Availability: Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users.

Authenticity: characteristic of a communication, document, or any data that ensures the quality of being genuine.

Active Attacks: tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems.

Adversary Behavioral Identification: common methods or techniques followed by an adversary to launch attacks on or to penetrate an organization's network.

Active Footprinting: gathering information about the target with direct interaction.

ARP Ping Scan: Attackers send ARP request probes to target hosts, and an ARP response indicates that the host is active.

ACK Flag Probe Scan: Attackers send TCP probe packets set with an ACK flag to a remote device, and then analyze the header information (TTL and WINDOW field) of received RST packets to determine if the port is open or closed.

Anonymizer: intermediate server placed between you as the end user and the website to access the website on your behalf and make your web surfing activities untraceable.

Audio Steganography: hiding secret information in audio files such as .MP3, .RM, and .WAV.

Advanced Persistent Threats: a type of network attack, where an attacker gains unauthorized access to a target network and remains undetected for a long period of time.

Antivirus Sensor System: collection of computer software that detects and analyzes malicious code threats such as viruses, worms, and Trojans.

Active Sniffing: injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections.

Address Resolution Protocol (ARP): stateless protocol used for resolving IP addresses to machine (MAC) addresses.

ARP Spoofing Attack: constructing many forged ARP request and reply packets to overload the switch.

Application Level Hijacking: gaining control over the HTTP's user session by obtaining the session IDs.

Anomaly Detection: detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system.

Application-Level Firewall: filter packets at the application layer of the OSI model (or the application layer of TCP/IP.

Application Proxy: filters connections for specific services.

API DDoS Attack: saturating an API with a huge volume of traffic from multiple infected computers (botnet) to delay API services to legitimate users.

Automated Web App Security Testing: technique employed for automating the testing process. These testing methods and procedures are incorporated into each stage of development to report feedback constantly.

Application Whitelisting: list of application components such as software libraries, plugins, extensions, and configuration files, which can be permitted to execute in the system.

Application Blacklisting: list of malicious applications or software that are not permitted to be executed in the system or the network.

Access point (AP): used to connect wireless devices to a wireless/wired network.

Association: process of connecting a wireless device to an AP.
Agent Smith Attack: carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps.
Android Rooting: exploiting security vulnerabilities in the device firmware and copying the SU binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the chmod command.
Asymmetric Encryption: uses different encryption keys, which are called public and private keys for encryption and decryption, respectively.
Advanced Encryption Standard (AES): specification for the encryption of electronic data.
Behavioral Indicators: used to identify specific behavior related to malicious activities.
Black Hats: individuals who use their extraordinary computing skills for illegal or malicious purposes.
BGP: routing protocol used to exchange routing and reachability information between different autonomous systems (AS) present on the Internet.
Brute-Force Attack: adversaries try every combination of characters until the password is broken.
Buffer Overflow: common vulnerability in an applications or programs that accepts more data than the allocated buffer.
Baiting: technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data.
Botnet: huge network of compromised systems and can be used by an attacker to launch denial-of-service attacks.
Broken Access Control: method in which an attacker identifies a flaw related to access control and bypasses the authentication, which allows them to compromise the network.
Base64 Encoding: scheme represents any binary data using only printable ASCII characters.
Bug Bounty Program: challenge hosted by organizations, websites, or software developers to tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities.
Blind/Inferential SQL Injection: attacker poses a true or false question to the database to determine whether the application is vulnerable to SQL injection.
Blacklist Validation: rejects all the malicious inputs that have been disapproved for protected access.
Bandwidth: amount of information that may be broadcast over a connection.
Basic service set identifier (BSSID): media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS).
Bluetooth: short-range wireless communication technology that replaces the cables connecting portable or fixed devices while maintaining high levels of security.
Bluesmacking: an attacker sends an oversized ping packet to a victim's device, causing a buffer overflow.
BlueSniff: proof-of-concept code for a Bluetooth wardriving utility.
BluePrinting: footprinting technique performed by an attacker to determine the make and model of a target Bluetooth-enabled device.
Btlejacking: detrimental to Bluetooth low energy (BLE) devices. The attacker can sniff, jam, and

take control of the data transmission between BLE devices by performing an MITM attack.
Bluejacking: activity of sending anonymous messages over Bluetooth to Bluetooth-enabled devices, such as laptop and mobile phones, via the OBEX protocol.
Bluesnarfing: theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, PDAs, and other devices.
Bluebugging: gaining remote access to a target Bluetooth-enabled device and using its features without the victim's knowledge or consent.
BYOD: a policy that allows an employee to bring their personal devices, such as laptops, smartphones, and tablets, to their workplace and use them to access the organization's resources by following the access privileges.
BlueBorne Attack: performed on Bluetooth connections to gain access and take full control of the target device.
Business Network: It comprises of a network of systems that offer information infrastructure to the business.
Basic Process Control System (BPCS): responsible for process control and monitoring of the industrial infrastructure.
Blowfish: type of symmetric block cipher algorithm designed to replace DES or IDEA algorithms.
Confidentiality: Assurance that the information is accessible only to those authorized to have access.
Close-in Attacks: in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information.
Cyber Kill Chain Methodology: component of intelligence-driven defense for the identification and prevention of malicious intrusion activities.
Cyber Terrorists: individuals with a wide range of skills, motivated by religious or political beliefs, to create fear of large-scale disruption of computer networks.
Clearing Tracks: the activities carried out by an attacker to hide malicious acts.
Cyber Threat Intelligence: collection and analysis of information about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks.
Competitive Intelligence Gathering: process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources, such as the Internet.
Common Vulnerability Scoring System (CVSS): published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
Common Vulnerabilities and Exposures (CVE): publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures.
Common Weakness Enumeration (CWE): category system for software vulnerabilities and weaknesses.
Combinator Attack: entries of first dictionary joined with those of the second dictionary to generate a new wordlist to crack the password of the target system.
Crypter: Software that protects malware from undergoing reverse engineering or analysis, thus making the task of the security mechanism harder in its detection.
Computer Worms: malicious programs that independently replicate, execute, and spread across the network connections, thus consuming available computing resources without human interaction.

Chain Letters: Emails that offer free gifts such as money and software on condition that the user forwards the mail to a specified number of people.
Compromised Insider: An insider with access to critical assets of an organization who is compromised by an outside threat actor.
CRIME Attack: client-side attack that exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS.
Circuit-Level Gateway Firewall: monitor requests to create sessions and determine if those sessions will be allowed.
Cross-Site Scripting (XSS) Attacks: exploit vulnerabilities in dynamically generated web pages, enabling malicious attackers to inject client-side scripts into web pages viewed by other users.
Cross-Site Request Forgery (CSRF) Attack: exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend.
Clickjacking Attack: tricking the victim into clicking on any malicious web page element that is placed transparently on the top of any trusted web page.
Cookie Poisoning: type of parameter tampering attack in which the attacker modifies the cookie contents to draw unauthorized information about a user and thus perform identity theft.
Cookie Sniffing: technique in which an attacker sniffs a cookie containing the session ID of the victim who has logged in to a target website and uses the cookie to bypass the authentication process and log in to the victim's account.
Cookie Replay: technique used to impersonate a legitimate user by replaying the session/cookie that contains the session ID of that user (as long as he/she remains logged in).
Critical Infrastructure: A collection of physical or logical systems and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health.
Cloud Computing: on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.
Container-as-a-Service (CaaS): services for container engines, management of containers, applications, and clusters through a web portal, or an API.
Community Cloud: multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction.
Cloud Consumer: A person or organization that uses cloud computing services.
Cloud Provider: A person or organization providing services to interested parties.
Cloud Carrier: An intermediary for providing connectivity and transport services between cloud consumers and providers.
Cloud Auditor: A party for making independent assessments of cloud service controls and taking an opinion thereon.
Cloud Broker: An entity that manages cloud services in terms of use, performance, and delivery, and maintains the relationship between cloud providers and consumers.
Container: package of an application/software including all its dependencies such as library files, configuration files, binaries, and other resources that run independently of other processes in the cloud environment.
Container Orchestration: automated process of managing the lifecycles of software containers and their dynamic environments.
Cloud Cryptojacking: unauthorized use of the victim's computer to stealthily mine digital

currency.
Cloudborne Attack: vulnerability residing in a bare-metal cloud server that enables the attackers to implant a malicious backdoor in its firmware.
Cloud Security Alliance (CSA): nonprofit global organization that provides rising awareness and promotes best practices and security policies to help and secure the cloud environment.
Cryptography: conversion of data into a scrambled code that is encrypted and sent across a private or public network.
CAST-128: symmetric-key block cipher having a classical 12-or 16-round Feistel network with a block size of 64 bits.
Camellia: symmetric-key block cipher having either 18 rounds (for 128-bit keys) or 24 rounds (for 256-bit keys).
Cryptanalysis: study of ciphers, ciphertext, or cryptosystems with the ability to identify vulnerabilities in them and thus extract plaintext from ciphertext even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.
Distribution Attacks: attackers tamper with hardware or software prior to installation.
Defense-in-Depth: security strategy in which several protection layers are placed throughout an information system.
Deep web: web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines.
Dark Web or Darknet: subset of the deep web that enables anyone to navigate anonymously without being traced.
Dumpster Diving: the attacker rummaging for information in garbage bins.
DNS Cache Snooping: DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.
DNSSEC Zone Walking: DNS enumeration technique where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured.
Dictionary Attack: file containing common words is loaded into a password cracking application that runs against user accounts.
Distributed Network Attack: recovering passwords from hashes or password-protected files using the unused processing power of machines across the network.
Document Steganography: technique of hiding secret messages transferred in the form of documents.
Downloader: A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system.
Dropper: A type of Trojan that covertly installs other malware files on to the system.
Dynamic Malware Analysis: executing the malware code to know how it interacts with the host system and its impact on the system after infection.
DHCP Starvation Attack: denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope.
DNS Poisoning: technique that tricks a DNS server into believing that it has received authentic information when it has not received any.
DNS Cache Poisoning: altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.

Diversion Theft: The attacker tricks a person responsible for making a genuine delivery into delivering the consignment to a location other than the intended location.
DoS Attack: attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.
DDoS Attack: a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system.
Distributed Reflection Denial-of-Service (DRDoS) Attack: the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.
Demilitarized Zone (DMZ): area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data.
Database Honeypots: fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration.
DNS Server Hijacking: Attacker compromises the DNS server and changes the DNS settings so that all the requests are redirected to attacker server.
Directory Traversal: attackers to access restricted directories, including application source code, configuration, and critical system files to execute commands outside the web server's root application directory.
DNS Rebinding Attack: bypass the same-origin policy's security constraints, allowing the malicious web page to communicate with or make arbitrary requests to local domains.
Dynamic Application Security Testing (DAST): black-box testing approach and is performed directly on running code to identify issues related to interfaces, requests/responses, sessions, scripts, authentication processes, code injections, etc.
Direct-Sequence Spread Spectrum (DSSS): technique that multiplies the original data signal with a pseudo-random noise-spreading code.
Directional Antenna: broadcast and receive radio waves from a single direction.
Dipole Antenna: straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line.
Distributed Control System (DCS): highly engineered and large-scale control system that is often used to perform industry specific tasks.
Docker: open source technology used for developing, packaging, and running applications and all its dependencies in the form of containers, to ensure that the application works in a seamless environment.
Data Encryption Standard (DES): symmetrical encipher and decipher on blocks of data consisting of 64 bits under control of a 56-bit key.
DSA: Federal Information Processing Standard for digital signatures.
Diffie–Hellman: cryptographic protocol that allows two parties to establish a shared key over an insecure channel.
Digital Signature: asymmetric cryptography to simulate the security properties of a signature in digital rather than written form.
DUHK Attack: cryptographic vulnerability that allows an attacker to obtain encryption keys used to secure VPNs and web sessions.
DROWN Attack: cross-protocol weakness that can communicate and initiate an attack on

servers that support recent SSLv3/TLS protocol suites.
Email Indicators: used to send malicious data to the target organization or individual.
Ethical Hacking: the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security.
Eavesdropping: act of secretly listening to the conversations of people over a phone or video conference without their consent.
Enumeration: process of extracting usernames, machine names, network resources, shares, and services from a system or network.
Exploit: A malicious code that breaches the system security via software vulnerabilities to access information or install malware.
Exploit Kit: platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, and buffer overflow scripts to the target system.
Elicitation: Attackers extract information from the victim by engaging him/her in normal and disarming conversations.
Egress Filtering: scans the headers of IP packets leaving a network.
Email Honeypots: fake email addresses that are specifically used to attract fake and malicious emails from adversaries.
Error Based SQL Injection: forces the database to perform some operation in which the result will be an error.
Electronic Security Perimeter: It is referred to as the boundary between secure and insecure zones.
Elliptic Curve Cryptography: modern public-key cryptography developed to avoid larger cryptographic key usage.
Federal Information Security Management Act (FISMA): comprehensive framework for ensuring the effectiveness of information security controls over information resources that support U.S. government operations and assets.
Footprinting: first step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system.
Folder Steganography: hidden and encrypted within a folder and do not appear to normal Windows applications, including Windows Explorer.
Fileless Malware: infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities.
File Fingerprinting: process of computing the hash value for a given binary code.
Forbidden Attack: type of man-in-the-middle attack used to hijack HTTPS sessions.
Firewall: hardware or software designed to prevent unauthorized access to or from a private network.
Flooding: attacker sends large quantity of traffic.
Firewalking: technique that uses TTL values to determine gateway ACL filters and it maps networks by analyzing the IP packet responses.
Frequency-Hopping Spread Spectrum (FHSS): method of transmitting radio signals by rapidly switching a carrier among many frequency channels.
Fault Injection Attacks: perpetrator injects any faulty or malicious program into the system to compromise the system security.
Gray Hats: individuals who work both offensively and defensively at various times.

Gaining Access: the point where the attacker obtains access to the operating system or applications on the target computer or network.

Google Hacking Database: authoritative source for querying the ever-widening reach of the Google search engine.

Global System for Mobile Communications (GSM): universal system used for mobile data transmission in wireless networks worldwide.

GOST Block Cipher: symmetric-key block cipher having a 32-round Feistel network working on 64-bit blocks with a 256-bit key length.

GNU Privacy Guard: software replacement of PGP and free implementation of the OpenPGP standard.

Host-Based Indicators: found by performing an analysis of the infected system within the organizational network.

Hacking: exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources.

Hacker: person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks.

Hacktivist: Individuals who promote a political agenda by hacking, especially by defacing or disabling websites.

Hash Injection/Pass-the-Hash (PtH) Attack: to inject a compromised hash into a local session and use the hash to validate network resources.

Host Integrity Monitoring: taking a snapshot of the system state using the same tools before and after analysis, to detect changes made to the entities residing on the system.

Hardware Protocol Analyzer: piece of equipment that captures signals without altering the traffic in a cable segment.

Honey Trap: technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company.

Hoax Letters: Emails that issue warnings to the user about new viruses, Trojans, or worms that may harm the user's system.

HTTP GET/POST Attack: attackers use a time-delayed HTTP header to maintain HTTP connections and exhaust web server resources.

HTTP Strict Transport Security (HSTS): web security policy that protects HTTPS websites against MITM attacks.

HTTP Public Key Pinning (HPKP): trust on first use (TOFU) technique used in an HTTP header that allows a web client to associate a specific public key certificate with a particular server to minimize the risk of MITM attacks based on fraudulent certificates.

Honeypot: information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.

Honeynets: networks of honeypots. They are very effective in determining the entire capabilities of the adversaries.

HTTP Response-Splitting Attack: web-based attack in which the attacker tricks the server by injecting new lines into response headers, along with arbitrary code.

Hotfixes: an update to fix a specific customer issue and not always distributed outside the customer organization.

HTML Encoding: represent special characters so they can be safely combined within an HTML document.
Hotspot: areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.
Hybrid Cloud: cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but are bound together to offer the benefits of multiple deployment models.
HMAC: type of message authentication code (MAC) that combines a cryptographic key with a cryptographic hash function.
Homomorphic Encryption: to secure and leave their data in an encrypted format even while it is being processed or manipulated.
Hardware-Based Encryption: uses computer hardware for assisting or replacing the software when the data encryption process is underway.
HSM: additional external security device that is used in a system for crypto-processing and can be used for managing, generating, and securely storing cryptographic keys.
Hard Drive Encryption: technology where the data stored in the hardware can be encrypted using a wide range of encryption options.
Hash Collision Attack: finding two different input messages that result in the same hash output.
Integrity: The trustworthiness of data or resources in terms of preventing improper or unauthorized changes.
Information Warfare: the use of information and communication technologies (ICT) to gain competitive advantages over an opponent.
Indicators of Compromise: clues, artifacts, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.
Information Assurance: the assurance that the integrity, availability, confidentiality, and authenticity of information and information systems is protected during the usage, processing, storage, and transmission of information.
Incident Management: set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent future recurrence of the incident.
Incident Handling and Response: process of taking organized and careful steps when reacting to a security incident or cyberattack.
ISO/IEC 27001: specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.
Impersonation: Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information.
ICMP ECHO Ping Scan: sending ICMP ECHO requests to a host. If the host is live, it will return an ICMP ECHO reply.
ICMP ECHO Ping Sweep: determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.
Inverse TCP Flag Scan: Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, where no response implies that the port is open, whereas an RST response means

that the port is closed.
IP Address Decoy: generating or manually specifying the IP addresses of decoys in order to evade an IDS or firewall.
IP Address Spoofing: changing the source IP addresses so that the attack appears to be coming from someone else.
Image Steganography: information is hidden in image files of different formats such as .PNG, .JPG, and .BMP.
Injector: A program that inserts its code into other vulnerable running processes and changes how they execute to hide or prevent its removal.
IRDP Spoofing: spoofed router advertisement message sent to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
Insider Attack: using privileged access to intentionally violate rules or cause threat to the organization's information or information systems in any form.
Identity Theft: crime in which an imposter steals your personally identifiable information such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes.
ICMP Flood Attack: a type of attack in which attackers send large volumes of ICMP echo request packets to a victim system directly or through reflection networks.
Ingress Filtering: prevents the source address spoofing of Internet traffic.
IPSec: protocol suite developed by the IETF for securing IP communications by authenticating and encrypting each IP packet of a communication session.
Intrusion Detection System (IDS): software system or hardware device that inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach.
Intrusion Prevention System (IPS): continuous monitoring systems that often sit behind firewalls as an additional layer of protection.
Insertion Attack: process where attacker confuses the IDS by forcing it to read invalid packets.
Injection Flaws: web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.
In-band SQL Injection: An attacker uses the same communication channel to perform the attack and retrieve the results.
Input Validation: helps developers to prevent user-supplied data influencing the logic of the code.
Industrial, Scientific, and Medical Band: set of wireless frequencies
iOS Trustjacking: vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge.
IoT: the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors.
Industrial Network: A network of automated control systems is known as an industrial network.
Industrial Protocols: Protocols used for serial communication and communication over standard Ethernet. S7, CDA, CIP, Modbus.
IT/OT Convergence (IIOT): integration of IT computing systems and OT operation monitoring systems to bridge the gap between IT/OT technologies for improving overall security, efficiency, and productivity.

Infrastructure-as-a-Service (IaaS): This service provides virtual machines and other abstracted hardware and operating systems (OSs), which may be controlled through a service application programming interface (API).

Identity-as-a-Service (IDaaS): This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services.

Jailbreaking: process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor.

Jamming Attack: type of attack in which the communications between wireless IoT devices are jammed so that they can be compromised.

Kerberos: network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography.

Keylogger: programs or hardware devices that monitor each keystroke as the user types on a keyboard, logs onto a file, or transmits them to a remote location.

Key Negotiation of Bluetooth (KNOB) attack: breach Bluetooth security mechanisms and perform am MITM attack on paired devices.

Kubernetes: open-source, portable, extensible, orchestration platform developed by Google for managing containerized applications and microservices.

Key Stretching: the process of strengthening a key that might be slightly too weak, usually by making it longer.

LDAP: Internet protocol for accessing distributed directory services.

Lawful Interception: legally intercepting data communication between two end points for surveillance on the traditional telecommunications, Voice over Internet Protocol (VoIP), data, and multiservice networks.

LDAP Injection Attack: exploits user parameters to generate an LDAP query.

Maintaining Access: the phase when the attacker tries to retain their ownership of the system.

Management Information Base (MIB): virtual database containing a formal description of all the network objects that can be managed using SNMP.

Markov-Chain Attack: Attackers gather a password database and split each password entry into 2-and 3-character long syllables; using these character elements, a new alphabet is developed, which is then matched with the existing password database.

Malware: malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.

Malicious Code: A command that defines malware's basic functionalities such as stealing data and creating backdoors.

Malware Analysis: process of reverse engineering a specific piece of malware to determine the origin, functionality, and potential impact of a given type of malware.

MAC Flooding: the flooding of the CAM table with fake MAC address and IP pairs until it is full.

MAC Spoofing/Duplicating: actively associated with a switch port and re-using one of those addresses.

Malicious Insider: A disgruntled or terminated employee who steals data or destroys the company's networks intentionally by introducing malware into the corporate network.

Multi-Vector Attack: attackers use combinations of volumetric, protocol, and application-layer attacks to disable the target system or service.

Man-in-the-Middle Attack: used to intrude into an existing connection between systems and intercept the messages being exchanged.
Man-in-the-Browser Attack: uses a Trojan horse to intercept the calls between the browser and its security mechanisms or libraries.
Malware Honeypots: used to trap malware campaigns or malware attempts over the network infrastructure.
MarioNet Attack: browser-based attack that runs malicious code inside the browser, and the infection persists even after closing or browsing away from the malicious webpage through which infection has spread.
Manual Web App Security Testing: testing a web application using manually designed data, customized code, and some browser extension tools to detect vulnerabilities and weaknesses associated with the applications.
Mobile Spam: unsolicited messages sent in bulk form to known/unknown phone numbers/email IDs to target mobile phones.
Mobile Device Management (MDM): platforms for over-the-air or wired distribution of applications and data and configuration settings for all types of mobile devices.
Multi Cloud: dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals.
Microservices: Monolithic applications are broken down into cloud-hosted sub-applications called microservices that work together, each performing a unique task.
Man-in-the-Cloud (MITC) Attack: performed by abusing cloud file synchronization services such as Google Drive or Drop Box for Data compromise, command and control (C&C), data exfiltration, and remote access.
MD5: algorithm takes a message of arbitrary length as the input and then outputs a 128-bit fingerprint or message digest of the input.
Non-Repudiation: A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
Network Indicators: useful for command and control, malware delivery, identifying the operating system, and other tasks.
Network Scanning: a set of procedures used for identifying hosts, ports, and services in a network.
Network Time Protocol (NTP): synchronize the clocks of networked computers.
National Vulnerability Database (NVD): A U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).
NTFS Data Stream: Windows hidden stream, which contains metadata for the file, such as attributes, word count, author name and access, and modification time of the files.
Negligent Insider: uneducated on potential security threats or who simply bypass general security procedures to meet workplace efficiency.
Network Level Hijacking: interception of packets during the transmission between a client and the server in a TCP or UDP session.
Network Address Translation (NAT): separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic separately.

Network Perimeter: outermost boundary of a network zone i.e. closed group of assets.
OS Discovery/Banner Grabbing: method used to determine the operating system running on a remote target system.
Obfuscator: A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it.
Obfuscating: IDS evasion technique used by attackers who encode the attack packet payload in such a way that the destination host can decode the packet but not the IDS.
OAuth: authorization protocol that allows a user to grant limited access to their resources on a site to a different site without having to expose their credentials.
Output Encoding: input is properly sanitized before being passed to database.
Orthogonal Frequency-Division Multiplexing (OFDM): method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other.
Omnidirectional Antenna: radiate electromagnetic (EM) energy in all directions.
OT: software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices.
Operational Technology Cyber Security Alliance (OTCSA): educates operators and manufacturers with constant technical awareness and provides guidelines to apply essential changes, updates, integrations, etc.
Passive Attacks: intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data.
Procedures: organizational approaches that threat actors follow to launch an attack.
Payment Card Industry Data Security Standard (PCI DSS): proprietary information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards.
Passive Footprinting: gathering information about the target without direct interaction.
Packet Fragmentation: the splitting of a probe packet into several smaller packets (fragments) while sending it to a network.
Proxy Server: application that can serve as an intermediary for connecting with other computers.
Password Cracking: used to recover passwords from computer systems.
Password Guessing: attempting to log on to the target system with different passwords manually.
Pass the Ticket Attack: technique used for authenticating a user to a system that is using Kerberos without providing the user's password.
PRINCE Attack: An advanced version of a combinator attack where instead of taking input from two different dictionaries, attackers use a single input dictionary to build chains of combined words.
Password Salting: technique where a random string of characters are added to the password before calculating their hashes.
Privilege Escalation: process of gaining more privileges than were initially acquired.
Packer: A program that allows all files to bundle together into a single executable file via compression to bypass security software detection.
Payload: A piece of software that allows control over a computer system after it has been

exploited.
Packet Sniffing: process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.
Passive Sniffing: monitoring packets sent by others without sending any additional data packets in the network traffic.
Piggybacking: entry into a building or security area with the consent of the authorized person.
Pop-Up Windows: Windows that suddenly pop up while surfing the Internet and ask for user information to login or sign-in.
Phishing: practice of sending an illegitimate email claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.
Pharming: social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website.
Professional Insider: Harmful insiders who use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black market bidders.
Ping of Death Attack: sending malformed or oversized packets using ICMP for denial of service
Pulse Wave DDoS Attack: attackers send a highly repetitive, periodic train of packets as pulses to the target victim every 10 minutes, and each specific attack session can last for a few hours to days.
Peer-to-Peer Attack: form of DDoS attack in which the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack.
Permanent Denial-of-Service Attack: attacks that cause irreversible damage to system hardware.
Protocol Anomaly Detection: built to explore anomalies in the way in which vendors deploy the TCP/IP specification.
Packet Filtering Firewall: layer 3 header is compared to a set of criteria before it is forwarded.
Production Honeypots: deployed inside the production network of the organization along with other production servers.
Port Scanning: identify open ports and the services running on these ports.
Patch: small piece of software designed to fix problems, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data.
Patch Management: process used to fix known vulnerabilities by ensuring that the appropriate patches are installed on a system.
Parabolic Grid Antenna: semi-dish in the form of a grid consisting of aluminum wires.
Purdue Model: widely used to describe internal connections and dependencies of important components in the ICS networks.
Programmable Logic Controller (PLC): small solid-state control computer where instructions can be customized to perform a specific task.
Platform-as-a-Service (PaaS): This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications.
Public Cloud: In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet.

Private Cloud: cloud infrastructure operated by a single organization and implemented within a corporate firewall.
Public Key Infrastructure (PKI): set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
Pretty Good Privacy (PGP): It is often used for data compression, digital signing, encryption and decryption of messages, emails, files, and directories, and to enhance the privacy of email communications.
Padding Oracle Attack: attackers exploit the padding validation of an encrypted message to decipher the ciphertext.
Reconnaissance: the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
Risk: the degree of uncertainty or expectation that an adverse event may cause damage to the system.
Risk Management: process of reducing and maintaining risk at an acceptable level by means of a well-defined and actively employed security program.
Risk Identification: Identifies the sources, causes, consequences, and other details of the internal and external risks affecting the security of the organization.
Risk Assessment: Assesses the organization's risk and provides an estimate of the likelihood and impact of the risk.
Risk Treatment: Selects and implements appropriate controls for the identified risks.
Risk Tracking: Ensures appropriate controls are implemented to handle known risks and calculates the chances of a new risk occurring.
Risk Review: Evaluates the performance of the implemented risk management strategies.
Remote Procedure Call: allows clients and servers to communicate in distributed client/server programs.
Replay Attack: packets and authentication tokens are captured using a sniffer. After the relevant information is extracted, the tokens are placed back on the network to gain access.
Rainbow Table: precomputed table that contains word lists like dictionary files, brute force lists, and their hash values.
Rootkits: programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time, and in the future.
Ransomware: type of malware that restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) to remove the restrictions.
Rogue DHCP Server Attack: The attacker sets server on the network the responds to DHCP requests with bogus IP addresses resulting in compromised network access.
Reverse Social Engineering: The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs.
RST Hijacking: injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgment number.
Research Honeypots: high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders.
Runtime application self protection: provides security to web and non-web application running on a server.

Reflector Antennas: used to concentrate EM energy that is radiated or received at a focal point.

Reverse Engineering: process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications.

RC4: variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation.

RC5: fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security).

RC6: symmetric-key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds.

Rivest Shamir Adleman (RSA): public-key cryptosystem for Internet encryption and authentication.

RIPEMD-160: 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel.

Rainbow Table Attack: type of cryptography attack where an attacker uses a rainbow table to reverse cryptographic hash functions.

Related-Key Attack: attack by exploiting the mathematical relationship between keys in a cipher to gain access over encryption and decryption functions.

Suicide Hackers: individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail terms or any other kind of punishment.

Script Kiddies: unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers.

State-Sponsored Hackers: individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.

Scanning: the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.

Supervised Learning: algorithms that input a set of labeled training data to attempt to learn the differences between the given labels.

Sarbanes Oxley Act: U.S.regulation to protect the public and investors by increasing the accuracy and reliability of corporate disclosures.

Shoulder Surfing: attacker stands behind the victim and secretly observes the victim’s activities on the computer, such as keystrokes while entering usernames, passwords, and so on.

Stealth Scan (Half-open Scan): abruptly resetting the TCP connection between the client and server before the completion of three-way handshake signals, thus leaving the connection half-open.

SCTP INIT Scanning: Attackers send an INIT chunk to the target host, and an INIT+ACK chunk response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.

SCTP COOKIE ECHO Scanning: Attackers send a COOKIE ECHO chunk to the target host, and no response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.

Source Routing: sending a packet to the intended destination with a partially or completely specified route (without firewall-/IDS-configured routers) in order to evade an IDS or firewall.

Source Port Manipulation: manipulating actual port numbers with common port numbers in order to evade an IDS or firewall.

SNMP Enumeration: process of enumerating user accounts and devices on a target system using SNMP.
Spyware: stealthy program that records the user's interaction with the computer and the Internet without the user's knowledge and sends the information to the remote attackers.
Steganography: technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
Spam/Email Steganography: the technique of sending secret messages by hiding them in spam/email messages.
Steganalysis: art of discovering and rendering covert messages using steganography.
Sheep Dip Computer: the analysis of suspect files, incoming messages, etc. for malware.
Static Malware Analysis: going through the executable binary code without executing it to have a better understanding of the malware and its purpose.
System Baselining: the process of capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system's state after executing the malware file.
SPAN Port: port that is configured to receive a copy of every packet that passes through a switch.
STP Attack: Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic.
Social Engineering: art of convincing people to reveal confidential information.
Spam Email: Irrelevant, unwanted, and unsolicited emails that attempt to collect financial information, social security numbers, and network information.
Scareware: Malware that tricks computer users into visiting malware infested websites, or downloading/buying potentially malicious software.
Spear Phishing: Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people.
Spimming: A variant of spam that exploits Instant Messaging platforms to flood spam across the networks.
SMiShing: act of using SMS text messaging system of cellular phones or other mobile devices to lure users into instant action, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.
Smurf Attack: attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network.
SYN Flood Attack: attacker sends a large number of SYN requests to the target server (victim) with fake source IP addresses.
Spoofed Session Flood Attack: Attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets.
Session Hijacking: an attack in which an attacker seizes control of a valid TCP communication session between two computers.
Signature Recognition: misuse detection, tries to identify events that indicate an abuse of a system or network resource.
Software Firewall: software program installed on a computer, just like normal software.
Stateful Multilayer Inspection Firewall: combine the aspects of (Packet Filtering, Circuit-Level Gateways, and Application-Level Firewalls).

Spam Honeypots: specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies.
Spider Honeypots: also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders.
Session Splicing: technique used to bypass the IDS where an attacker splits the attack traffic into many packets such that no single packet triggers the IDS.
Static Application Security Testing (SAST): white-box testing, complete system architecture (including its source code) or application/software to be tested is already known to the tester.
Source Code Review: used to detect bugs and irregularities in the developed web applications.
16-bit Unicode Encoding: It replaces unusual Unicode characters with "%u" followed by the character's Unicode code point expressed in hexadecimal.
SQL Injection: technique used to take advantage of un-sanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database.
Service Set Identifier (SSID): 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network.
Simjacker: vulnerability associated with a SIM card's S@T browser (SIMalliance Toolbox Browser), a pre-installed software incorporated in SIM cards to provide a set of instructions.
Sybil Attack: The attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks.
Side-Channel Attack: The attacker extracts information about encryption keys by observing the emission of signals i.e. "side channels" from IoT devices.
Supervisory Control and Data Acquisition (SCADA): centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure.
Safety Instrumented Systems (SIS): automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in the industry.
Software-as-a-Service (SaaS): This cloud computing service offers application software to subscribers on-demand over the Internet.
Security-as-a-Service (SECaaS): It provides services such as penetration testing, authentication, intrusion detection, anti-malware, security incident and event management.
Serverless Computing: cloud-based application architecture where application infrastructure and supporting services are provided by the cloud vendor as they are needed.
Symmetric Encryption: uses the same key for encryption as it does for decryption.
Serpent: 128-bit symmetric block cipher with 128-, 192-, or 256-bit key sizes.
Secure Hashing Algorithm (SHA): This algorithm generates a cryptographically secure one-way hash; it was published by the National Institute of Standards and Technology as a US Federal Information Processing Standard.
Secure Sockets Layer (SSL): application layer protocol developed by Netscape for managing the security of message transmission on the Internet.
Tactics, Techniques, and Procedures (TTPs): the patterns of activities and methods associated with specific threat actors or groups of threat actors.
Tactics: guidelines that describe the way an attacker performs the attack from beginning to the end.
Techniques: technical methods used by an attacker to achieve intermediate results during the attack.

Threat Modeling: risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application.
The Digital Millennium Copyright Act (DMCA): It defines the legal prohibitions against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information.
Traceroute: program uses ICMP protocol and TTL field to discover routers on the path to a target host.
Toggle-Case Attack: Attackers try all possible combinations of upper and lower cases of a word present in the input dictionary.
Trojan: program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that the code can get control and cause damage, such as ruining the file allocation table on your hard disk.
Tailgating: accessing a building or secured area without the consent of the authorized person.
Throttling: the setting up of routers for server access with a logic to throttle incoming traffic levels that are safe for the server.
TCP/IP Hijacking: using spoofed packets to seize control of a connection between a victim and target machine.
Two-Factor Authentication: authentication in addition to a user's password.
Twofish: Feistel cipher.
Threefish: large tweakable symmetric-key block cipher in which the block and key sizes are equal, i.e., 256, 512, and 1024.
TEA: Feistel cipher that uses 64 rounds.
TPM: crypto-processor or chip that is present on the motherboard that can securely store the encryption keys, and it can perform many cryptographic operations.
Transport Layer Security (TLS): protocol to establish a secure connection between a client and a server and ensure the privacy and integrity of information during transmission.
Unsupervised Learning: algorithms that input unlabeled training data to attempt to deduce all the categories without guidance.
UDP Ping Scan: Attackers send UDP packets to target hosts, and a UDP response indicates that the host is active.
UDP Flood Attack: An attacker sends spoofed UDP packets at a very high packet rate to a remote host on random ports of a target server using a large source IP range.
UDP Hijacking: A network-level session hijacking where the attacker sends forged server reply to a victim's UDP request before the intended server replies to it.
URL Encoding: process of converting URL into valid ASCII format so that data can be safely transported over HTTP.
UTF-8: variable-length encoding standard that uses each byte expressed in hexadecimal and preceded by the % prefix.
Union SQL Injection: an attacker combines a forged query with a query requested by the user using a UNION clause.
USB Encryption: additional feature for USB storage devices that offers onboard encryption services.
Vulnerability Research: process of analyzing protocols, services, and configurations to discover

the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.
Vulnerability Assessment: in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand the exploitation.
Vulnerability Exploitation: the execution of multiple complex, interrelated steps to gain access to a remote system.
Video Steganography: hiding secret information in a carrier video file.
Virus: self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.
Vishing: impersonation technique (electronic fraud) in which the attacker tricks individuals to reveal personal and financial information using voice technology such as the telephone system, VoIP, etc.
VPN: private network constructed using public networks, such as the Internet.
Vulnerability Scanning: identify vulnerabilities and misconfigurations.
White Hats: individuals who use their hacking skills for defensive purposes.
Website Footprinting: the monitoring and analysis of the target organization's website for information.
Whois: query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system.
Wire Sniffing: form of wire sniffing or wiretapping in which hackers sniff credentials during transit by capturing Internet packets.
Windows Management Instrumentation (WMI): feature in Windows administration that provides a platform for accessing Windows system resources locally and remotely.
Windows Remote Management (WinRM): Windows-based protocol designed to allow a user to run an executable file, modify system services, and the registry on a remote system.
Whitespace Steganography: user hides the messages in ASCII text by adding white spaces to the ends of the lines.
Wiretapping: process of the monitoring of telephone and Internet conversations by a third party.
Whaling: type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information.
Web Server: computer system that stores, processes, and delivers web pages to clients via HTTP.
Website Defacement: unauthorized changes made to the content of a single web page or an entire website, resulting in changes to the visual appearance of the web page or website.
Web Server Misconfiguration: configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft.
Website Mirroring: copy an entire website and its content onto a local drive.
Web Applications: interface between end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser.
Web Service: application or software that is deployed over the Internet and uses standard

messaging protocols such as SOAP, UDDI, WSDL, and REST to enable communication between applications developed for different platforms.
Web-based Timing Attack: type of side-channel attack performed by attackers to retrieve sensitive information such as passwords from web applications by measuring the response time taken by the server.
Web Spidering/Crawling: automatically discover the hidden content and functionality by parsing HTML forms and client-side JavaScript requests and responses.
WS-Address Spoofing: attacker sends a SOAP message containing fake WS-address information to the server. The header consists of the address of the endpoint selected by the attacker rather than the address of the web service client.
Web API: application programming interface that provides online web services to client-side apps for retrieving and updating data from multiple online sources.
Webhooks: user-defined HTTP callback or push APIs that are raised based on events triggered, such as receiving a comment on a post or pushing code to the registry.
Web Shell: malicious piece of code or script that is developed using server-side languages such as PHP, ASP, PERL, RUBY, and Python and are then installed on a target server.
Web Application Fuzz Testing: black-box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications.
Whitelist Validation: effective technique in which only the list of entities that have been approved for secured access are accepted.
Wi-Fi: WLANs based on IEEE 802.11 standard, which allows the device to access the network from anywhere within an AP range.
Wired Equivalent Privacy (WEP): security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN.
Wi-Fi Protected Access (WPA): security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication.
WPA2: upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES-based encryption mode with strong security.
WPA3: advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm.
Wireless Intrusion Prevention Systems: protect networks against wireless threats and enable administrators to detect and prevent various network attacks.
Wrapping Attack: performed during the translation of the SOAP message in the TLS layer where attackers duplicate the body of the message and sends it to the server as a legitimate user.
Web of Trust (WOT): trust model of PGP, OpenPGP, and GnuPG systems.
Xmas Scan: type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device.
XML External Entity Attack: server-side request forgery (SSRF) attack that can occur when a misconfigured XML parser allows applications to parse XML input from an unreliable source.
Yagi Antenna: unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF.

YAK: public-key-based Authenticated Key Exchange (AKE) protocol.
Zones and Conduits: network segregation technique used to isolate the networks and assets to impose and maintain strong access control mechanisms.
Zero Trust Network: security implementation that assumes that every user trying to access the network is not a trusted entity by default and verifies every incoming connection before allowing access to the network.