other.
- **Channel Bonding** – technique of combining multiple channels to increase the overall data transfer rate, often used in the context of Wi-Fi networks to enhance bandwidth.
- **Wi-Fi Analyzer & Wireless Access Points (WAP) are tools used to troubleshoot wireless signal loss and low wireless network signal coverage.**
- **Omnidirectional Antenna** – a common antenna type used as standard equipment on most Aps for indoor WLAN deployments; provides a 360-degree horizontal signal coverage.
- **4G/5G are broadband cellular network technologies.**
- **Wi-Fi** – 2.4/5.0 GHz frequency range wireless network technology implemented in the IEEE 802.11 series of standards.
- **Bluetooth** – a popular 2.4 GHz short-range wireless technology used for connecting various personal devices in a WPAN. Pairing security feature is a **PIN code.**
- **MBM – Mobile Device Management:** the enforcement of mobile device policies and procedures.
- **Remote Wipe** – erase data on a lost or stolen mobile device.
- **Geofencing** – type of technology that provides control over the usage of a mobile device within a designated area.
- **Push Notification** – used to describe information delivery from a server to a client performed without a specific request from the client.
- **Unified Endpoint Management (UEM)** – a software tool that provides a single management interface for mobile devices, PCs, printers, IoT devices and wearables.
- **Mobile Application Management (MAM)** – a dedicated mobile app management software.
- **Security-Enhanced Android (SEAndroid) – a type of mobile OS implementing stricter, Linux-based access security controls.**
- **Storage Segmentation** – a mobile security solution that enables separate controls over the user and enterprise data.
- **MicroSD HSM** - a dedicated cryptographic processor residing on a miniature flash memory card.

- **Rooting** – the capability of gaining root access or administrative access to the operating system and system applications on Android devices.
- **Jailbreaking** – removal of software restrictions imposed by Apple.
- **Carrier Unlocking** – modifying a mobile device's operation in such a way that it can be used with any service provider.
- **Over-the-Air (OTA)** – mobile device updates delivered over a wireless connection.
- **Rich Communication Services (RCS)** – technology designated as a successor to SMS and MMS.
- **On-The-Go (OTG)** – technology that enables establishing direct communication links between USB devices.
- **Embedded Geotag** – privacy-related security risk connected with public sharing of pictures taken with smartphones.
- **Wi-Fi Direct** – technology that enables establishing direct communication links between two wireless devices without an intermediary WAP.
- **Mobile Hotspot** – a type of WLAN that enables network access through a mobile device that acts as a portable WAP.
- **BYOD** – Bring Your Own Device
- **COPE** – Corporate Owned, Personally Enabled
- **CYOD** – Choose Your Own Device
- **Virtual Desktop Infrastructure (VDI)** – a mobile device that acts as a terminal for accessing data and applications hosted on a remote server.
- **Secure Web Gateway (SWG)** – a software component or hardware device designed to prevent unauthorized traffic from entering an internal network of an organization.
- **Identity Provider (IdP)** – a trusted third-party service for validating user identity in a federated identity system.
- **Username and Password & SSH Key can be used to verify the identity of a client while establishing a session over TCP port 22.**
- **Shared Account** – violates the concept of non-repudiation.
- **Service Account** – NOT designed for end user use.
- **Password Length & Complexity** – two factors that are considered important for creating strong passwords.
- **Password Vault** – a credential manager program that stores usernames and passwords in an encrypted form.
- **Knowledge-Based Authentication (KBA)** – security questions that cover personal details that should be known by the user.
- **Challenge Handshake Authentication Protocol (CHAP)** – the authentication process involves a challenge-response mechanism, that

periodically re-authenticate the client at random intervals to prevent session hijacking.

- **Password Authentication Protocol (PAP)** – an obsolete authentication protocol that sends passwords in cleartext.
- **802.1X is an IEEE standard for implementing Port-based Network Access Control (NAC).**
- **Characteristic features of RADIUS:** primarily used for network access, encrypts only the password in the access-request packet, & combines authentication and authorization.
- **Single Sign-On (SSO)** – an authentication subsystem that enables a user to access multiple, connected system components after a single login on only one of the components.
- **Security Assertion Markup Language (SAML)** – XML-based markup language for exchanging authentication and authorization data.
- **Characteristics of TACACS+:** encrypts the entire payload of the access-request packet, primarily used for device administration, & separates authentication and authorization.
- **OAuth** – open standard for **Authorization**.
- **OpenID Connect** – protocol used for **Authentication.**
- **Kerberos** – the authentication protocol that is commonly used to enable SSO in Windows-based network environments. Countermeasures **Replay attacks**. The **Network Time Protocol (NTP)** ensures the reliability of the authentication process.
- **Attribute-Based Access Control (ABAC)** – the access control model that defines access control rules with the use of statements that closely resemble natural language.
- **Role-Based Access Control (RBAC)** – group-based access control in MS Windows environments.
- **Rule-Based Access Control (RBAC)** – granted or denied depending on contents of Access Control List (ACL); implemented in network devices such as firewalls to control inbound and outbound traffic based on filtering rules.
- **File Access Control Lists (FACL)** - rule-based access control mechanism associated with files and/or directories.
- **Pluggable Authentication Module (PAM)** – provides control over elevated (administrative) accounts.
- **Public Key Infrastructure (PKI)** – a hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates.
- **Certificate Authority (CA)** – type of third-party that issues digital certificates used for creating digital signatures and public-private key pairs.

- **The PKI role of a Registration Authority (RA) includes:** accepting requests for digital certificates & authenticating the entity making the request.
- **To check to see if a digital certificate has been revoked use:** Certificate Revocation List (CRL) & Online Certificate Status Protocol (OCSP).
- **The fastest way to check the validity of a digital certificate is:** OCSP
- **Certificate Signing Request (CSR)** – method for requesting a digital certificate.
- **Certificate Revocation List (CRL)** – allows a check for validity of digital certificates even when the internet is not available.
- **Wildcard Certificate** – digital certificate type that allows multiple subdomains to be protected by a single certificate.
- **Subject Alternative Name (SAN) Certificate** – digital certificate that allows multiple domains to be protected by a single certificate.
- **Characteristic features of the Distinguished Encoding Rules (DER) digital certificate format:** encoded in binary format, .der and .cer file extensions, & generally used for Java servers.
- **Characteristic features of the Privacy Enhanced Email (PEM) digital certificate format:** encoded in text (ASCII Base64) format, .pem, .crt, .cer, and .key file extensions, & generally used for Apache servers or similar configurations.
- **Characteristic features of the Personal Information Exchange (PFX) and P12 digital certificate format:** .pfx and .p12 file extensions, encoded in binary format, & generally used for Microsoft Windows servers.
- **Characteristic features of the P7B digital certificate format:** encoded in text (ASCII Base64) format, .p7b file extensions, & generally used for Microsoft Windows and Java Tomcat servers.
- **Stapling** – checking digital certificate revocation status without contacting CA.
- **Pinning** – a depreciated security mechanism designed to defend HTTPS websites against impersonation attacks performed with the use of fraudulent digital certificates.
- **Key Escrow** – a trusted third-party storage solution providing backup source for cryptographic keys.
- **Recovery Agents** – an individual with access to key databases and permission level allowing him/her to extract keys from escrow.
- **Certificate Chaining** – the process of verifying authenticity of a newly received digital certificate.
- **Ping** – used to test the reachability of a host on an IP network.

- **Traceroute** – displays route and time taken for packets to travel from a to b. (Linux)
- **Nslookup** – used to query DNS to obtain domain name or IP address mapping, or other DNS records.
- **Dig** – tool for querying DNS name servers.
- **Tracert** – traces route that packets take to each destination host and displays the IP and round-trip times for each hop. (Windows)
- **Nmap** – used for discovering hosts and services on a network.
- **Pathping** – combines ping and tracert in Windows.
- **Hping** – used for security auditing and testing of firewalls and networks.
- **Netstat** – provides information about network connections, routing tables, interface statistics, masquerade connections, and other network-related information.
- **Banner** – describes a text message containing system information details displayed after connecting to a service on a server.
- **Banner Grabbing** – practice of connecting to an open port on a remote host to gather more information about its configurations.
- **Netcat** – network debugging and exploration tool that can read and write data across TCP or UDP.
- **theHarvester** – used for gathering OSINT.
- **Cuckoo** – anti-malware tool that enables automated analysis of suspicious files in a sandbox environment.
- **Tcpreplay** – command-line interface (CLI) packet-crafting tool.
- **Journalctl** – Linux utility for querying and displaying logs that are stored in binary form.
- **Tcpdump** – packet-capturing tool used in Unix-like operating systems.
- **WinHex** – multi-function disk and binary data editor used for low-level data processing, data recovery, and digital forensics.
- **FTK Imager** – tool for creating forensic images of computer data.
- **Autopsy** – open-source forensics platform that allows to examine the contents of a hard drive or mobile device and recover evidence from it.
- **MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)** – globally accessible knowledge base of Adversary Tactics, Techniques, and Procedures (TTPs) based on observations from real-world attacks.
- **Session Initiation Protocol (SIP)** – protocol used for managing real-time sessions that include voice, video, application sharing, or instant messaging services.
- **NXLog** – cross-platform log-managing tool.

- **NetFlow** – Cisco-designed IP traffic collection method that does not offer packet sampling.
- **Non-repudiation** – concept and legal term that refers to the assurance that a party involved in a communication or transaction cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- **Memorandum of Understanding (MOU)** – document that outlines the understanding between two or more parties regarding their common goals and objectives.
- **Memorandum of Agreement (MOA)** – outlines the terms and conditions of an agreement between parties, indicating a commitment to fulfill specific obligations.
- **Master Service Agreement (MSA)** – agreement that specifies generic terms to simplify the negotiation of future contracts between the signing parties.
- **Business Process Automation (BPA)** – use of technology to automate complex business processes and functions beyond routine tasks.
- **AUP** – Acceptable Use Policy
- **Anonymized data** – data that is made anonymous in such a way that the original subject or person described by the data can no longer be identified.
- **Pseudo-anonymization** – replaces personal data with artificial identifiers.

□

Ports:

File Transfer Protocol (FTP) **20/21** Port 21 is the control port while port 20 is used to transfer files.

Secure Shell (SSH) **22** Designed to transmit data through a remote connection.

SSH File Transfer Protocol **22** A completely separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers.

TACACS+ **49** Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services.

Domain Name System (DNS) **53** Used to associate IP addresses with domain names.

Dynamic Host Configuration Protocol (DHCP) **67/68** This network management protocol is used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one public IPv4 address.

Hypertext Transfer Protocol (HTTP) **80** Protocol used for websites and most internet traffic.

Kerberos **88** Network authentication protocol

that allows for communication over a non-secure network.
Post Office Protocol (POP) **110** E-mail protocol that allows e-mail clients to communicate with e-mail servers. POP provides only one-way communication.
Internet Message Access Protocol (IMAP) **143, 993** E-mail protocol used by e-mail clients to communicate with e-mail servers. Provides two-way communication unlike POP.
Simple Network Management Protocol (SNMP) **161/162** Protocol used to monitor and manage network devices on IP networks.
Lightweight Directory Access Protocol (LDAP) **389** Used to manage and communicate with directories.
Hypertext Transfer Protocol Secure (HTTPS) **443** Secure version of HTTP that used TLS for encryption. Most websites use HTTPS instead of HTTP.
Lightweight Directory Access Protocol Secure (LDAPS) **636** Secure version of LDAP that uses TLS for encryption.
File Transfer Protocol Secure (FTPS) **989/990** FTPS uses TLS for encryption. It can run on ports 20/21 but is sometimes allocated to ports 989/990.
Internet Message Access Protocol Secure (IMAPS) **993** Secure version of IMAP that uses TLS for encryption.
Post Office Protocol 3 Secure (POP3S) **995** Secure version of POP that uses TLS for encryption.
Remote Authentication Dial-In User Service (RADIUS) **1812, 1813** Used to provide AAA for network services.
Secure Real Time Protocol (SRTP) **5004** SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP.
Layer 2 Tunneling Protocol (L2TP) **1701** Used to create point to point connections, like VPNs over a UDP connection. Needs IPSec for encryption. Designed as an extension to PPTP. Operates at the data link layer but encapsulates packets at the session layer.
Point to Point Tunneling Protocol (PPTP) **1723** Based on PPP. Deprecated protocol for VPNs.
Remote Desktop Protocol **3389** Windows proprietary protocol that provides a remote connection between two computers.
Point to Point Tunneling Protocol **1723** Based on PPP. Deprecated protocol for VPNs.
3-way handshake: When a client is trying to establish a TCP connection. First, the client sends a synchronized packet to the server, the server then sends back a synchronized and acknowledged packet back to the client, then the client sends an acknowledged packet to the server and a connection is established.
What is an IP: An internet protocol is a set of rules for exchanging data between computers across a network.

C – Confidentiality: only those who have the authorized permission can access the information.

I – Integrity: the accuracy and reliability of data and information

A – Availability: authorized users can access the information when needed.