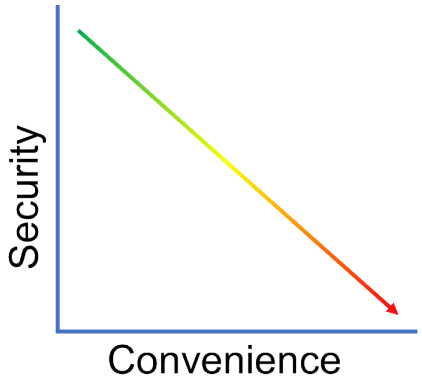
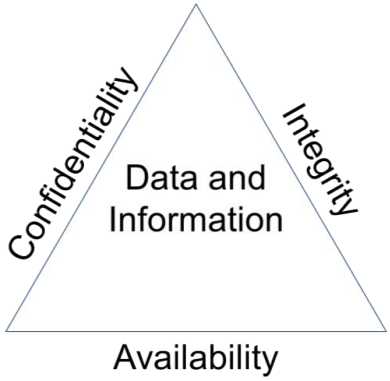
COMPTIA SECURITY+

Overview of security



CIA Triad



Confidentiality - Information has not been disclosed to unauthorized people
Integrity - Information has not been modified or altered without proper authorization
Availability - Information is able to be stored, accessed, or protected at all times

1.0 THREATS, ATTACKS AND VULNERABILITIES

Threat vector: The method or path used by a threat actor to compromise a target.
Threat actor: An individual or group who is responsible for carrying out a threat.
Threat target: A system, organization, or asset that is targeted by a threat actor.
Transitive Access Attack: An attack in which an attacker gains access to a resource by exploiting a trust relationship between two systems. The attacker gains access to one system, then uses that access to gain access to another system.
Lateral movement - moves to systems at the same trust level. This can provide access to new data or different views of the network depending on how the systems and security are configured.
Vertical movement - is sometimes referenced when gaining access to systems or accounts with a higher security or trust level.
Maneuver - CompTIA defines "maneuver" in the context of threat hunting as how to think like a malicious user to help you identify potential indicators of compromise in your environment.

Pillaging - is a term that refers to the act of looting or plundering a town, city, or other location. In the context of information security, the term "data pillaging" can refer to the unauthorized access, theft, and exfiltration of sensitive data from a network or system by a malicious actor.

Refactoring/obsfucation - a program by automated means can include adding additional text, comments, or nonfunctional operations to make the program have a different signature without changing its operations. This is typically not a manual operation due to the fact that antimalware tools can quickly find new versions. Instead, refactoring is done via a polymorphic or code mutation technique that changes the malware every time it is installed to help avoid signature-based systems.

Attacks

Malware

Virus - Malicious code that runs on a machine without the user's knowledge and infects the computer when executed. **Viruses** require a user action in order to reproduce and spread

- **Boot sector** - Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up
- **Macro** - Virus embedded into a document and is executed when the document is opened by the user
- **Program** - Program viruses infect an executable or application
- **Multipartite** - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
- **Encrypted**
- **Polymorphic** - Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection
- **Metamorphic** - Virus that is able to rewrite itself entirely before it attempts to infect a file (advanced version of polymorphic virus)
- **Stealth**
- **Armored -** Armored viruses have a layer of protection to confuse a program or person analyzing it

Malware: A malicious software that performs bad functions to our computer or other devices on the network.

Crypto-malware: A malicious program that encrypts programs and files on the computer in order to extort money from the user.

Ransomware: Denies access to a computer system or data until a ransom is paid. Can be spread through a phishing email or unknowingly infected website.

Worm: A self-contained infection that can spread itself through networks, emails, and messages.

Trojan: A form of malware that pretends to be a harmless application.

Rootkit: A backdoor program that allows full remote access to a system.

Keylogger: A malicious program that saves all of the keystrokes of the infected machine.

Bots: AI that when inside an infected machine performs specific actions as a part of a larger entity known as a botnet.

RAT - A remote access Trojan (RAT) is malware that gives the attacker remote access to the victim's machine.

Logic bomb: A malicious program that lies dormant until a specific date or event occurs.
Backdoor: Allows for full access to a system remotely.
Potentially unwanted programs (PUP) - Though not directly malicious, they can pose risks to user privacy as well as create annoyances like popups or other unwanted behaviors.

- **Spyware** - Malware that secretly gathers information about the user without their consent. Captures keystrokes made by the victim and takes screenshots that are sent to the attacker
- **Adware** - Displays advertisements based upon its spying on you
- **Grayware** - Software that isn't benign nor malicious and tends to behave improperly without serious consequences.
- **Easter Egg** - Non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature.
- **SPIM** - Unsolicited commercial messages sent via an instant messaging system.

Social Engineering attacks

Social engineering: The practice of using social tactics to gain information from people or get people to do something.
Prepending - refers to when an attacker prepends, or attaches, a trustworthy value like "RE:" or "MAILSAFE: PASSED" to a message in order to make the message appear more trustworthy.

Pretexting – building false sense of trust. is a social engineering technique where attackers use a reason that is intended to be believable to the target for what they are doing.
Phishing: Sending a false email pretending to be legitimate to steal valuable information from the user.
Smishing - a term that combines SMS and phishing.
Spear phishing: Attacks that target specific users with inside information.
Whaling: An attack on a powerful or wealthy individual like a CEO.
Vishing: An attack through a phone or voice communications.
Tailgating: Closely following individuals with keys to get access to secure areas.
Impersonation: Taking on the identity of an individual to get access into the system or communications protocol.
Dumpster diving: Going through a business's or person's trash to find thrown away valuable information or possessions.
Shoulder surfing: Watching as a person enters information.
Hoax: False information that deceives the user into compromising security by making them believe they are at risk.
Watering hole attack: A security attack that targets a specific highly secured group by infecting a commonly visited website by the group's members.

Elicitation (wydobycie informacji) - the process of eliciting information through conversation to gather useful information, is a key tool in a penetration tester's social engineering arsenal.
Insider Threat - Most dangerous threat to organizational security, A person who works for or with your organization but has ulterior motives. Employees who steal your information are insider threats.
Diversion Theft - When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.

Principles (reasons for effectiveness):

Authority: The actor acts as an individual of authority.
Intimidation: Frightening or threatening the victim.
Consensus (social proof): Convince based on what's normally expected.
Scarcity: Limited resources and time to act.
Familiarity: The victim is well known.
Trust: Gain their confidence, be their friend.
Urgency: Limited time to act, rush the victim.

Weaknesses in applications

Cookie is a small text file that a website stores on a user's computer. Cookies can be used to store information about a user's preferences, login information, and browsing history. They can also be used for tracking purposes, which can be a security concern.

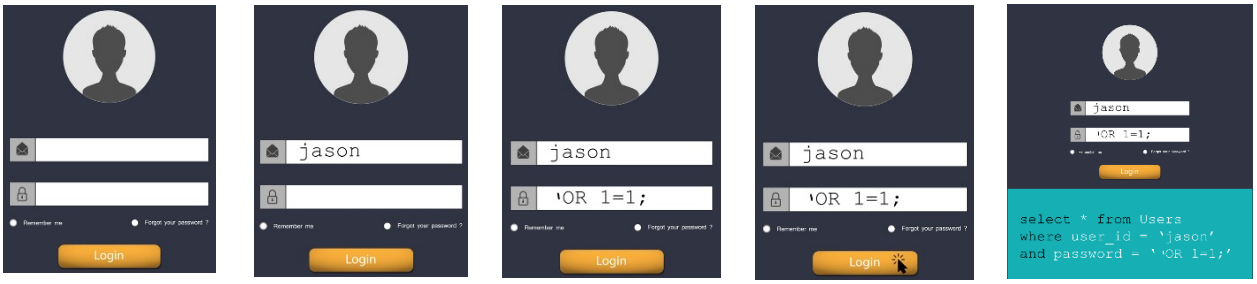
- **Flash cookie/Locally Shared Object (LSO)** is a type of cookie that is stored on a user's computer by Adobe Flash. Unlike traditional cookies, LSOs can store more data and persist even after a user has deleted their regular cookies.

Attachment is a file that is attached to an email message or other type of communication. Attachments can be used to deliver malware, such as viruses, to a user's computer.
Malicious add-on is a type of software that is designed to cause harm to a user's computer or compromise sensitive information. Malicious add-ons can be installed on a user's computer through phishing attacks or by visiting a malicious website.
Header manipulation refers to the practice of modifying the header information in a communication, such as an email message. This can be used to trick a user into thinking that a message came from a trusted source, or to hide the true source of the message.
Local File Inclusion (LFI) is a type of web application vulnerability that allows attackers to include local files in a web page or application. This can allow attackers to access sensitive information or execute malicious code on the server.
Remote File Inclusion (RFI) is a type of web application vulnerability that allows attackers to include remote files in a web page or application. This can allow attackers to execute malicious code on the server and gain control over the system.

Examples of attacks

Eavesdropping - Near-field communication (NFC) is susceptible to an attacker eavesdropping on the signal. is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission.

SQL Attack (Structured Query Language) is a type of attack that exploits vulnerabilities in a web application's database management system to extract sensitive information or compromise the database. These attacks typically involve sending malicious SQL commands to the database, such as SQL injection attacks.



Integer overflow attack is a type of attack that exploits a vulnerability in software when an arithmetic operation results in a value that is too large to be stored in an integer variable. This can cause the variable to wrap around to a negative value, potentially allowing an attacker to execute arbitrary code on the affected system.

Downgrade attack is a type of attack that involves forcing a communication channel to use a less secure protocol or encryption method. This can make it easier for attackers to intercept and manipulate network traffic.

Directory traversal/command injection attack is a type of attack that exploits a vulnerability in a web application to execute arbitrary commands or access sensitive files on the server. The attacker can use techniques such as directory traversal or command injection to manipulate the web application into executing malicious commands or accessing sensitive files.

Buffer overflow attack is a type of attack that exploits a vulnerability in software by sending more data to a buffer than it can hold. This can cause the data in the buffer to overflow into adjacent memory, potentially allowing an attacker to execute arbitrary code on the affected system.

Variable A and B before buffer overflow

Variable Name	A								B	
Value	[null string]								1979	
Hex Value	00	00	00	00	00	00	00	00	07	BB

Overflowing variable A changes variable B

Variable Name	A								B	
Value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856	
Hex Value	65	78	63	65	73	73	69	76	65	00

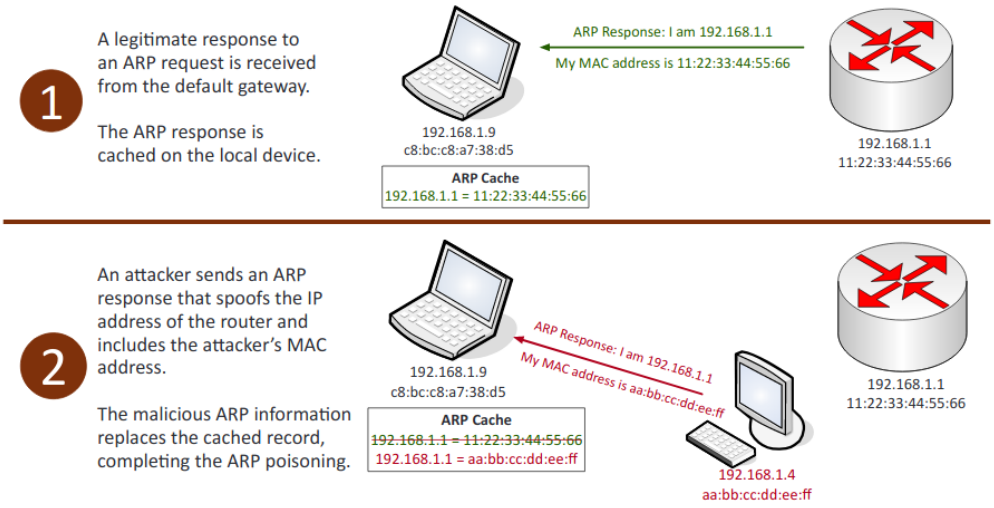
Injection: Occurs from processing invalid data, inserts code into the vulnerable computer program and changes the course of execution.

- **LDAP (Lightweight Directory Access Protocol) injection attack** is a type of attack that exploits a vulnerability in an application's LDAP implementation to extract sensitive information or compromise the application. These attacks typically involve sending malicious LDAP commands to the application's LDAP server.
- **XML (Extensible Markup Language) injection attack** is a type of attack that exploits a vulnerability in a web application's XML processing to extract sensitive information or

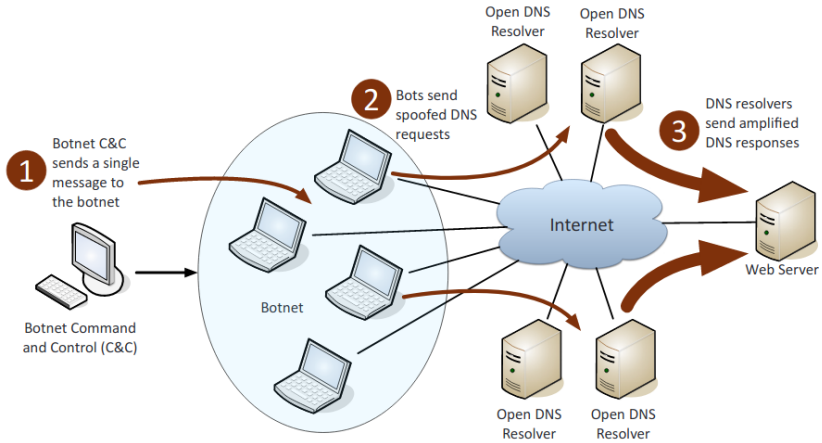
compromise the application. These attacks typically involve injecting malicious XML data into the application, which can be used to steal sensitive information or execute arbitrary code.

- **DLL injection** - the malware attempts to inject code into the process of some library.

Privilege escalation: An attack that exploits a vulnerability that allows them to gain access to resources that they normally would be restricted from accessing.



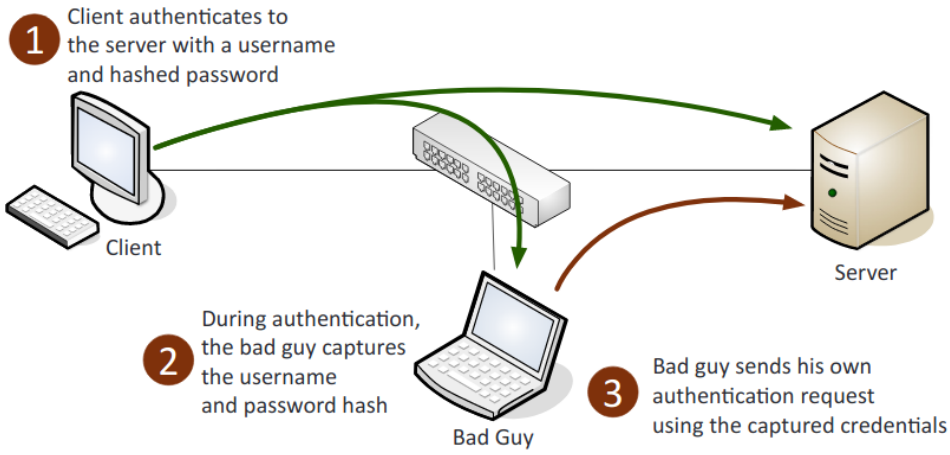
ARP poisoning: The act of falsifying the IP-to-MAC address resolution system employed by TCP/IP. Allows an attacker to essentially take over any sessions within the LAN. ARP Poisoning is prevented by VLAN segmentation and DHCP snooping



MAC flooding attacks - attempt to overflow a switch's CAM table, causing the switch to send all traffic to all ports rather than to the port that a given MAC address is associated with. Although this was possible with many older switches, most modern switches are less susceptible to this type of attack, and some have security capabilities built in to prevent this type of attack.

Zero day: The aim is to exploit flaws or vulnerabilities in targeted systems that are unknown or undisclosed to the world in general. Meaning that there is no direct or specific defense to the attack; which puts most systems vulnerable assets at risk.

Replay: Is a network-based attack where a valid data transmission is rebroadcasted, repeated, or delayed.



Pass the hash: An authentication attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is commonly associated with the Microsoft NTLM (New Technology LAN Manager) protocol.

Driver manipulation:

- **Shimming**: The process of injecting alternate or compensation code into a system in order to alter its operations without changing the original or existing code.
- **Refactoring**: Rewrites the internal processing of code without changing its behavior.

MAC spoofing: The attacker falsifies the MAC address of a device.

IP spoofing: An intruder uses another site's IP address to masquerade as a legitimate site.

SQL Injection vs XSS vs XSRF vs CSRF

SQL injection attacks target the database behind a web application. The attacker injects malicious SQL code into a vulnerable input field, which the web application processes and executes, resulting in unauthorized access to the database. To identify SQL injection attacks, look for suspicious SQL queries in your application logs.

- Example 1: SELECT * FROM users WHERE username = 'admin' AND password = '123456' OR 1=1;
- Example 2: SELECT * FROM users WHERE id = 1; DROP TABLE users;
- Example 3: INSERT INTO users (username, password) VALUES ('admin', 'password'); SELECT * FROM users;

Cross Site Scripting (XSS) attack is a type of web-based attack that exploits vulnerabilities in a web application to inject malicious code into a web page viewed by other users. The injected code can steal sensitive information from the victim's browser, such as login credentials or personal information. To identify XSS attacks, look for suspicious scripts in your application logs.

- Stored/Persistent - Attempts to get data provided by the attacker to be saved on the web server by the victim
- Reflected - Attempts to have a non-persistent effect activated by a victim clicking a link on the site
- DOM-based - Attempt to exploit the victim's web browser

XSS is a client-side vulnerability that targets other application users, while SQL injection is a server-side vulnerability that targets the application's database.

XSRF (Cross-Site Request Forgery): occur when an attacker tricks a victim into performing an action on a web application without their knowledge or consent. For example, the attacker might send the victim a link that, when clicked, performs an action on the victim's behalf, such as transferring money or changing a password. To identify XSRF attacks, look for requests that are not initiated by the user, or that do not include the expected anti-CSRF token.

- Example 1: POST /transfer_money HTTP/1.1 Host: example.com Content-Type: application/x-www-form-urlencoded Transfer-Amount: $100 To-Account: 1234567890
- Example 2: GET /change_password?password=new_password HTTP/1.1 Host: example.com
- Example 3: POST /delete_account HTTP/1.1 Host: example.com Content-Type: application/x-www-form-urlencoded

CSRF (Cross-Site Request Forgery): CSRF attacks are similar to XSRF attacks, but they specifically target POST requests. An attacker tricks a victim into submitting a form on a web application without their knowledge or consent. To identify CSRF attacks, look for POST requests that are not initiated by the user, or that do not include the expected anti-CSRF token.

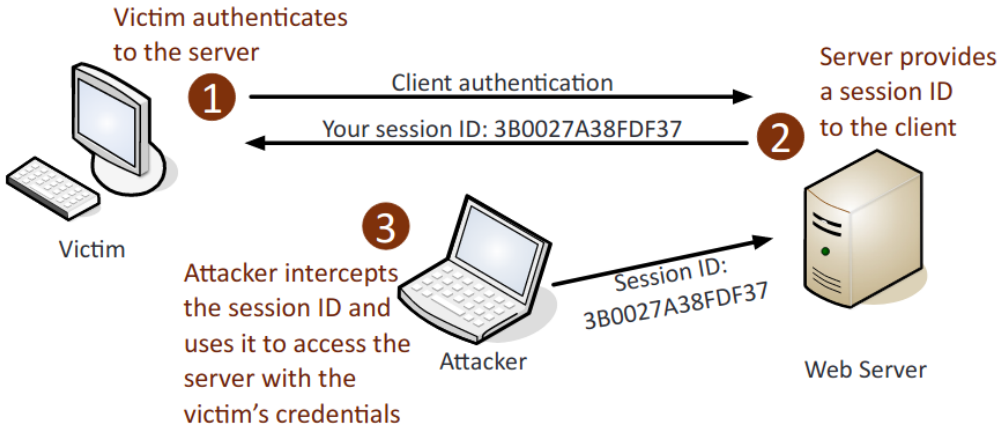
- Example 1: POST /submit_form HTTP/1.1 Host: example.com Content-Type: application/x-www-form-urlencoded Form-Field1: Value1 Form-Field2: Value2
- Example 2: POST /update_profile HTTP/1.1 Host: example.com Content-Type: application/x-www-form-urlencoded Profile-Field1: Value1 Profile-Field2: Value

Hijacking attacks

Clickjacking: Deceives the user into clicking on a malicious link by adding the link to a transparent layer over what appears to be a legitimate web page.

Domain hijacking: The act of changing the registration of a domain name without the permission of the victim.

Session hijacking: An attack in which an attacker attempts to impersonate the user by using their legitimate session token.



Typosquatting - have a URL that is named very similarly to a real site so that when users mistype the real site's URL they will go to the fake site. The other options are all methods of attacking a website, but in this case, the actual website was not attacked. Instead, some users are visiting a fake site.

Session Theft - Attacker guesses the session ID for a web session, enabling them to take over the already authorized session of the client

TCP/IP Hijacking - Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access

Blind Hijacking - Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not

Man-in-the-Browser (MITB) - Occurs when a Trojan infects a vulnerable web browser and modifies the web pages or transactions being done within the browser

Man-in-the-middle (MITM): The attacker alters the communication between two parties who believe they are directly communicating.

Password attacks

Brute Force Attack: This is a type of attack that tries every possible combination of characters to guess the correct password.

Password spraying - is a specific type of brute force attack which uses a smaller list of common passwords for many accounts to attempt to log in.

Dictionary Attack: This is a type of attack that uses a list of words, phrases or commonly used passwords to guess the correct password.

Hybrid Attack: This is a combination of both Brute Force and Dictionary Attack, where the attacker tries a combination of commonly used passwords and other characters to guess the correct password.

Rainbow Table Attack: This is a type of attack that uses precomputed tables of hashes of common passwords to quickly find the correct password.

Key Logger Attack: This is a type of attack where a malicious software is used to capture keystrokes, including passwords, as the user types them.

DoS attacks

DoS (Denial of Service): Flooding a target machine or resource with many requests to overload the system and prevent use of its resources. Attempt to send more packets to a host than they can handle.

Amplification: A type of attack where a malicious actor exploits vulnerabilities in a system to amplify their attack traffic, effectively magnifying the impact of the attack.

Distributed Denial of Service (DDoS): A type of DoS attack that involves multiple compromised systems being used to flood a target system, making it unavailable to legitimate users.

- **Botnets:** A type of DDoS attack where a network of infected devices, or bots, is used to launch attacks against target systems.
- **DNS Amplification** - Attack which relies on the large amount of DNS information that is sent in response to a spoofed query on behalf of the victimized server

Application-layer DoS: A type of DoS attack that targets the application layer of a system, using techniques such as excessive requests or malformed data to overload the system and make it unavailable.

Ping Flood - An attacker attempts to flood the server by sending too many ICMP echo request packets (which are known as pings)

- **Ping of Death** - An attack that sends an oversized and malformed packet to another computer or server

Smurf Attack - Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (victim server), using up bandwidth and processing

Fraggle Attack - Attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets

SYN Flood - Variant on a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions but never completes the 3-way handshake

XMAS Attack - A specialized network scan that sets the FIN, PSH, and URG flags set and can cause a device to crash or reboot

Teardrop Attack - Attack that breaks apart packets into IP fragments, modifies them with overlapping and oversized payloads, and sends them to a victim machine

Permanent Denial of Service - Attack which exploits a security flaw to permanently break a networking device by reflashing its firmware

Fork Bomb - Attack that creates a large number of processes to use up the available processing power of a computer

To stop DoS: blackholing, sinkholing, IPS, DDoS mitigator

DNS attacks

DNS poisoning: Is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.

Unauthorized Zone Transfer - Occurs when an attacker requests replication of the DNS information to their systems for use in planning future attacks

Altered Hosts File - Occurs when an attacker modifies the host file to have the client bypass the DNS server and redirects them to an incorrect or malicious website. Windows stores the hosts file in the following directory: \%systemroot%\system 32\drivers\etc

Pharming - Occurs when an attacker redirects one website's traffic to another website that is bogus or malicious

Domain Name Kiting - Attack that exploits a process in the registration process for a domain name that keeps the domain name in limbo and cannot be registered by an authenticated buyer

Wireless attacks

WPS (WiFi Protected Setup): Allows users to easily configure a wireless network, sometimes by using only a PIN. The PIN can be found through a brute force attack.

RFID (Radio Frequency Identifier): Communicates with a tag placed in or attached to an object using radio signals. Can be jammed with noise interference, the blocking of radio signals, or removing/disabling the tags themselves.

NFC (Near Field Communication): A wireless technology that allows for smartphones and other devices to establish communication over a short distance.

"War driving/war chalking" refers to the act of driving or walking around in a vehicle or on foot while using a wireless device to search for wireless access points (APs). The objective is to identify APs that have poor security configurations or those that are left unsecured, making them vulnerable to attacks.

"Jamming attack" is a wireless network attack in which the attacker deliberately interferes with the normal operation of wireless networks by disrupting the transmission of signals between the wireless devices and the APs.

Replay: This is a passive attack where the attacker captures wireless data, records it, and then sends it on to the original recipient without them being aware of the attacker's presence.

IV (Initialization Vector): A random number used to increase security by reducing predictability and repeatability.

Rogue AP (Access Point): An unauthorized WAP (Wireless Access Point) or Wireless Router that allows for attackers to bypass many of the network security configurations and opens the network and its users to attacks.

- **"Evil twin attack"** is a type of rogue AP attack in which the attacker creates a fake wireless access point with a similar name to a legitimate one to trick users into connecting to it. Once connected, the attacker can steal sensitive information or launch further attacks.

Bluejacking (sending attack): Sending unauthorized messages to a Bluetooth device.

Bluesnarfing (downloading attack): Gaining unauthorized access to, or stealing information from a Bluetooth device

Disassociation: Removes clients from a wireless network.

Cryptographic attacks

Birthday: Used to find collisions in hashes and allows the attacker to be able to create the same hash as the user. Exploits that if the same mathematical function is performed on two values and the result is the same, then the original values are the same.

Rainbow tables: Large pregenerated data sets of encrypted passwords used in password attacks.

Dictionary: A password attack that creates encrypted versions of common dictionary words and then compares them against those in a stolen password file. Guessing using a list of possible passwords.

Collision: When two different inputs produce the same hash value.

Downgrade: Forces a system to lessen its security, this allows for the attacker to exploit the lesser security control. It is most often associated with cryptographic attacks due to weak implementations of cipher suites. Example is TLS > SSL, a man-in-the-middle POODLE attack exploiting TLS v1.0 - CBC mode.

Replay: The attacker captures network packets and then retransmits them back onto the network to gain unauthorized access.

Brute force: A password-cracking program that tries every possible combination of characters:

- Online: Is against a live logon prompt.
- Offline: The attack is working on their own independent computers to compromise a password hash.

Threat Actor Types And Attributes.

Types of actors:

Script kiddies: A person who uses pre-existing code and scripts to hack into machines, because they lack the expertise to write their own.

Hacktivist: An individual who is someone who misuses computer systems for a socially or politically motivated agenda. They have roots in the hacker culture and ethics. Hacker on a mission.

Organized crime: These are professionals motivated ultimately by profit. They have enough money to buy the best gear and tech. Multiple people perform specific roles: gathering data, managing exploits, and one who actually writes the code.

Nation states/APT: An APT is an advanced persistent threat, these are massive security risks that can cost companies and countries millions of dollars. Nation states have very sophisticated hacking teams that target the security of other nations. They often attack military organizations or large security sites, they also frequently attack power plants.

Insiders: Someone who is inside the company who has intricate knowledge of the company and how its network works. They can pinpoint a specific vulnerability and may even have access to multiple parts of the network.

Competitors: Rival companies, can bring down your network or steal information through espionage.

Attributes of actors:

Internal/external: Internal is inside the company, can be intentional, unintentional. External is someone outside the company trying to get in.

Level of sophistication: Is the skill of the hacker and the complexity of the attack.

Resources/funding: The amount of money and the value of the tech and gear being used.

Intent/motivation: The reason for the attack, can be for political, monetary, or social reasons.

Use of Open-source intelligence (OSINT): Data that is collected through publicly available information. This can be used to help make decisions. Can be used by threat actors to help find their next target or how to best attack their target. OSINT is also incredibly helpful for mitigating risks and for identifying new threat actors.

The impact associated with types of vulnerabilities

Race conditions: The behavior of a software, electronic, or another system's output is dependent on the timing, sequence of events, or a factor out of the user's control. **A race condition** - can occur when multiple threads in an application are using the same variable and the situation is not properly handled.

Vulnerabilities due to:

- **End-of-life systems**: No longer receives updates, and at a high risk to compromise.
- **Embedded systems**: Programs added for automation and/or monitoring. Can allow for malicious programs to gain access through the added programs.
- **Lack of vendor support**: Vendor does not support the product: does not update, improve, or protect the product.

Improper input handling: The system does not properly validate data, allows for an attacker to create an input that is not expected. Allows for parts of the system vulnerable to unintended data.

Improper error handling: The error messages display sensitive or private information that give the user too much data.

Default/weak configuration/Misconfiguration – vulnerable to attacks.

Resource exhaustion: A denial of service occurs, the amount of resources to execute an action are expended, making it unable for the action to be performed.

Untrained users: Users are not properly informed on how to use the systems. This means that mistakes will more likely occur and that the system's resources may be abused.

Improperly configured accounts: Users should only be allowed to access the parts that they need to complete their work.

Vulnerable business processes: All tasks, procedures, and functions should be properly assessed and the most valuable and vulnerable should be heavily protected.

Weak cipher suites and implementations: Use of older and less robust cryptographic algorithms.

Memory/buffer vulnerability:

- **Memory leak**: is a programming error that occurs when a program does not properly manage memory allocation and does not release unused memory, leading to a gradual loss of available

memory over time. Memory leaks can cause performance issues and system crashes if not addressed.

- **Integer/buffer overflow**: Too much data for the computer's storage/memory capacity/buffer
- **NULL Pointer dereference**: Failed deference can cause memory corruption and the application to crash.

System sprawl/undocumented assets: Lack of internal inventory and allowing unsecure devices and systems to connect to the network.

Architecture/design weaknesses: An insecure and poorly designed network. Ex. Not segmenting the systems or internal network.

New threats/zero day: A zero-day threat, is a flaw that is unknown to the teams patching and fixing flaws.

Improper certificate and key management: Allowing for unauthorized access to certificates and keys, which allows for sensitive data to be decrypted. And allowing for certificates to expire.

2.0 TECHNOLOGIES AND TOOLS

Common protocols

21 TCP	**FTP (File Transfer Protocol)**	used to transfer files from host to host
22 TCP/UDP	**SSH, SCP, SFTP (Secure Shell)**	Secure Shell is used to remotely administer network devices and systems. SCP is used for secure copy and SFTP for secure FTP.
23 TCP/UDP	**Telnet**	Unencrypted method to remotely administer network devices.
25 TCP	**SMTP (Simple Mail Transfer Protocol)**	used to send email over the Internet
53 TCP/UDP	**DNS (Domain Name Service)**	used to resolve hostnames to IPs and IPs to hostnames
69 UDP	**TFTP (Trivial FTP)**	used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host
80 TCP	**HTTP (Hyper Text Transfer Protocol)**	used to transmit web page data to a client for unsecured web browsing
88 TCP/UDP	**Kerberos**	Used for network authentication using a system of tickets within a Windows domain
110 TCP	**POP3 (Post Office Protocol v3)**	used to receive email from a mail server
119 TCP	**NNTP (Network News Transfer Protocol)**	used to transport Usenet articles
135 TCP/UDP	**RPC/DCOM-scm**	Remote Procedure Call is used to located DCOM ports request a service from a program on another computer on the network
137-139 TCP/UDP	**NetBIOS**	used to conduct name querying, sending of data, and other functions over a NetBIOS connection
143 TCP	**IMAP (Internet Message Access Protocol)**	used to receive email from a mail server with more features than POP3
161 UDP	**SNMP (Simple Network Management Protocol)**	used to remotely monitor network devices

162 TCP/UDP	**SNMPTRAP**	Used to send Trap and InformRequests to the SNMP Manager on a network
389 TCP/UDP	**LDAP (Lightweight Directory Access Protocol)**	used to maintain directories of users and other objects
443 TCP	**HTTPS (Hyper Text Transfer Protocol Secure)**	used to transmit web page data to a client over an SSL/TLS-encrypted connection
445 TCP	**SMB (Server Message Block)**	used to provide shared access to files and other resources on a network
465/587 TCP	**SMTP with SSL/TLS (Simple Mail Transfer Protocol)**	used to send email over the Internet with an SSL and TLS secured connection
514 UDP	**Syslog**	used to conduct computer message logging, especially for routers and firewall logs
636 TCP/UDP	**LDAP SSL/TLS**	used to maintain directories of users and other objects over an encrypted SSL/TLS connection
860 TCP	**iSCSI**	is used for linking data storage facilities over IP
989/990 TCP	**FTPS (File Transfer Protocol Secure)**	used to transfer files from host to host over an encrypted connection
993 TCP	**IMAP4 with SSL/TLS (Internet Message Access Protocol)**	used to receive email from a mail server over an SSL/TLS- encrypted connection
995 TCP	**POP3 (SSL/TLS) (Post Office Protocol v3)**	used to receive email from a mail server using an SSL/TLS-encrypted connection
1433 TCP	**Ms-sql-s (Microsoft SQL server)**	used to receive SQL database queries from clients
1645/1646 UDP 1812/1813 UDP	**RADIUS (Remote Authentication Dial-In User Service)**	used for authentication and authorization (1645),(1812) and accounting (1646),(1813)
1701 UDP	**L2TP (Layer 2 Tunnel Protocol)**	used as an underlying VPN protocol but has no inherent security
1723 TCP/UDP	**PPTP (Point-to-Point Tunneling Protocol)**	is an underlying VPN protocol with built-in security
3225 TCP/UDP	**FCIP (Fibre Channel IP)**	used to encapsulate Fibre Channel frames within TCP/IP packets
3260 TCP	**iSCSI Target**	iSCSI Target is as the listening port for iSCSI-targeted devices when linking data storage facilities over IP
3389 TCP/UDP	**RDP (Remote Desktop Protocol)**	used to remotely view and control other Windows systems via a Graphical User Interface
3868 TCP	**Diameter**	A more advanced AAA protocol that is a replacement for RADIUS
6514 TCP	**Syslog over TLS**	used to conduct computer message logging, especially for routers and firewall logs, over a TLS-encrypted connection

VoIP (Voice over Internet Protocol): A technology that allows voice communication over the internet or other IP-based networks. Associated vulnerabilities include eavesdropping, unauthorized access, and denial of service attacks.

Ports vs Protocols

Ports: In the context of networking, a port is a numerical identifier assigned to a specific service or application. A port number is used to route incoming data to the correct application or service on a device. There are 65535 ports available for use, ranging from 0 to 65535. Each port is associated with a specific service or application.

Protocols: A protocol is a set of rules and standards that govern how data is transmitted over a network. A protocol defines the format of the data being transmitted, the methods used to transmit the data, and the rules for error detection and correction.

In summary, ports identify specific applications or services on a device, while protocols define the rules and standards for transmitting data over a network.

Network storage protocols

SAN (Storage Area Network): is a high-speed, dedicated network that provides block-level access to data storage. A SAN is typically comprised of a network of storage devices, such as disk arrays, and a network of servers, connected by a high-speed network. The main purpose of a SAN is to provide centralized storage for an organization, allowing multiple servers to access the same data without having to store it locally. SANs are designed for high-speed data transfer and are used for applications that require high-performance data access, such as database and file servers.

- It requires proper zoning, masking, and encryption techniques to prevent unauthorized access and data breaches
- Access controls and monitoring mechanisms should be implemented to ensure the integrity and confidentiality of data

NAS (Network Attached Storage): is a dedicated file-level data storage server connected to a network, allowing multiple users to access its shared storage. Unlike a SAN, which provides block-level access to data, a NAS provides file-level access to data. A NAS device typically includes a processor, memory, and one or more storage drives, and can be used to store, share, and manage files, such as documents, photos, and videos.

SAN	VS	NAS
Fibre Channel		Ethernet (RJ45)
Expensive		Not expensive
For big companies		For home and small business
Requires more administration		Easier to manage
Servers access data as if it were a local hard drive (blocks)		Data accessed as if it were a network-attached drive (files)
SCSI, iSCSI, FCoE		I/O protocols: NFS, SMB/CIFS, HTTP
Works with virtualization		Does not work with virtualization
Fault tolerant network with redundant functionality		Entry level systems often have a single point of failure, e.g. power supply
High speed using Fibre Channel, 2 gigabits to 128 gigabits per second.		Speed dependent on local TCP/IP usually Ethernet network

NAS devices are typically more cost-effective than SANs and are designed for environments that require low-cost, simple, file-level storage.

SAN > NAS

Network storage protocols (hardware and software)

Fibre Channel (FC/światłowód): A high-speed data transfer protocol for storage area networks.

FC over Ethernet (FcoE/rj45): A converged network technology that allows Fibre Channel traffic over Ethernet networks.

Internet SCSI (iSCSI): A protocol for transmitting SCSI commands over TCP/IP network for accessing storage devices.

Cases – secure solutions

Voice and video	SRTP
Time synchronization	NTPsec (Secure network time protocol): Used to securely sync all the devices' clocks on the network.
Email and web	S/MIME and HTTPS
File transfer	FTPS or SFTP
Directory services	LDAPS or SASL - SASL (Simple Authentication and Security Layer): Provides a source of additional authentication using many different methods, such as Kerberos or client certificates.
Remote access	SSH
Domain name resolution	DNSSec
Routing and switching	SNMPv3, SSH, or HTTPS. - SNMPv3: Provides continentality, integrity, and authentication. HTTPS: Allows for browser-based management.
Network address allocation	DHCP, there is no secure version it. DHCP starvation attack: Using spoofed MAC addresses to exhaust the amount of DHCP's pool. Can configure a switch to limit the number of MAC addresses on an interface.

Secure network components – Hardware/Software

Firewall

Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

1. **ACL (Access control lists):** A list of rules that can be used to control traffic based on networks, subnets, IP addresses, ports, and some protocols.
2. **Application-based vs. network-based:**
    - **Application-based**: It is typically software running on a system. Protects the user from applications and services by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall.
    - **Network-based**: Filters traffic by port number based on rules and allows only authorized traffic to pass in and out of the network
3. **Stateful vs. stateless:**

- **Stateful**: Stateful firewalls block traffic based on the state of the packet within a session. It adds and maintains information about a user's connections in a state table, referred to as a connection table.
- **Stateless**: Stateless firewalls uses rules within an ACL to identify allowed and/or block traffic through packet filtering. Does not keep track of flows.

4. **Implicit Deny** - Traffic is denied the ability to enter or leave the network because there is no specific rule that allows it
5. **Web Application Firewall -** Firewall installed to protect your server by inspecting traffic being sent to a web application. A WAF can prevent a XSS or SQL injection.
6. **MAC Filtering**
7. **Explicit Allow** - Traffic is allowed to enter or leave the network because there is an ACL rule that specifically allows it
8. **Explicit Deny** - Traffic is denied the ability to enter or leave the network because there is an ACL rule that specifically denies it
9. **Most operate at Layer 3 (blocking IP addresses) and Layer 4 (blocking ports)**

Basic commands:

Deny: This command blocks traffic and prevents it from passing through the firewall. The traffic is dropped without any notification to the source or destination.

Example command: deny ip any any

Drop: This command is similar to deny, but it silently drops traffic without generating any log messages or notifications.

Example command: drop tcp any any

Reject: This command blocks traffic and sends a message to the source informing it that the traffic has been rejected. The destination does not receive the traffic.

Example command: reject icmp any any

Permit: This command allows traffic to pass through the firewall based on the defined rules. Traffic that does not match the rules is blocked.

Example command: permit tcp any any eq 80

Monitor: This command displays real-time information about network traffic passing through the firewall.

Example command: monitor interface ethernet1/1

iptables is a Linux-based firewall program that allows system administrators to control incoming and outgoing network traffic. It uses a set of rules to determine how network packets are handled, allowing administrators to specify which packets should be allowed or denied based on various criteria such as source and destination IP address, protocol type, and port number. iptables is a powerful tool that can be used to secure networked systems against unauthorized access and other security threats.

Host-based firewall: A firewall that is on a single host that only restricts incoming and outgoing network activity for that host.

Next-Generation Firewall (NGFW) is a type of firewall that includes advanced security features such as deep packet inspection, intrusion prevention, and application awareness. NGFWs are designed to provide better protection against modern network threats and can also be used to enforce policies for network access and usage.

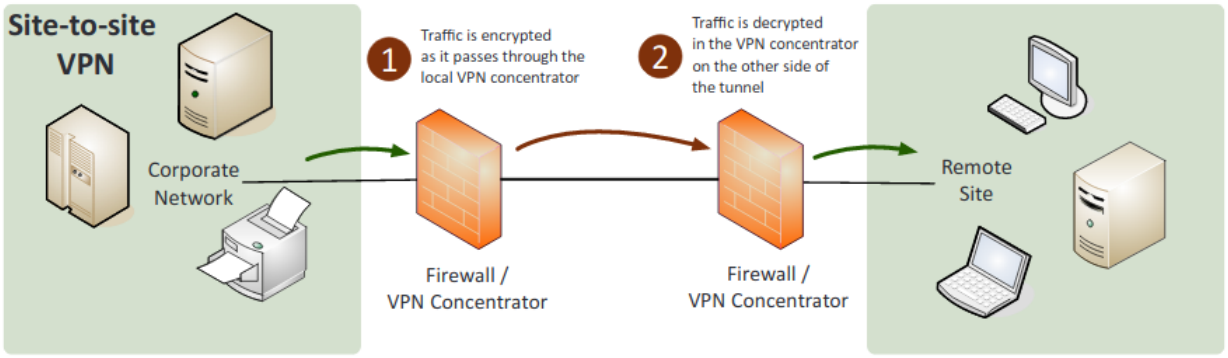
Web Application Firewall (WAF) is a type of security device that protects web applications from attacks such as SQL injection, cross-site scripting (XSS), and other application-layer threats. It operates at the application layer (layer 7) of the OSI model and can be deployed either in front of the web application, or integrated into the web application itself.

VPN concentrator

VPN concentrator: A type of router device that allows for the secure creation of VPN connections and for the safe delivery of messages between VPN nodes. Allows for the handling of a large quantity of VPN tunnels.

Remote access vs. site-to-site:

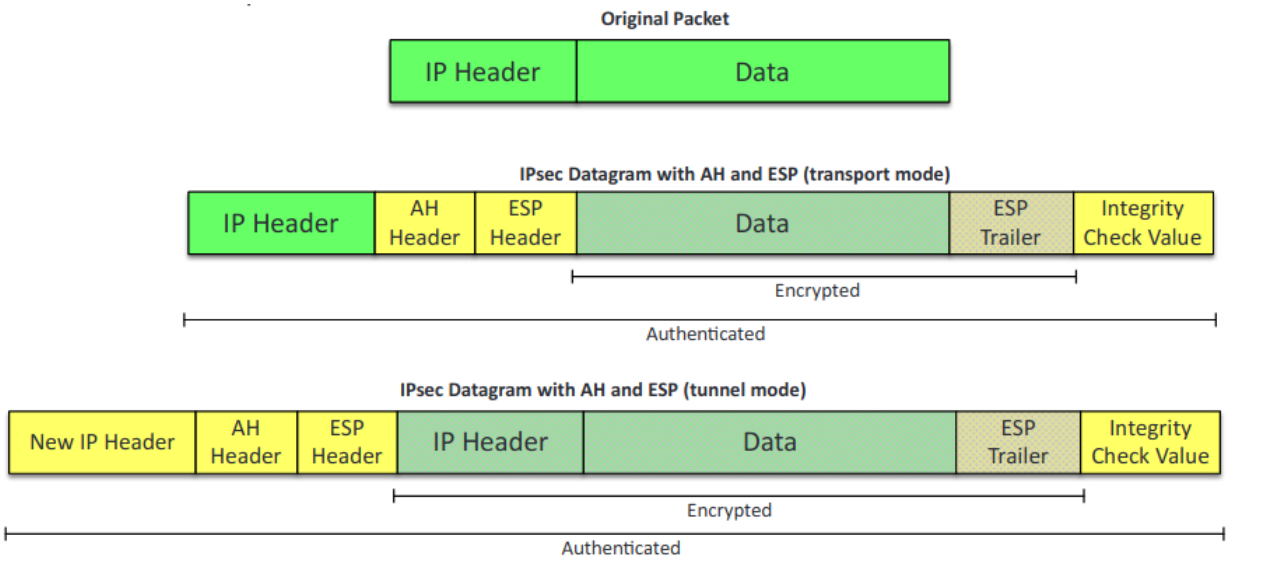
- **Remote access**: Allows users to connect to a private network from a remote location, typically through a client application installed on their device.
- **Site-to-site**: Connects two or more networks together, allowing devices on each network to communicate securely with devices on the other network.



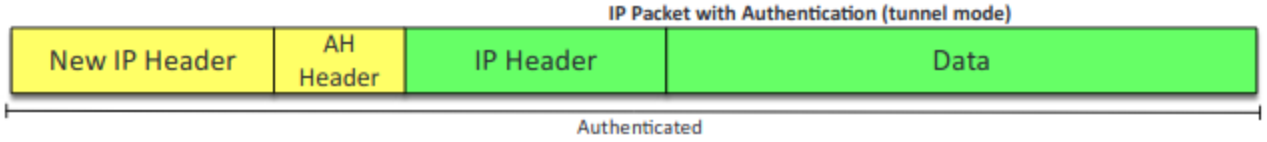
IPsec (Internet Protocol Security) is a set of protocols for secure communication over IP networks. It provides security for data transmission by using encryption, authentication, and integrity protection. IPsec can be used to secure communication between hosts, between routers, and between security gateways and endpoints. It can be used with either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (Ipv6). IPsec is widely used to provide secure virtual private networks (VPNs) and secure communications over the internet. It is considered secure and is a commonly used standard for secure communication over IP networks.

- **Tunnel** mode: The default mode for IPSec, the entire pack is protected.

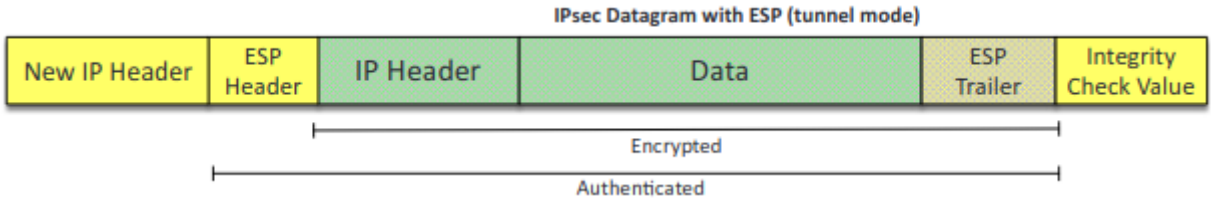
- **Transport** mode: Used for end-to-end communications in IPSec. Ex. encrypted Telnet or Remote Desktop session from a workstation to a server.



- **Authentication Header** (AH): IPsec protocol that authenticates that the packets received were sent from the source identified in the header. MD5, SHA-1 or SHA-2.

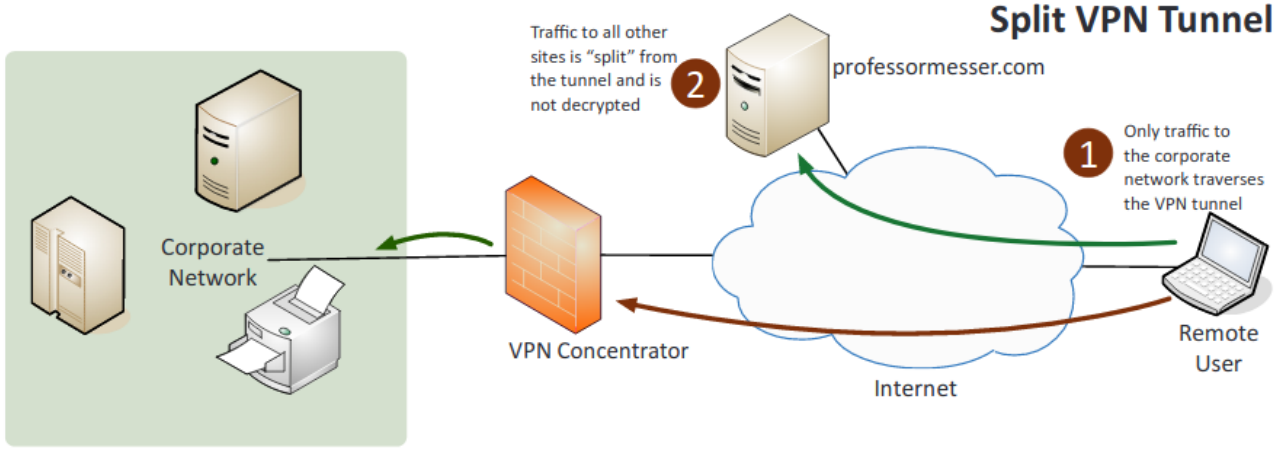


- **ESP** (Encapsulating Security Payload): IPSec component that provides the same services as AH and also ensures confidentiality when sending data. MD5, SHA-1 or SHA-2 for hash, 3DES or AES for encryption.

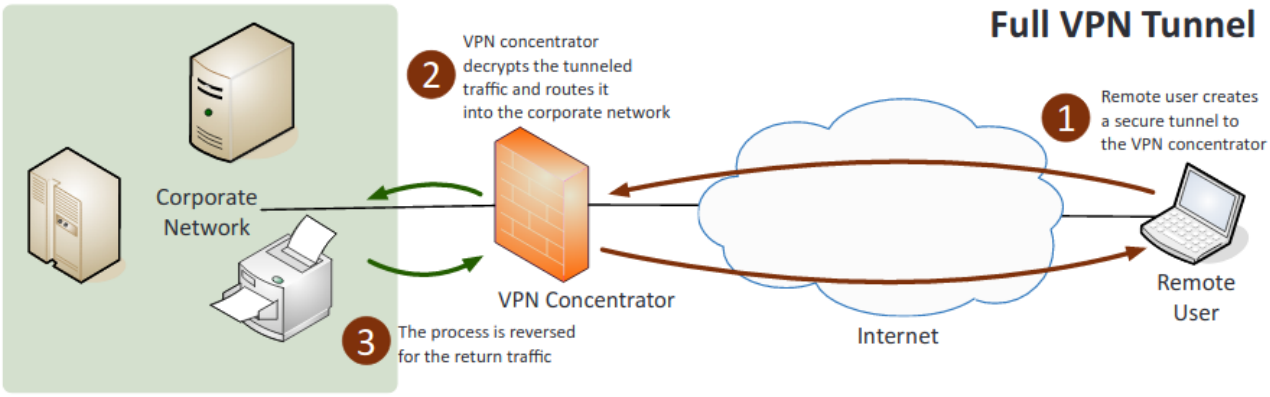


Split tunnel vs. full tunnel:

- **Split tunnel**: Only some traffic over the secure VPN while the rest of the traffic directly accesses the internet **(only corporate resources are encrypted)**



- **Full tunnel**: All of the traffic is sent over the secure VPN.



TLS: The replacement of SSL to encrypt data-in-transit. Uses certificates issued by CAs.

SSL/TLS VPN: Uses the SSL/TLS protocol to create a secure, encrypted connection between a client and a server.

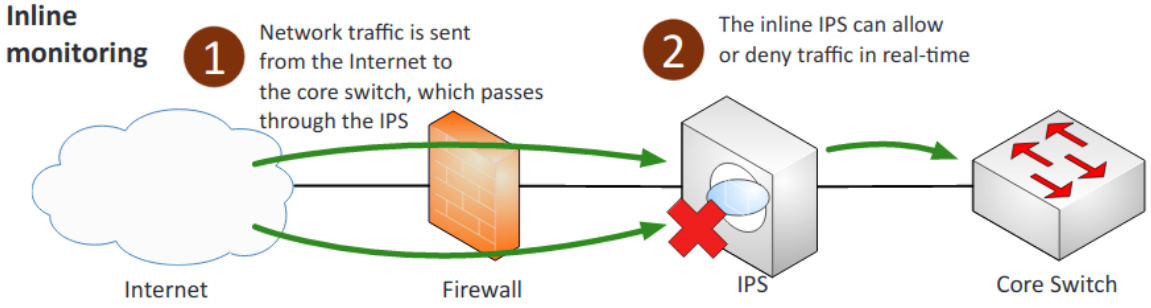
Always-on VPN: The user does not connect and disconnect and instead is always connected.

Client-to-Site VPN: Similar to a remote access VPN, but instead of connecting to a single device, users connect to a network as a whole.

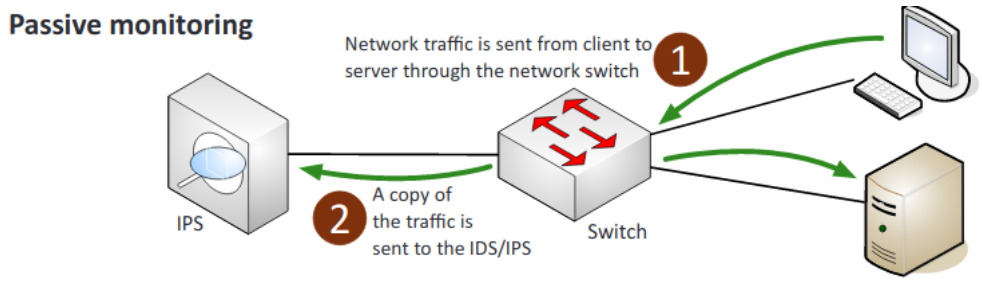
NIPS/NIDS

Network Based Intrusion Prevention System (NIPS) is a type of security device that analyzes network traffic in real-time to identify and prevent security threats. It operates at the network layer (layer 3) of the OSI model and can be deployed inline, meaning it sits in the network path between the source and destination, allowing it to inspect all network traffic.

1. **Signature-based**: Detects attacks based on known attack patterns documented as attack signatures.
2. **Heuristic/behavioral**: It detects attacks by comparing traffic against a baseline to find any anomalies.
3. **Anomaly**: Abnormal packets or traffic.
4. **Inline vs. passive:**
   - **Inline**: Connected directly to the network and monitors the flow of data as it occurs.



- **Passive**: Connected through a switch or port on the network and receives a copy of the flow of data as it occurs.



5. **In-band vs. out-of-band:**
    - **In-band**: Sits in the network, can quickly warn of or prevent malicious traffic.
    - **Out-of-band**: Can only warn of malicious traffic. When identifies it, sends reset frames.
6. **Rules**: Standards set to differentiate good traffic from suspicious traffic.
7. **Analytics**: Shows the amount, type and history of traffic coming through.
    - **False positive**: NIPS blocks legitimate incoming traffic.
    - **False negative**: NIPS allows harmful incoming traffic.

Router

Router is a networking device that forwards data packets between computer networks. Routers use routing tables to determine the best path for forwarding data. They also have the ability to provide network layer (layer 3) address translation (NAT) and can be used to provide a demilitarized zone (DMZ) between a public and private network.

1. **ACLs** (Access Control List): A list of permit or deny rules detailing what can or can't enter or leave the interface.
2. **Anti-Spoofing**: Prevent a bad guy from using someone else's address. Filter reserved IP addresses.
3. **NAT (Network Address Translation)** is a technique used to allow a single device, such as a router, to be used as an intermediary between an organization's internal network and the public internet. NAT allows multiple internal devices to share a single public IP address while still allowing those devices to communicate with the public internet. NAT helps to conserve global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

The difference in operation between an RJ45 switch and a router mainly concerns the scale. Switches are used to connect multiple devices to one network, such as computers, printers, phones, etc. Meanwhile, a router is used to connect such networks together.

Switch > Router

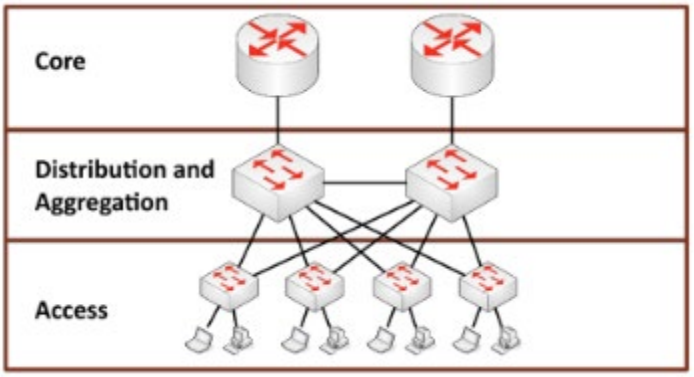
Switch

Switch is a networking device that connects devices together on a computer network and uses packet switching to forward data to its destination. Switches operate at the data link layer (layer 2) of the OSI model and provide a higher level of performance compared to a router by reducing the need for network layer routing.

1. **Port security** is a feature that allows administrators to specify which devices are allowed to connect to a specific port. This helps to prevent unauthorized devices from accessing the network and provides a means of controlling access to the network. Port security can be implemented using methods such as MAC address filtering or 802.1X authentication.
2. **Layer 2 vs. Layer 3:**
    - **Layer 2**: Packets are sent to a specific switch port based on destination MAC addresses.
    - **Layer 3**: Packets are sent to a specific next-hop IP address, based on destination IP address.
3. **Loop prevention/protection**: is a feature that helps to prevent network loops, which can occur when a device receives a packet that it has already processed. Loops can cause network congestion and slow down network performance, so loop protection helps to prevent this by detecting and breaking the loop.
4. **Flood guards** are security features that prevent malicious traffic from overwhelming the device and causing a denial-of-service attack. Flood guards are typically implemented in switches and routers and help to prevent network congestion and protect the network from security threats.

Multilayer switch is a device that can perform functions at multiple layers of the OSI model, including the network layer (layer 3) and the data link layer (layer 2). This allows for the combination of switching and routing functions in a single device, providing greater flexibility and efficiency for network traffic management.

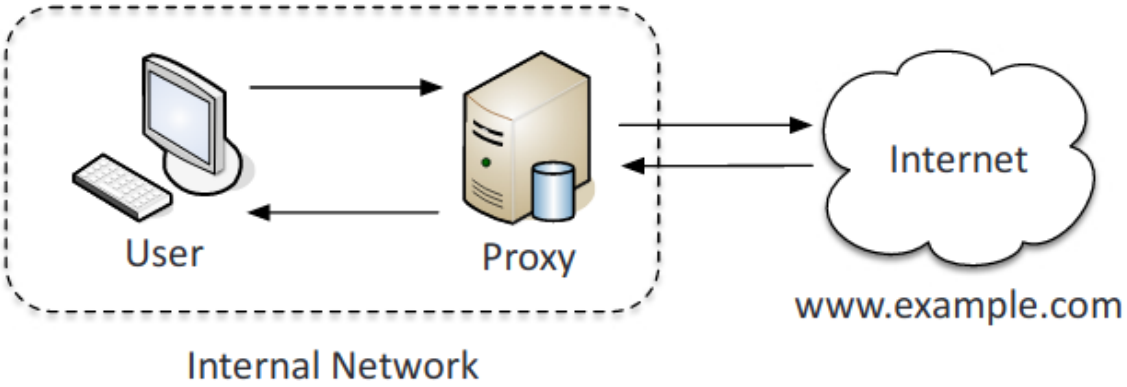
Aggregation switch: Uplinks to upper layer core switch and links down to the access switch.



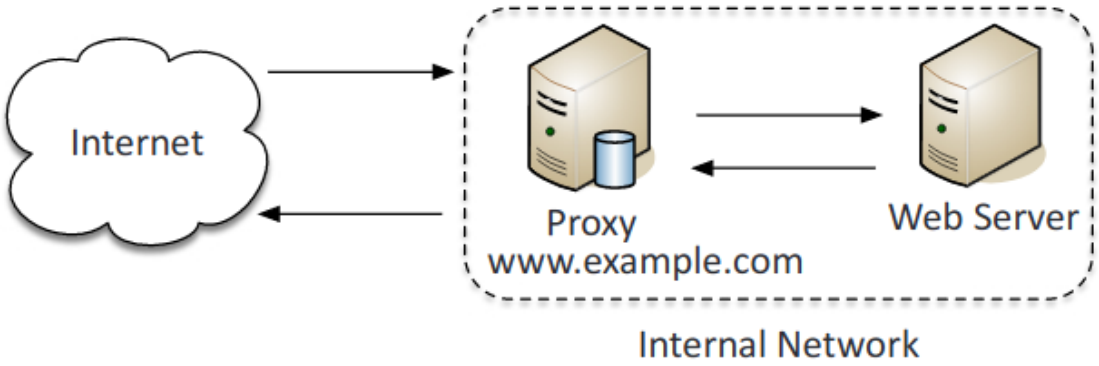
Proxy (worse VPN)

Proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. It can be used to enhance security by hiding the identity of client machines, as well as for bypassing content filters.

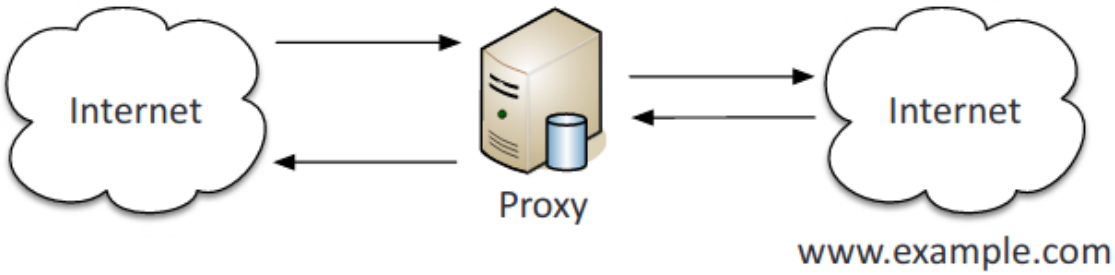
1. **Forward proxy**: Forwards requests from internal clients to external servers.



2. **Reverse proxy**: Takes in requests from the Internet and forwards them to an internal web server.



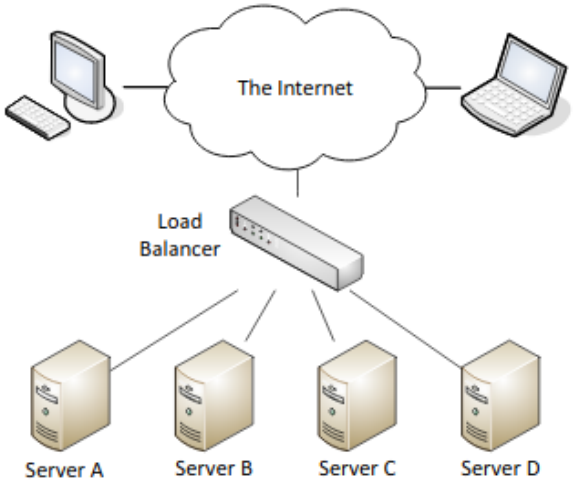
3. **Transparent**: Accepts and forwards requests without performing any modifications on them.



4. **Application/multipurpose**: A type of proxy server that knows the application protocols that it supports.

Load balancer

Load balancer (reverse proxy) is a device that distributes network or application traffic across multiple servers to ensure efficient use of resources and prevent overload. Load balancers help ensure high availability and scalability by distributing incoming requests to multiple servers.



1. **Scheduling**: Sends requests to servers using set rules.
    - **Affinity**: Sends client requests to the same server based on the client's IP address.
    - **Round-robin**: Sends requests in a predefined order.
2. **Active-passive**: Some servers are not active and only go active to take excess traffic or if an active server fails.
3. **Active-active**: All servers are actively processing requests
4. **Virtual IPs**: An IP address and a specific port number that can be used to reference different physical servers. Provides IP addresses that can float between two or more physical network nodes and provide redundancy.

Access point

SSID (Service Set Identifier) is a unique identifier used to name a wireless local area network (WLAN). It allows stations to connect to a specific wireless network and helps distinguish it from other wireless networks that may be in the same area.

MAC filtering: A method of controlling access on a wired or wireless network by denying unapproved MAC address access to a device.

Signal strength: The quality and distance of a signal.

Band selection/width: Can be set between 2.4 GHz and 5 GHz depending on which 802.11 protocol is being used.

Antenna types:

- **Omnidirectional**: Signal is evenly distributed on all sides but has no ability to focus the signal.
- **Directional**: Focus the signal increasing distance. (Yagi and parabolic)
- **Fat**: Has everything necessary to handle wireless clients. If end-user deploys several Fat Wireless Access Points, each one needs to be configured individually.
- **Thin**: Acts as a radio and antenna that is controlled by a wireless switch. If multiple thin wireless access points are deployed, the entire configuration takes place at the switch.

Antenna placement:

- Controller-based: Require a controller for centralized management and are not manually configured.
- Standalone: Do not require a controller and are generally used in smaller environments.

LWAPP (Lightweight Access Point Protocol): Manages multiple access points simultaneously.

Power level controls refer to the setting of the transmission power of wireless devices, such as access points or routers, in order to control the coverage area of the network.

Secure access point solutions:

- **WPA-Enterprise (Wi-Fi Protected Access Enterprise)** is a security protocol for wireless networks that provides enhanced security compared to WPA-Personal. It uses a centralized authentication server and requires user authentication through Extensible Authentication Protocol (EAP).
- **EAP (Extensible Authentication Protocol)** is a framework for authentication that is used in Wi-Fi networks to provide secure authentication for wireless clients. It supports multiple authentication methods, including username and password, digital certificates, and smart cards. EAP is used in WPA-Enterprise to provide user authentication for wireless clients.

SIEM (Security Information and Event Management)

Systemy SIEM zapewniają całościowy wgląd w to, co dzieje się w sieci w czasie rzeczywistym i pomagają zespołom IT w aktywny sposób w walce z zagrożeniami. Wyjątkowość rozwiązań SIEM polega na połączeniu zarządzania incydentami bezpieczeństwa z zarządzaniem informacjami o monitorowanym środowisku. Dla organizacji, która chce pełnej widoczności i kontroli nad tym, co dzieje się w ich sieci w czasie rzeczywistym, rozwiązania SIEM mają kluczowe znaczenie.

1. **Aggregation**: The gathering of log and event data from the different network security devices used on the network.

2. **Correlation**: Relating various events to identifiable patterns. If those patterns threaten security, then action must be taken.
3. **Automated alerting and triggers**: Sends messages based on configured rules based on events that occur within the log files.
4. **Time synchronization**: Ensures that the time is the same across devices so that all security events are recorded at the same time using Network Time Protocol.
5. **Event de-duplication**: Trimming event logging so that the same event is not recorded over and over again, overflowing log space.
6. **Logs/WORM**: Prevents alteration of logs and archives the source logs with write protection.

DLP (Data Loss Prevention)

DLP is software used to secure sensitive data - it monitors data and advanced algorithms enable data protection in the event of a threat. In the event of an attempt to copy or send data, the software blocks the action and sends a warning to the administrator of the anomaly. DLP is also a tool that allows for verification of the effectiveness of the security policy implemented in the company, which in turn allows for the refinement of procedures.

1. **USB blocking**: Prevents the use of USBs
2. **Cloud-based**: Prevents sensitive data from being stored on the cloud without proper encryptions and authorization.
3. **Email**: Protects against email fraud and from valuable data from being sent through email.

NAC (Network Access Control)

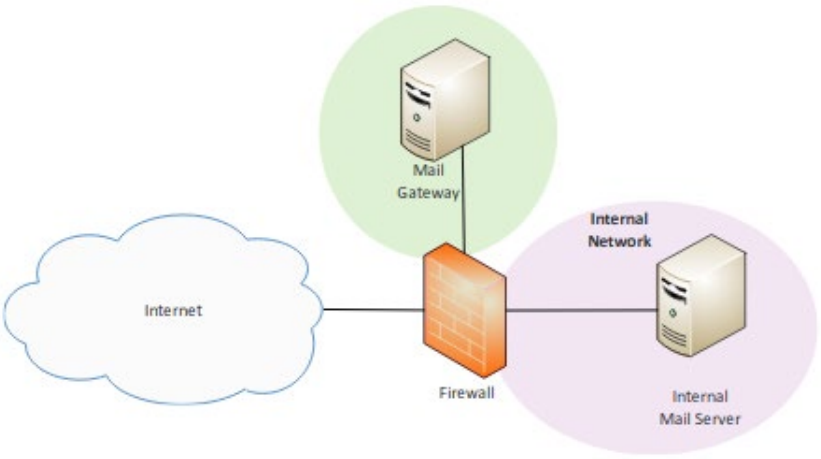
NAC enforces security policies on devices that access networks to increase network visibility and reduce risk. NAC is a security solution that helps organizations control and monitor access to their networks. NAC solutions typically use a combination of hardware, software, and policies to control and monitor network access, including the authentication and authorization of users and devices, the enforcement of security policies, and the quarantine of devices that do not meet security requirements.

1. **Dissolvable vs. permanent:**
    - **Dissolvable**: Disappears after reporting information to the NAC device.
    - **Permanent**: Resides on end devices until uninstalled.
2. **Host health checks**: Reports sent by network access control to gather information on installed devices.
3. **Agent vs. agentless:**
    - **Agent**: Is installed on the end device.
    - **Agentless**: Is not installed on the device itself but instead is embedded within a Microsoft Windows Active Directory domain controller.

Mail gateway

Mail gateway: Examines and processes all incoming and outgoing email.

1. **Spam filter**: An on-premises software solution for filtering, well spam emails.
2. **DLP** Prevents certain information leaving the organization via email.
3. **Encryption**: Encrypt and decrypts emails being sent and received across networks.



SOAR

SOAR (Security Orchestration, Automation, and Response) - is a technology solution used in cybersecurity that integrates and automates processes across different security systems, allowing organizations to respond more quickly and efficiently to security incidents. SOAR solutions typically include capabilities for threat intelligence management, incident response, and automated workflows. By automating repetitive tasks and integrating disparate security tools, SOAR platforms can help security teams increase their efficiency and effectiveness in detecting, investigating, and responding to security incidents.

The rest of solutions

Bridge: Provides interconnection with other bridge networks using the same protocol.

SSL/TLS accelerators: The process of offloading processor-intensive public-key encryption for TLS or its SSL to a hardware accelerator.

SSL decryptors: Allows for the user to view inside of passing Secure HTTP traffic.

DNS sinkhole is a technique used to redirect malicious domain name system (DNS) queries to a non-existent or invalid IP address. This is done to prevent access to malicious websites or to block malware from communicating with its command-and-control server.

Media gateway: Converts media streams between disparate telecommunications technologies.

SWG (Secure Web Gateway/Web Security Gateway): is a type of security device that is designed to protect an organization's network from web-based threats. It operates at the application layer (layer 7) of the OSI model and can perform functions such as URL filtering, web content filtering, and application control.

- **NG-SWG (Next-Generation Secure Web Gateway)** is a type of security solution that provides web filtering and protection against web-based threats. NG-SWGs typically include features such as URL filtering, malware detection, and content inspection to help prevent attacks like phishing, malware downloads, and data exfiltration.

HTTP security header refers to a set of response headers that can be used to enhance the security of web applications. These headers can help to prevent attacks such as cross-site scripting (XSS) and clickjacking.

Securing the BIOS

BIOS (Basic Input Output System) - Firmware that provides the computer instructions for how to accept input and send output. Most basic system in machine.

UEFI (Unified Extensible Firmware Interface) – more sophisticated version of BIOS, with visible mouse and GUI.

Hardening of BIOS:

- Flash the BIOS
- Use a BIOS password
- Configure the BIOS boot order
- Disable the external ports and devices
- **Secure boot**
    - **Measured boot** is a security feature that ensures that a system boots up in a trusted state by measuring the integrity of the boot process. When a system is started, a secure boot chain is initiated that verifies the integrity of each component in the boot process, from the BIOS to the operating system kernel. The measurements are recorded in a secure boot log, which can be used for verification and attestation purposes.
    - **Boot attestation** is a security feature that allows a remote party to verify that a system has booted up in a trusted state by checking the measurements recorded in the secure boot log. This can be used to ensure that the system has not been tampered with or compromised before allowing it to access sensitive resources. Boot attestation can be performed by a remote attestation service, which compares the measurements of the local system with a known good configuration to determine whether the system is trustworthy.

Evaluation of network security - Tools

Fingerprinting a server is a process of identifying a server's operating system, installed applications, and other configuration details by analyzing network packets, server responses, and other data. This information can be used to identify potential vulnerabilities that could be exploited by attackers.

Protocol analyzer (packet sniffer): Hardware or software that captures packets to decode and analyze their contents. Allows for you to easily view traffic patterns, identify unknown traffic, and verify packet filtering and security controls.

Big data analytics: Allows for the user to store large amounts of data and then easily go through it.

Network scanners: A computer program used for scanning networks to obtain user names, host names, groups, shares, and services.

- **Rogue system detection**: Find devices that are not supposed to be on the network, such as rogue APs.
- **Network mapping**: Identifying all devices on a network along with a list of ports on those devices.

Wireless scanners/cracker:

- **Wireless scanners**: Is for wireless monitoring, it scans wireless frequency bands in order to help discover rogue APs and crack passwords used by wireless APs.
- **Wireless cracker**: Uses wireless attacks to test if an attacker could find the passwords to gain access to parts of your network.

Password cracker: A program that uses the file of hashed passwords, such as a rainbow table, and then attempts to break the hashed passwords of the network. Getting the hashes is the hardest part.

Configuration compliance scanner: A vulnerability scanner that verifies systems are configured correctly and meet the minimum-security configurations, it typically does this by comparing the system to a file that has the proper configurations. This is an ongoing task and can be integrated with the logon process.

Exploitation frameworks: An already created set of exploits that already have all the major components designed, the user just needs to figure out how to inject them into the network.

Data sanitization tools: Tools that overwrite data on hard drives so that it is unrecoverable.

Steganography tools: Allows for the user to embed data into an image, video, sound files, or packets.

Honeypots and honeynets are security tools that are used to detect and monitor malicious activity on a network. A honeypot is a simulated network service or application that is designed to attract and trap attackers.

Honeynet is a network of honeypots that are used to provide a more comprehensive picture of the attacker's activities. These tools allow security professionals to observe attackers in action and gather information about their tactics, **techniques, and procedures (TTPs)**, which can then be used to improve the overall security of the network.

Backup utilities: Important to protect data from being lost, downtime, or corrupted.

Banner grabbing is a technique used to gather information about a target system through its open ports. By connecting to the target system's port, a hacker can retrieve the banner, which often contains information about the operating system, web server, and other applications running on the system.

Penetration testing and vulnerability scanning (vulnerability scanner)

Command line tools

ping: Tests reachability, it is a primary troubleshooting tool.

netstat (Network statistics) **Netstat** is a command-line tool used to display information about network connections, routing tables, and network interface statistics:

- netstat -a: Show all active connections.
- netstat -b: Show binaries, for Windows.
- netstat -n: Does not resolve names.

tracert (Windows)/**traceroute** (MacOS/Linux): Uses the ICMP (Internet Control Message Protocol) time to live (TTL) error message to map the path of a packet. Time in TTL is measured in hops, TTL = 1 for the first router, and 2 refers to the second router.

nslookup/**dig** (Domain Information Groper):

- **nslookup**: Used to gather information from DNS servers, lookups names and IP addresses.
- **dig** (Domain Information Groper): More advanced than nslookup and shows more detailed domain information.

arp (Address Resolution Protocol): Used to view MAC addresses.

- Arp -a: Views the local arp table.

ipconfig/ip/ifconfig:

- ipconfig/ifconfig: Shows the Windows/Linux TCP/IP configuration.
- ip: Used to replace ifconfig on Linux. Shows and manipulates settings on the network interface card (NIC).

tcpdump: A command-line packet analyzer that allows to capture packets from the command line.

nmap: It is designed to scan a network and create a map, this is useful as a vulnerability scanner because it can find open ports and unsecured access points.

netcat: Is used to safely connect to remote systems using command line instead of a front-end application. Can also be used for banner grabbing.

Analyze And Interpret Output From Security Technologies

Antivirus/advanced malware tools, firewall, DLP, Patch management tools (including silent patching),

Intrusion detection/prevention systems:

- **Intrusion Detection System (IDS)** is a security technology that monitors network traffic for malicious or unusual activity, raises an alert and/or takes defensive action when it detects such activity.
- **Intrusion Prevention System (IPS)** is an advanced version of IDS that not only detects but also actively blocks malicious traffic before it can cause harm to the system.
- **Host-based intrusion detection system (HIDS)**: Runs on a single computer and alerts of potential threats to help warn of attacks against that host.
- **Host-based intrusion prevention system (HIPS)**: Runs on a single computer and intercepts potential threats to help prevent attacks against that host.

Endpoint Detection and Response (EDR) is a cybersecurity technology that detects and responds to threats on endpoint devices, such as laptops and servers. EDR solutions typically use machine learning and behavior analysis to identify anomalous activity and provide real-time alerts to security teams.

File integrity check (FIC): An application that can verify that the files have not been modified using hash algorithms to authenticate the file.

File Integrity Monitoring (FIM): A security solution that monitors and verifies the integrity of files and system configurations to detect any unauthorized changes that may pose a risk to the organization.

Application whitelisting/blacklisting: The practice of allowing only approved programs to run on a computer, computer network, or mobile device.

Removable media control: Blocks users from using USB drives, CD/DVD drives or portable hard drives/flash drives.

UTM (Unified Threat Management): A group of security controls combined in a single solution that can inspect data streams for malicious content and block it.

Data execution prevention (DEP): Memory regions are marked as non-executable which prevents code from being executed. This protects against memory abuse attacks such as buffer overflows.

Troubleshoot Common Security Issues

Unencrypted credentials/clear text: All authentication must be encrypted.

Logs and events anomalies: Block all outside access until the issue is fixed, backup and preserve the current logs, and if possible, restrict access to more sensitive data till the issue is fixed.

Permission issues: Determine how much access a specific user needs to be able to complete their job. Confirm permissions on initial configurations, perform periodic audits, and provide a process for changes and updates.

Access violations: Segmentation fault, OS locks you out, or prevents access to restricted memory. A user is able to properly logon and then access systems they don't have proper authorization for.

Certificate issues: Certificates should be signed by someone trusted, be up to date, and be properly checked.

Data exfiltration is a form of a security breach that occurs when an individual's or company's data is copied, transferred, or retrieved from a computer or server without authorization

Misconfigured devices:

- **Firewall**: Provide too much access, and to audit when using a large rule base.
- **Content filter**: URLs are not specific, and some protocols are not filtered.
- **Access points**: No encryption mechanisms and Open configurations from the wireless side.

Weak security configurations: Make sure to regularly upgrade equipment and update firmware. Using hash algorithms that are susceptible to collisions.

Personnel issues: The weakest link

- **Policy violation**: Transferring private data or visiting unsafe websites.
- **Insider threat**: Authenticated users have free reign. Assign correct user rights and permissions.
- **Social engineering**: Deceit can cause employees to give up personal or valuable data.
- **Social media**: Sharing private data or personal information.
- **Personal email**: Uses company resources and leaves the network vulnerable.

Unauthorized software: Don't know what it is: could conflict with company software, could be malware, or could be useful for work.

Baseline deviation: Everything is well documented, any changes to the norm should be noted, and no remote access until it matches the baseline.

License compliance violation (availability/integrity): Make sure licenses are up to date and valid.

Asset management: Identify and track assets to respond faster to security risks. Keep detailed records of the most valuable assets. Usually, automated.

Authentication issues: The more factors the safer, makes sure the user is actually the correct person.

Mobile Devices Secured

Connection methods and its risks

1. **Cellular**: Network used for mobile phones.
    - Potential Risks: Cellular devices are susceptible to traffic monitoring, location tracking, and gain access to the device from anywhere in the world.
    - SIM Cloning & ID Theft (solution – Subscriber Identity Module)
    - Mobile device theft (solution – remote lock/wipe, pin, encryption)
2. **WiFi**: A local area network that uses high frequency radio signals to transmit and receive data over short distance.
    - Potential Risks: If the WiFi connection is not encrypted it is vulnerable to eavesdropping. Jamming frequencies or interferences can cause a denial of service.

3. **Satellite Communications (SATCOM)** that is used for communications in remote areas and during natural disasters.
    - Potential Risks: SATCOM devices are at risk of leaking geopositioning data and remote code execution, and are not easily updated remotely.
4. **Bluetooth**: Allows electronic devices like cell phones and computers to exchange data over short distances using radio waves.
5. **NFC (Near Field Communication)**: Enable two electronic devices in short proximity to each other. Typically used as a payment system, but can also be used as an identity token and to help pair Bluetooth devices.
    - Potential Risks: Active devices can perform a remote capture up to a ten meter range. Jamming frequencies or interferences can cause a denial of service. Can be vulnerable to relay and replay attacks.
6. **ANT/ANT+**: A wireless sensor protocol that uses a 2.4 GHz ISM (industrial, scientific, and medical) band to communicate. Used in heart monitors, sports and fitness sensors.
    - Potential Risks: At risk of jamming band, and eavesdropping because encryption is vulnerable.
7. **Infrared**: Electromagnetic waves of frequencies lower than the red of visible light. Used to control entertainment devices and other IR devices.
8. **USB (Universal Serial Bus)**: A cable used to connect mobile devices to other devices. Is comparatively safer than wireless because it requires a physical connection and data is not allowed to be transferred without being unlocked first.

Mobile device management concepts:

Application management: Limiting which applications can be installed on a device.
Content management: Limiting access to content hosted on company systems, and controlling access to company data stored on mobile devices.
Remote wipe: Allows for the deletion of all data and possibly even configuration settings from a device remotely.
Geofencing: Using GPS to define geographical boundaries where the app can be used.
Geolocation: The location of a device identified by GPS.
Screen locks: Prevents someone from being able to pick up and use a mobile device.
Push notification services: Send messages to mobile devices from apps without user intervention.
Passwords and pins: Keep the device safe with something you know.
Biometrics: Keep the device safe with something you are.
Context-aware authentication: Uses multiple elements to authenticate a user and a mobile device.
Containerization: isolating and protecting the application, including any data used by the application.
Storage segmentation: Separates the information on a device into partitions.
Full device encryption: Scramble all of the data on the device. Protects against loss of confidentiality.

Enforcement and monitoring

Third-party app stores: Anything that isn't from the Apple's App Store or Google Play. More likely to be a risk to security.
Rooting/jailbreaking:

- **Rooting**: Android, the process of modifying the device to gain root-level (full administrator) access.
- **Jailbreaking**: the process of removing all software restrictions from the device.

Sideloading: The process of copying an application package to a mobile device.
Custom firmware: The removal of the pre-installed firmware and replacing it.
Carrier unlocking: Means the device can be used by any carrier.
Firmware OTA updates: The over the air downloading of: upgrades, patches, and improvements to the existing firmware.
Camera use: Disable it except for certain locations to prevent espionage.
SMS/MMS: Sending alerts through text messages.
External media: Disable it to prevent the transferring of files through physical ports.
USB OTG (Universal Serial Bus On-The-Go): A cable used to connect mobile devices to other devices.
Recording microphone: Disable it to prevent people from being able to listen in on conversations.
GPS tagging: Adding GPS information to the video, photo giving its location
WiFi direct/ad hoc: Means for wireless devices to connect directly to each other without a wireless access point.
Tethering: The process of sharing an Internet connection from one mobile device to another.
Payment methods: To pay for services wirelessly over a limited area.

Deployment models:

BYOD (Bring Your Own Device): Employees to connect their own personal devices to the corporate network to work.
COPE (Corporate Owned, Personally Enabled): Are owned by the organization, but can be used personally by employees.
CYOD (Choose Your Own Device): Employees can purchase devices on the list and bring them to work. The company then supports, monitors, and manages the device.
Corporate-owned: Company owns and controls all aspects, no personal info at all, most secure for company.
VDI (Virtual Desktop Infrastructure)

BYOD challenges

Data ownership: When personal and professional data are stored on the same device, it can be difficult to determine who owns and is responsible for the data.
Device support: With a variety of different devices being used, it can be difficult for IT teams to provide support for all of them.
Patch and antivirus management: It can be challenging to ensure that all BYOD devices are up-to-date with the latest patches and protected with antivirus software.
Forensics: When an incident occurs, it can be difficult to conduct forensics on a device that is not owned by the organization.
Privacy challenges: Personal devices may contain sensitive personal information that can be difficult to protect when used for work purposes.
Onboard cameras/devices: Onboard cameras and other devices can present security risks, as they may be used to capture sensitive information.

Architecture/infrastructure consideration: Organizations need to consider how BYOD devices will interact with their existing infrastructure and architecture.

Legal concerns: BYOD can raise a number of legal concerns, such as liability for data breaches and compliance with data protection regulations.

3.0 ARCHITECTURE AND DESIGN

Frameworks, Best Practices And Secure Configuration Guides.

Industry-standard frameworks and reference architectures

Framework: Is a collection of standardized policies, procedures and guides, meant to direct a: user, firm, or any organization.

Regulatory: Is a framework that is based on mandated laws and regulations. HIPAA is an example of this.

Non-regulatory: The common standards and best practices that the organization follows.

National: Framework based on the laws of a single country.

International: Framework based on the laws of multiple countries.

Industry-specific frameworks: Frameworks based on the standards and regulations of a certain industry.

Benchmarks/secure configuration guides

Benchmarks/secure configuration guides: Instructions that have been developed over years that are designed to give organizations the best and most secure configurations for a particular system.

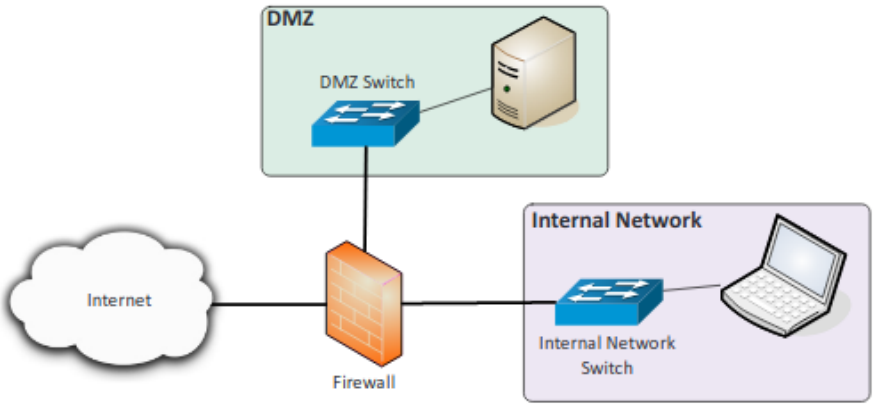
Platform/vendor-specific guides: Hardening guides that are specific to the software or platform, also you can get feedback from the manufacturer or internet interest groups. System default configurations are unsecured and at high risk for exploits.

General purpose guides: Security configuration guides that are generic in scope.

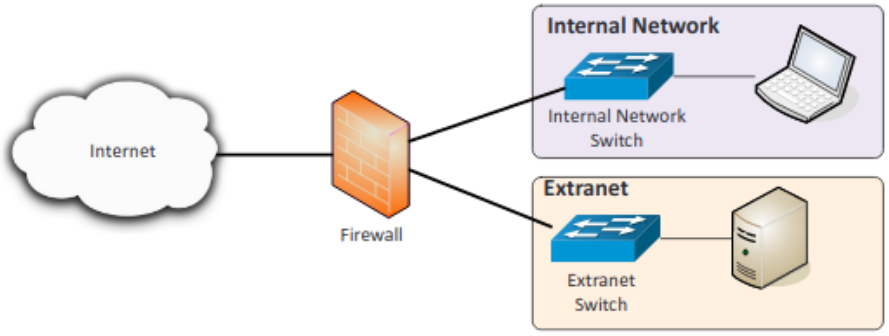
Secure Network Architecture Concepts

Zones/topologies

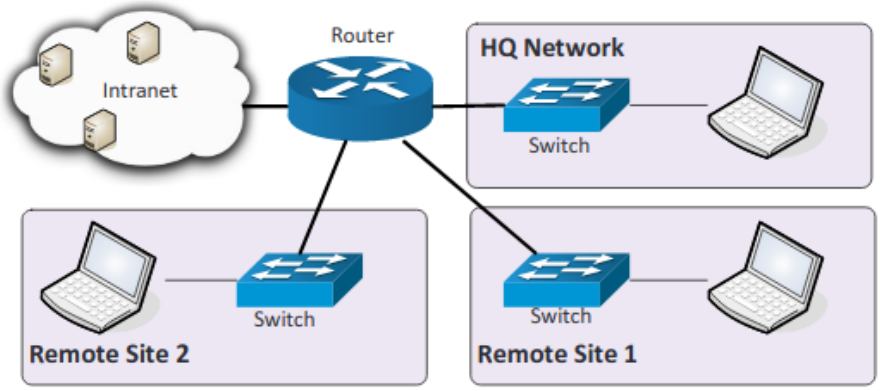
DMZ (Demilitarized Zone, perimeter network, buffer zone) is a physical or logical network segment that separates an organization's internal network from the public internet. The DMZ is designed to provide an additional layer of security to the internal network by hosting critical systems and services that need to be publicly accessible, such as web servers and email servers. This way, if the DMZ is compromised, the attacker will not have direct access to the internal network.



Extranet: Private network that can only be accessed by authorized individuals. Links a company with its suppliers and customers.



Intranet: A private network that exclusively for the use of the members of the organization, cannot be accessed by anyone outside the organization.



Wireless: Generally, requires a login, an example is an internal wireless network at work.
Guest: Network with access to the internet but no access to the internal network. Is useful in congested areas and is generally unsecured.
Honeynets: Dummy Network to attract and fool attackers.
Ad hoc: A wireless network without an access point, the connected devices communicate directly.

Separation for performance, security, or compliance

Network separation refers to the practice of dividing a network into separate subnets or virtual LANs (VLANs) to improve security and isolate different segments of the network. This helps to prevent unauthorized access to sensitive areas of the network and reduce the impact of security breaches.

Types of network separations

- **Physical**: Devices are separate and cannot directly communicate unless physically connected. Does not scale well.
- **Logical** (VLAN): Separate areas are segmented for different networks, but still housed on the same switch. To connect them you need a layer 3 device, such as a router.

Virtualization: The hardware to separate networks is virtualized, including routers, switches, and other devices apart from the infrastructure. Easier to manage from a security standpoint and everything can be segmented.

Air gaps: Network where the devices are physically separate from another and don't share any components to **communicate**. Great for security but be careful with removable media.

VLAN management refers to the process of configuring and maintaining virtual local area networks (VLANs) on a network. This includes creating VLANs, assigning devices to VLANs, and managing the

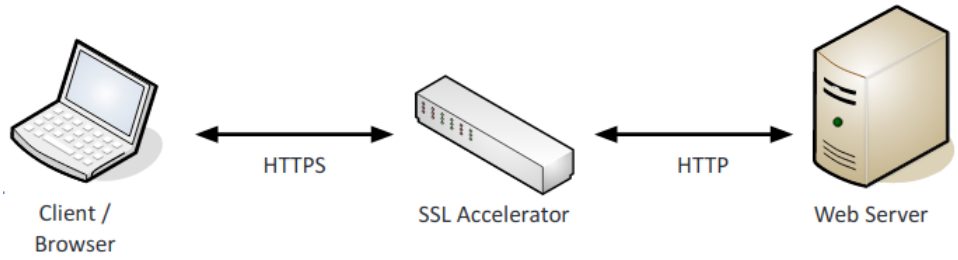
security and access control of the VLANs. VLAN management is an important aspect of network security and helps to ensure that sensitive information is protected.

Security device/technology placement

Sensors: Can give transactions, logs, or other raw data. Can be integrated or built-into switches, servers, firewalls, routers, or other network devices.

Correlation engines: Can be built in SIEM, tries to compare and correspond data collected from the sensors to determine if an attack is present.

SSL accelerators: Offloads the SSL process to a hardware accelerator. SSL handshake is complicated and time consuming.



Taps and port mirror: Physical tap sees what is happening in traffic packets, and software port mirror sends a copy of the traffic packets. Is better for light traffic.

SDN (Software Defined Networking) Aims to separate the hardware layer from the control. The network is fully virtualized with software, and then separated into the control (configuration) and data plane (forwarding and firewalling). Directly programmable from a central location, often automatically.

Network security enchancement techniques

Monitoring system logs, **hardening systems, firewalls, IDS, IPS, Virtual Private Networks**

Establishing a security posture: This involves developing and implementing security policies, procedures, and guidelines to ensure the consistent application of security measures across the organization. It also involves regularly reviewing and updating these measures to keep up with changing security threats.

Secure Systems Design

Hardware/firmware security

1. **FDE (Full Disk Encryption)** - Programs and technologies that encrypt everything on the storage drive.
2. **Self-Encrypting Drive (SED),** is a type of hard drive that automatically encrypts data as it is written to the drive, without requiring any user input. This provides an additional layer of security for sensitive data.
3. **TPM (Trusted Platform Module)** is a security chip or component that is built into a computer's motherboard, which is used to securely store and protect cryptographic keys, passwords, and other sensitive data. TPM provides hardware-based security functions such as secure boot, secure storage of keys, and remote attestation of a device's configuration and integrity.
4. **HSM (Hardware Security Module)** is a dedicated cryptographic processor that provides secure storage and management of digital keys and other sensitive information. HSMs are commonly used for key management, encryption, and digital signing in applications that require high levels of security, such as financial transactions, digital identity management, and government security.

TPM and HSM are both specialized security hardware-based devices designed to provide secure storage and processing of sensitive information. They have different usage.

5. **Secure boot and attestation**: Processes that checks and validates system files during the boot process.
6. **Supply chain**: The process of getting a product or a service from the beginning supplier to the user.
7. **Hardware root of trust**: Shows that there was a secure starting point, this is proved by TPMs having a private key burned into the hardware.

Operating systems

OEM – original equipment manufacturer – means that the product was manufactured by the original company.

Types of systems:

- **Network**: Supports servers, workstations, and other network-connected devices.
- **Server**: Designed to function as a server.
- **Workstation**: Optimized for user applications such as email and office apps.
- **Appliance**: A system designed to serve a purpose.
- **Kiosk**: A system or computer with a touch screen designed to provide information or directions.
- **Mobile OS**: The OS of phones, tablets, and other handheld devices.

Peripherals risks

Wireless keyboards: Operate in the clear allowing for the capturing of keystrokes with a receiver to be controlled remotely.

Wireless mice: Operate in the clear allowing for the capturing of movements or to be controlled remotely.

Displays: Vulnerable to shoulder surfing, firmware hacks, and eavesdropping.

WiFi-enabled MicroSD cards: Portable storage device that has access to 802.11 Wi-Fi file transfers.

External storage devices: No authentication allows for anyone to read, write and move files.

Digital cameras: Easy to steal data.

SQL vs NoSQL databases

Data Structure: SQL databases store data in a structured way, in tables with fixed columns and rows, and require a pre-defined schema. NoSQL databases store data in an unstructured way, allowing for more flexibility in the types of data that can be stored.

Scalability: NoSQL databases are often better suited for large-scale applications with high data volumes and multiple nodes, as they are designed to be horizontally scalable. SQL databases, on the other hand, are often vertically scalable and require more complex and expensive hardware to handle large volumes of data.

Querying: SQL databases use a standardized language, SQL (Structured Query Language), to query the data, which allows for complex joins and transactions. NoSQL databases often use their own query languages, which may be more limited in functionality, but faster and more flexible in handling unstructured data.

ACID Compliance: SQL databases are generally ACID (Atomicity, Consistency, Isolation, Durability) compliant, which means that they ensure data integrity and consistency through transactional processing. NoSQL databases may sacrifice ACID compliance for higher scalability and performance.
Use cases: SQL databases are often used for traditional business applications, such as accounting, finance, and customer relationship management (CRM). NoSQL databases are often used for web and mobile applications, big data analytics, and real-time applications.

Overall, the choice between SQL and NoSQL databases will depend on the specific needs of the application, as well as the scale, complexity, and type of data being stored and queried.

Secure Staging Deployment Concepts

Sandboxing: Virtualizes a deployment process, allows for machines to be completely isolated from each other, and is similar to the environment that will be used.
Environment: Usually tested in the actual environment that the product will be used in.

Stages of software development and deployment (DTSP)

1. **The Development** environment is where software development takes place, including coding, testing, debugging, and collaboration among developers.
2. **The Testing** environment is where software is tested for functionality and performance, including unit testing, integration testing, and system testing.
3. **The Staging** environment is a replica of the Production environment used to test the software in a production-like environment. This environment is used to identify issues and verify that everything works as expected before deploying the software to the Production environment.
4. **The Production** environment is where the software is deployed and used by end-users. It is the live system that should be stable, secure, and highly available.
   Using DTSP helps ensure that software is thoroughly tested before deployment and that changes are made in a controlled and consistent manner. It also enables developers and testers to work collaboratively without impacting the Production environment.

Secure baseline: Defines the core of what the development team must do. Lays out what will need to be updated in the future.
Integrity measurement: Tests against the baseline to keep it secure.
Agile methodology is a way to manage a project by breaking it up into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage. Once the work begins, teams cycle through a process of planning, executing, and evaluating.

Support of systems and software

Continuous monitoring is the process of regularly and systematically collecting and analyzing data to assess the security posture of an organization's information systems. This involves monitoring various aspects of the systems such as network traffic, system logs, user activity, and vulnerabilities to identify potential threats or risks. The goal of continuous monitoring is to provide real-time visibility into the security posture of the organization and to enable prompt detection and response to security incidents.
Continuous deployment is a software development practice where changes to software are automatically and continuously deployed to production environments as soon as they are approved and

pass the necessary tests. This process involves automating the entire software development lifecycle, including building, testing, and deployment, to ensure that changes are delivered quickly and reliably. Continuous deployment is often used in agile software development environments to increase the speed and efficiency of software delivery.

Continuous validation is the process of continuously testing and validating software to ensure that it meets the required standards and specifications. This involves automating the testing process and running tests continuously throughout the software development lifecycle to identify and address issues early in the process. Continuous validation is essential to ensure that software is of high quality and meets the requirements of stakeholders.

Continuous integration is a software development practice where developers regularly integrate their code changes into a shared repository, and automated build and testing processes are triggered to ensure that the changes are integrated successfully and do not introduce errors. The goal of continuous integration is to enable developers to work collaboratively and to identify and resolve issues quickly and efficiently. Continuous integration is often used in agile software development environments to improve code quality and speed up the development process.

The Security Implications Of Embedded Systems

Embedded systems: These are specialized computer systems designed for specific tasks, such as controlling machinery or monitoring systems. They often have limited processing power and memory, making them vulnerable to attacks. To mitigate risks in embedded systems, it's important to secure the communication channels and restrict access to the system. Firmware updates and patches should also be regularly applied.

To mitigate these risks, some best practices include:

- Implementing strong access controls and authentication mechanisms
- Conducting regular vulnerability assessments and penetration testing
- Hardening systems by disabling unnecessary services, protocols, and interfaces
- Implementing encryption
- Monitoring and logging all system activity
- Keeping systems and software up to date
- Providing security awareness training to employees

Embedded systems examples:

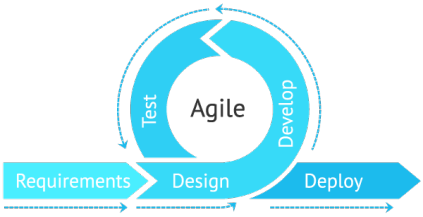
1. **Smartphones, game consoles, in-vehicle computing systems**
2. **SCADA (Supervisory Control and Data Acquisition)** systems are used for controlling, monitoring, and analyzing industrial devices and processes. The system consists of both software and hardware components and enables remote and on-site gathering of data from the industrial equipment .
3. **Smart devices/IoT** (Internet of Things): A mobile device that allows the user: customizable options, applications to help make daily activities easier, and an AI to assist in tasks.
4. **Mainframes** are large, centralized computer systems used by many organizations to store and process large amounts of data. To mitigate risks in mainframes, it's important to restrict access to

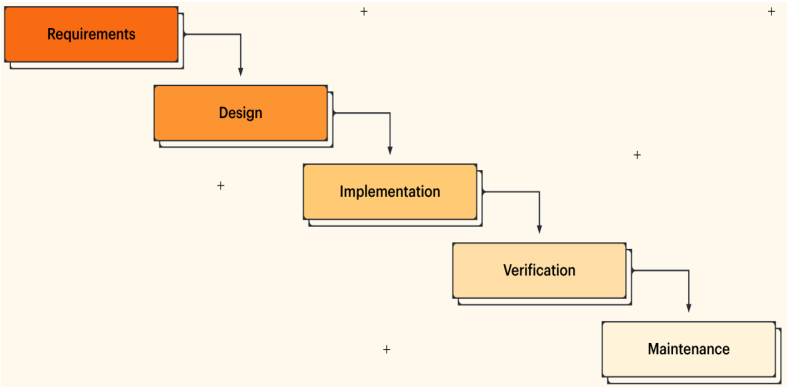
the system and implement strong authentication methods. Regular audits and vulnerability scans can also help identify potential security weaknesses.

5. **HVAC stands for Heating, Ventilation, and Air Conditioning**, which are the systems used to control the temperature, humidity, and air quality in a building or facility.
6. **Mobility as a Service (MaaS),** is a concept that involves providing transportation services as a package or subscription, rather than individual services. This may include various modes of transportation, such as public transit, ride-sharing, and bike-sharing, and is often enabled by digital technologies and platforms.
7. **System on a Chip (SoC)** An embedded device where the entire system is on the chip.
8. **Real Time Operating Systems (RTOS)** Attempts to use predictability to see what happens to meet real time requirements, the guesses must be secured.
9. **Printers/Multi-Function Devices (MFDs)**: Contains logs, documents, and sensitive information that can be accessed and stolen.
10. **Camera systems**: Videos recorders and cameras are IP devices. The risk is that they can be hacked.
11. **Special purpose:**
    - Medical devices: Can be attacked leaving patients at risk.
    - Vehicles: Contains onboard Wi-Fi vulnerable to threats.
    - Aircraft/UAV: Can have communications intercepted.

Secure Application Development And Deployment Concepts.

1. **Development life-cycle models:**





- **Waterfall**: A sequential development process that flows like a waterfall through all phases of a project with each phase completely wrapping up before the next phase begins.
- **Agile**: Flexible: allows for collaboration between groups, and can go back and fix previous iterations.

2. **Secure DevOps:**
    - Security automation: Tools that automatically tests security functions, penetration, and for vulnerabilities.
    - Continuous integration: The basic set of security checks while developing.
    - Baselining: Comparing current performance to previously set metric.
    - Immutable systems: Are locked and unable to change. To update the entire platform must be updated.
    - Infrastructure as code: Turns the devices into code to allow for focusing on the application needs instead of based on available infrastructure.

3. **Version control and change management:** The ability to track change and ability to revert to previous versions.
4. **Provisioning and deprovisioning**: The adding and removing of assets over time. Installing new devices and uninstalling old ones.

Secure coding techniques

1. **Application hardening/patch management, encryption, obsfucation/camouflage**
2. **Proper error handling**: Errors do not crash the system, allow for elevated privileges, or expose private information.
3. **Proper input validation**: Sanitizing data to make sure it is correct and secure before using.
4. **Normalization**: Applying rules to a database design to ensure that the proper information goes in the proper places.
5. **Stored procedures**: A program in the database that enforces the business rules.
6. **Code signing**: Assigning a digitally signed certificate to code.
7. **Code reuse/dead code**: Reusing code in multiple contexts. Code that cannot be executed.
8. Server-side vs. client-side execution and validation:
    - **Server-Side**: Code runs on the server.
    - **Client-Side**: Code runs in the browser, is highly vulnerable to attacks.
9. **Memory management**: Checking and ensuring that the program does not use too much memory.
10. **Use of third-party libraries and SDKs**: Commonly used so is better understood by attackers.
11. **Data exposure**: Disclosing private information to attackers.
12. **Exception handling**: The process of detecting and managing errors in software code, typically through the use of catch blocks or similar mechanisms that allow for graceful recovery and secure handling of unexpected conditions.
13. **Client side and server side validation**: The process of validating input data on both the client (user) side and server side of a software application to prevent malicious input and attacks like SQL injection.
14. **Cross-site scripting (XSS) prevention**: Techniques used to prevent the injection of malicious code into web applications, particularly through user input fields. This includes sanitizing input data, encoding output data, and other strategies to prevent unauthorized code execution.
15. **Cross-site request forgery (XSRF) prevention**: Techniques used to prevent attackers from executing unwanted actions on behalf of authenticated users, particularly through the use of hidden tokens and other techniques to prevent unauthorized form submissions.
16. **Application configuration baseline**: A set of secure configuration settings and requirements for software applications, designed to ensure that all applications are consistently configured to meet established security standards.

Code quality and testing

Static code analyzers: Checks source code for: conformance to coding standards, quality metrics, and for data flow anomalies.

Dynamic analysis (fuzzing): Providing unexpected inputs to cause the application to crash.

Stress testing: Seeing how many users a program can handle at a time.

Sandboxing: Using a virtual machine to run the program in a simulated environment to determine if it will properly run. Does not affect production equipment.

Model verification: Ensuring the program meets specifications and performs its purpose.

Compiled vs. runtime code:

- **Compiled Code**: Code that is optimized by an application and converted into an executable.
- **Runtime Code**: The code that is interpreted as it runs.

Cloud And Virtualization Concepts

Hypervisor: A software, firmware or hardware that creates, manages, and operates virtual machines.

- **Type I**: Known as bare metal, runs on the hardware.
- **Type II**: Known as hosted, runs on top of the operating system.
- **Application cells/containers**: Abstracting applications from the platform into containers allowing for applications to run without launching an entire virtual machine. This provides portability and isolation, and less overhead than VM.

Cloud storage: The process of storing data in an off-site location that is leased from a provider.

Live migration occurs when a VM is moved from one physical server to another over the network.

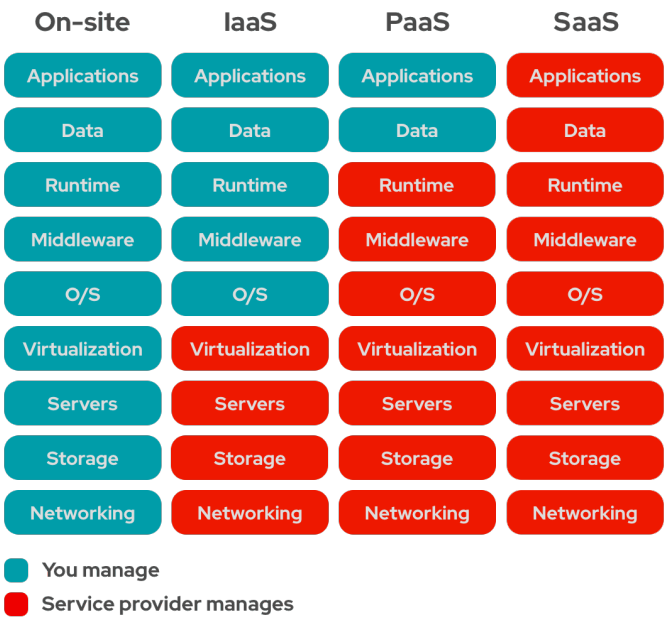
VDI (Virtual Desktop Infrastructure)/VDE (Virtual Desktop Environment): The virtualization of a user's desktop where the applications are running in the cloud or in a data center, the user runs as little of the application as possible on the local device.

Fog Computing is a distributed computing architecture that brings computational resources closer to the edge of the network, reducing latency and improving performance for IoT devices and applications. In fog computing, data is processed at the edge of the network, rather than being transmitted to a central data center for processing.

Virtual Private Cloud (VPC) is a cloud computing model that provides a private, isolated virtual network in the cloud for an organization's use. VPCs can help organizations control access to cloud resources and improve.

Cloud deployment models:

SaaS (Software as a Service) is a cloud computing model in which a third-party provider delivers software applications over the internet, usually on a subscription basis. SaaS eliminates the need for organizations to install and maintain software applications on their own systems, instead allowing them to access the software via the internet. SaaS is typically offered as a service, with the provider handling all aspects of maintenance, updates, and security. Examples: email services, customer relationship management (CRM) systems, and project management tools.



PaaS (Platform as a Service) is a cloud computing model in which a third-party provider delivers a platform that enables organizations to develop, run, and manage their applications and services. PaaS includes all the infrastructure required to build and deploy applications, including servers, storage, and databases. This eliminates the need for

organizations to invest in and maintain their own infrastructure, making it easier and more cost-effective to develop and deploy applications. Examples: Heroku, Amazon Web Services (AWS) Elastic Beanstalk, and Microsoft Azure.

IaaS (Infrastructure as a Service) is a cloud computing model in which a third-party provider delivers infrastructure services over the internet, including computing resources such as servers, storage, and networking. IaaS eliminates the need for organizations to invest in and maintain their own physical infrastructure, allowing them to access the services they need on a pay-per-use basis. Examples: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

IaaS → PaaS → SaaS

XaaS - The term "XaaS" refers to anything as a service, a broad reference to the huge number of options that exist for services via third-party providers.

A la carte (cloud service) refers to a cloud computing model where customers can select and pay for only the specific services they need, rather than purchasing a pre-defined package of services. This provides greater flexibility and cost savings for customers.

Cloud classifications

Public Cloud is a cloud computing service that is owned and operated by a third-party service provider and made available to the general public over the Internet. Public clouds allow users to rent computing resources, such as storage and processing power, on a pay-per-use basis without having to invest in and maintain their own infrastructure. Public clouds are typically cost-effective, scalable, and accessible from anywhere with an Internet connection.

Private Cloud is a cloud computing environment that is dedicated to a single organization and is not made available to the general public. Private clouds can be built and maintained by the organization itself or by a third-party service provider and offer the benefits of cloud computing, such as scalability and cost savings, while maintaining control over the security and privacy of the data and applications.

Hybrid Cloud is a combination of both public and private clouds that allows organizations to take advantage of the benefits of both types of clouds. A hybrid cloud allows organizations to keep sensitive data and applications on a private cloud for security reasons while using public clouds for non-sensitive data and applications. This allows organizations to take advantage of the cost savings, scalability, and accessibility of public clouds while maintaining control over the security and privacy of sensitive data.

Community Cloud is a cloud computing environment that is shared by multiple organizations that have a common set of security, privacy, and compliance requirements. Community clouds are typically operated by a third-party service provider and offer the benefits of a shared infrastructure while maintaining the security and privacy of the data and applications. Community clouds are used by organizations in the same industry or geographic region and are cost-effective, scalable, and secure.

On-premise vs. hosted vs. cloud:

- **On-premise**: Built and managed by the company's data center. Allows for complete control over it. Has a high investment cost and operational cost.
- **Hosted**: Leasing the network and storage that is off site. Access and availability depends on the design. Has No investment cost, and a moderate operational cost
- **Cloud**: Leasing the network and storage that can be on or off site. Has no investment cost, and a low operational cost. Can be accessed anywhere, anytime and has high mobility.

VM threats and solutions

VM Escape - An attack that allows an attacker to break out of a normally isolated VM by interacting directly with the hypervisor

Data Remnants - Contents of a virtual machine that exist as deleted files on a cloud-based server after deprovisioning of a virtual machine

Security as a service (SECaaS): The provider implements their security services into your environment via the cloud, such as: authentication anti-virus, anti-malware, IDS, and event management.

VM sprawl avoidance: The avoiding of a VM getting too large for the admin to properly manage. To avoid it the admin should: enforce a strict process for deploying VMs, have a library of standard VM images, archive or recycle under-utilized VMs, and implement a Virtual Machine Lifecycle management.

VM escape protection: The avoiding of an attacker accessing the host system from within the VM. To avoid it: keep hosts and guests up to date with current patches.

CASB (Cloud Access Security Broker) is a security solution that provides visibility and control over cloud services used by an organization, helping to enforce security policies and protect against data loss. The CASB serves as a policy enforcement center, consolidating multiple types of security policy enforcement and applying them to everything your business utilizes in the cloud.

Cloud storage security practices

- Cloud storage providers must implement security controls such as data encryption, access controls, and monitoring to prevent data breaches and unauthorized access
- Data stored in the cloud must be properly classified and protected according to its sensitivity level to ensure compliance with relevant regulations

Resiliency and automation strategies to reduce risk

1. Automation/scripting:
   - **Automated courses of action**: Automated scripts that give a basis for secured configuration with a secured template. Can be configured to accommodate for constant changes or can be launched on a specific schedule.
   - **Continuous monitoring**: Monitors IDS/ logs, networks, SIEMs, and other systems for changes and threats.
   - **Configuration validation**: Reviewing the settings of the system to ensure that its security settings are configured correctly.
2. **Templates**: Gives a basis for secured configuration with a standard secured configuration.
3. **Master image**: Is crafted configuration of a software or entire system. Created after the target system is installed, patched, and configured.
4. **Non-persistence**: Changes are possible. Due to risks of unintended changes, multiple protection and recovery options must be established.
   - **Snapshots**: A copy of the live current operating environment.
   - **Revert to known state**: Is a recovery process that goes back to a previous snapshot.
   - **Rollback to known configuration**: Just a collection of settings. Does not usually include software elements.

- **Live boot media**: A portable storage device that can boot a computer. Is read-to-run or a portable version of the OS.

5. **Elasticity**: The ability for the system to adapt to a workload by allocating and providing resources in an automatic manner.
6. **Scalability**: The ability to handle an ever-increasing workload and able to accommodate future growth.
7. **Distributive allocation**: Is providing resources across multiple services or servers as necessary instead of preallocation or concentrated resources based on physical system location.
8. **Redundancy**: Secondary or alternate solutions, it's an alternate means to complete tasks. Helps reduce single points of failure and boosts fault tolerance.
9. **Fault tolerance**: The ability for the: network, system, or computer to provide a service while withstanding a certain level of failures. Aids in avoiding a single point of failure, a SPoF is anything that is mission critical.
10. **High availability**: Refers to a system that is able to function for extended periods of time with little to no downtime.
11. **Redundant Array of Independent Disks (RAID)** Is a high availability solution. Employs multiple hard drives in a storage volume with a level of drive loss protection, except for RAID 0.

RAID Level	Description	Details
RAID 0	Striping without parity	High performance, no fault tolerance
RAID 1	Mirroring	Duplicates data for fault tolerance, but requires twice the disk space
RAID 5	Striping with parity	Fault tolerant, only requires an additional disk for redundancy
RAID 0+1, RAID 1+0, RAID 5+1, etc.	Multiple RAID types	Combine RAID methods to increase redundancy

Raid 0 - splitting data across two disks simultaneously (increases speed, but if one disk fails, you lose data)

Raid 1 - duplicate files on two disks simultaneously (mirror)

Raid 4 - one disk can fail, but data usefulness remains. Striping across multiple disks. The service area is responsible for data recovery.

RAID 10, also known as RAID 1+0, is a data storage technology that combines the benefits of both RAID 1 (mirroring) and RAID 0 (striping). It provides both data redundancy and increased data performance by combining the mirrored data on two sets of drives with striping.

Physical Security Controls

Control types

Administrative controls are policies, procedures, and regulations that provide guidance for protecting physical and environmental assets. **Technical controls** involve the use of technology, such as locks, cameras, and alarms, to prevent unauthorized access to facilities and equipment. **Operational controls** are processes and procedures that support and enforce the security measures implemented by administrative and technical controls.

Control solutions

1. **Lighting**: If the perimeter is properly lit it can deter thieves, break-ins, and other criminal activity.
2. **Signs**: Allows for controlled entry point, is a psychological deterrent, and helps new and visitors find their way. Informs of security cameras, safety warnings, and that an area is restricted.
3. **Fencing/gate/cage**: A fence sets the boundaries of the property and protects against casual intruders. Gates allow for controlled entry and exit. Cages protect assets from being accessed by unauthorized individuals.
4. **Security guards**: Humans are adaptable, can adjust to live events, and can react to real time intrusion events. Can intervene and control the security devices.
5. **Alarms**: Notify security personnel and the authorities of unauthorized activities.
6. **Safes/Secure cabinets/enclosures**: Restricts unauthorized personnel from accessing assets.
7. **Protected distribution/Protected cabling**: Is a standard on how to safely transmit unencrypted data. Protects from wire-taps.
8. **Access control vestibule/Mantrap** is a type of physical security measure that is used to control access to a building or secure area. It consists of an enclosed space that is situated between two doors, where individuals are screened for authorized access before being allowed to enter the secure area. Access control vestibules may include features such as security cameras, metal detectors, biometric scanners, and other security measures to ensure that only authorized personnel are granted access. This type of security measure is commonly used in high-security environments, such as government buildings, data centers, and financial institutions.
9. **Airgap**: Ensure secure networks are physically isolated from unsecure networks.
10. **Lock types**: Can use a key, key-pad, cards, or biometrics.
11. **Biometrics**: Uses physical characteristic, such as a fingerprint, for authentication.
12. **Barricades/bollards**: Stops and guides traffic, it can also prevent the entrance of vehicles.
13. **Tokens/cards**: Items necessary to gain access to secured areas of the building. Can contain information that can identify and authorize an individual.
14. **Environmental controls:**
    - **HVAC**: Keeps servers from overheating and shutting down.
    - **Hot and cold aisles**: Allows for air flow control and for the air to move through the data center strategically.
    - **Fire suppression**: Protects the equipment from fire, smoke, corrosion, heat, and water damage. Early fire detection is vital for protecting personal and equipment from harm.
    - **Special Hazard Protection** - Clean Agent System - Fire suppression system that relies upon gas (HALON, FM-200, or CO2) instead of water to extinguish a fire.
15. **Cable locks**: Protects small equipment from theft.
16. **Screen filters**: Reduces the range of visibility to prevent shoulder suffering.
17. **Cameras**: Deters criminal activity and creates a record of events.
18. **Motion detection**: Senses movement and sound in a specific area.
19. **Logs**: Document visitor access, allows for the identifying and record keeping of everyone who has access to the premise.
    - **Log aggregation** is the process of collecting and combining log data from multiple sources into a single location for analysis. This helps simplify log management and enables easier and

faster troubleshooting of issues. Examples of log aggregation tools include Elasticsearch, Splunk, and Logstash.

- **Log collectors** are tools that collect log data from various sources and forward it to a central log aggregator. They may also perform some level of pre-processing on the logs, such as filtering out noise or adding additional metadata. Examples of log collectors include Fluentd, rsyslog, and syslog-ng.

Log collectors → Log aggregators

- **Log parsers** are tools that parse log data to extract relevant information and present it in a more readable format. They can be used to identify specific patterns or anomalies in log data and to help with troubleshooting issues. Examples of log parsers include awk, sed, and grep.
- **Log enrichment** is the process of adding additional metadata to log data to provide more context and make it easier to analyze. This may include information such as the hostname, IP address, or user ID associated with a particular log event. Examples of log enrichment tools include Loggly and Graylog.

20. **Infrared detection**: Detects and monitors changes in the temperature.
21. **Key management**: Ensure only authorized individuals only have access to the areas they need to complete their work.
22. **Shielding**
    - Shielded Twisted Pair (STP) adds a layer of shielding inside the cable
    - Faraday Cage - Metal screen to protect equipment from electrostatic and electromagnetic influences.

4.0 IDENTITY AND ACCESS MANAGEMENT

Identity And Access Management Concepts

AAA authetication

AAA protocol (Authentication, Authorization, and Accounting protocol), which is a security framework used for granting access to resources, tracking user activity, and enforcing policies.

- **Identification**: Finding the unique individual on the system.
- **Authentication**: The ability to tell if an individual is actually who they claim they are.
- **Authorization**: Determining what an individual can and cannot access on a system.
- **Accounting**: The tracking of an individual's actions on the system.

Multifactor authentication: Uses at least two of the factors of authentication.

- **Something you are** (biometric, face recognition)
- **Something you have** (smart card, usb token, phone)
- **Something you know** (password, pin, pattern)
- **Somewhere you are** (location, IP, geolocation area)
- **Something you do** (handwriting, typing technique, biometrics)

Federation: The authenticating and authorizing between two parties. Ex. Logging onto Facebook with Google account.

Single sign-on (SSO): Only uses one of the factors of authentication.

Transitive trust: There are more than two entities, one entity is trusted because they are trusted by someone the company trusts.

Install And Configure Identity And Access Services.

Lightweight Directory Access Protocol (LDAP): Queries information about the directory. Is a hierarchical structure; CN = Common Name, OU = Organizational Unit, DC = Domain Controller. Utilizes TCP/IP, TCP/UDP ports 389.

Secure LDAP: LDAP over SSL/TLS, uses TCP on port 636.

Kerberos: developed for mutual authorization between client and server. It uses a ticket granting system for authorization.

Terminal Access Controller Access Control System (TACACS+): Runs TCP over port 49, encrypts all parts of communication. Does not suffer due to security issues caused by RADIUS. Authorization and Authentication are separated for granular control.

Challenge Handshake Authentication Protocol (CHAP): Authenticates PPP clients to the server. Uses a one-way hash based on a shared secret that is compared on the client and server end. Does not send plaintext over the wire.

Password Authentication Protocol (PAP): Username and password are sent as plaintext and are no longer used.

MS-CHAP (Microsoft CHAP): Delivers a two-way, mutual authentication between the server and client. Separate keys are created for sent and received data. Is seen as weak due to it using a 5-bit encryption system, same as NTLM.

RADIUS (Remote Authentication and Dial-in User service): Combines authentication and authorization, only encrypts the passwords, each network device must contain an authorization configuration. There is no command logging, and minimal vendor support. Uses ports 1812 for authentication and authorization and port 1813 for accounting functions.

SAML (Security Association Markup Language): Authenticates through a third-party source to gain access, the resource is not responsible for the authentication. The request is passed through a trusted third-party server.

- The three roles are: Principle (the user or client), identity provider (the one who assures the identity of the principle), and service provider (a web service of some type.)

OpenID Connect: OpenID Connect handles the authentication part of the identification process and uses OAuth for authorization.

OAUTH (Open Standard for Authorization): Token authorization happens in the background. Uses a logon from a larger trusted service.

Shibboleth: An open-source software that uses SAML to provide a third-party federated SSO authentication.

Secure token: An authentication mechanism that can be used to identify and authenticate, and to deny and allow access.

Soft Token is a software-based authentication method that generates a one-time password (OTP) for use in two-factor authentication (2FA). Soft tokens are typically installed on a userKVMS

NTLM (New Technology LAN Manager): Used for authenticating in a Windows domain, was replaced by Kerberos for the most part.

- NTMLv2: Is the most common form used, is somewhat insecure.

Context-aware authentication is a security approach that takes into account contextual factors when granting access to a resource. Contextual factors may include the user's location, device, behavior, and other attributes. By evaluating these factors, context-aware authentication can provide a more secure and flexible approach to authentication.

Impossible Travel Time is a security alert generated by a system when a user's access activity shows that they could not have physically traveled the distance between two locations in the time reported. This alert is used to detect and prevent potential unauthorized access attempts

Implement Identity And Access Management Controls.

Access control is the process of restricting access to resources based on policies and rules that determine who or what is allowed to access those resources. It involves managing access to systems, applications, data, and other resources to ensure that only authorized users are granted access while unauthorized users are denied.

A trusted operating system (OS) is an operating system that provides a level of security and integrity beyond that of a typical operating system. It is designed to prevent unauthorized access and to protect against malicious software and attacks. A trusted OS includes features such as access control, auditing, encryption, and secure boot to ensure the security and integrity of the system.

1. **Access control models:**
   - **MAC (Mandatory Access Control):** Based on classification rules. Objects are given sensitivity labels, subjects given clearance labels, and users obtain access by having the correct clearance. The classifications are hierarchical.
   - **DAC (Discretionary Access Control):** Is based on user identity. Users are granted access through ACLs placed on objects through the object's owner or creator.
   - **ABAC (Attribute Based Access Control):** Assigning access and privileges through a scheme of attributes. Relations and criteria determine access; time of day, location, and/or IP address.
   - **Rule-based access control (RBAC)** is an access control model that uses a set of rules to determine whether to grant or deny access to a resource. These rules can be based on a variety of factors, such as the user's job function, the resource being accessed, or the time of day.
   - **Access control list (ACL)** is a list of permissions that specifies which users or groups are granted or denied access to a particular resource. ACLs can be used to control access to files, directories, and other resources.

- **Separation of duties (SoD)** is a security principle that states that critical tasks should be divided among two or more people, so that no one person has complete control over them. This helps prevent fraud and errors by making it more difficult for any one person to abuse their privileges.
- **The principle of least privilege (PoLP)** is a security concept that states that users should only be given the minimum level of access necessary to perform their jobs. This helps reduce the risk of accidental or intentional damage caused by users with excessive privileges.
- **Implicit deny** is a default-deny access control mechanism that denies access to any resource that has not been explicitly granted access. This means that if a user or process is not explicitly granted access to a resource, access is automatically denied.
- **Time of day restrictions** limit access to resources based on the time of day. For example, an organization may restrict access to a sensitive database to certain hours of the day when authorized personnel are available to monitor activity.
- **Role-based access control (RBAC)** is an access control model that assigns users to roles based on their job function, and then grants access to resources based on those roles. This helps simplify administration and reduces the risk of granting excessive privileges to individual users.
- **Lattice-based Access Control** - Utilizes complex mathematics to create sets of objects and subjects to define how they interact. Only in high security systems due to its complex configuration

2. **Physical access control:**
    - **Proximity cards**: A smart card that does not require direct contact.
    - **Smart cards**: Cards that contain identification/authentication information in an integrated circuit chip. Often uses dual factor authentication; something you have (the card), and something you know (a pin or password).
3. **Biometric factors: Verifies identity through physical features.**
    - **Fingerprint scanner**: Scans the unique patterns of the fingerprint to grant access.
    - **Retinal scanner**: Blood vessels in the back of the retina.
    - **Iris scanner**: Scans the Iris.
    - **Voice recognition**: The identification and translation of spoken language for authorization of a user. Is vulnerable to impersonation.
    - **Facial recognition**: The identification of an individual from a digital image or a video frame. Is vulnerable to impersonation.
    - **Vein recognition** is a technology that uses near-infrared light to scan and identify the unique patterns of veins in a person's hand or finger. Vein recognition is considered highly accurate and secure and is used in applications such as access control and time and attendance.

False Acceptance Rate (FAR) refers to the probability that the system will incorrectly accept an unauthorized user as an authorized one. This can happen, for example, if the system's threshold for determining a match between the biometric sample and the stored template is set too low.

False Rejection Rate (FRR) refers to the probability that the system will incorrectly reject an authorized user as unauthorized. This can happen, for example, if the biometric sample taken at the time of authentication is of low quality or if the user has a medical condition that affects the biometric feature.

CER (Equal Error Rate) is measure commonly used in biometric authentication systems, which represents the point at which FAR and FRR are equal. At this point, the system is said to have achieved optimal performance, balancing the risk of false positives and false negatives.

4. **Tokens**
    - **Hardware**: A device that displays and constantly generates a pin or password.
    - **Software**: An app or software that generates a token.
    - **HOTP/TOTP**: Open source standards to generate one-time use passwords.
        - HOTP (HMAC-based One-Time Password): Can be used only once before it expires.
        - TOTP (Time-based One-time Password): Only last for around 30 seconds before it expires.
5. **Certificate-based authentication**:
    - **PIV (Personal identity verification)/CAC (Common access card)/smart card**: Cards that have embedded certificates and a photo ID for authorization. The US DOD uses CAC/PIV.
    - **IEEE 802.1x**: Offers port-based authentication to wireless and wired networks to prevent rogue devices from connecting to secured ports.

Account roles/ownership/priviledge types

Shadow IT refers to the use of technology, such as software, hardware, or cloud services, without the approval or knowledge of an organization's IT department. Shadow IT can pose security risks and may result in compliance violations or data breaches.

Account types:

- **User account**: An account that is a collection of information that identifies an individual and grants them specific areas of the network or system.
- **Shared and generic**: Multiple individuals sign into a single account. No workplace should have these, cannot distinguish the actions of the user.
- **Guest accounts**: An anonymous shared logon account.
- **Service accounts**: Performs specific maintenance actions, such as a backup, account and server operators.
    - **Incident response team (IRT)**: Responsible for handling incidents within the department.
- **Privileged accounts**: Access is set to access rights, generally referred to as system or network administrative accounts.
- **Executive user**: Responsible for the overall operation of the application, makes decisions and evaluates goals.

Ownership:

- **Data owner**: Executive level manager, responsible for data security.
- **System administrator**: Are responsible for the overall security of a system and enable the applications and data.
- **System owner**: Executive level manager, has overall responsibility for the system.

Roles in company

CTO (Chief Technology Officer) is a high-level executive responsible for overseeing the technology strategy and operations of a company. The CTO typically works closely with other executives and stakeholders to ensure that the company's technology initiatives align with its overall business objectives.

DPO (Data Protection Officer) is a position responsible for ensuring that a company's data processing activities comply with relevant data protection laws and regulations. The DPO typically works with other executives and stakeholders to develop and implement data protection policies and procedures.

The Chief Information Officer (CIO) is a senior executive responsible for the information technology (IT) strategy, infrastructure, and operations of an organization. The CIO ensures that technology is aligned with business goals, manages IT budgets, and oversees cybersecurity and data management.

DBA (Database Administrator) is a person responsible for managing and maintaining a company's database systems. The DBA typically ensures that the databases are secure, backed up, and optimized for performance.

User roles safe solutions

General Concepts:

- **Least privilege**: Rights and permission are set to bare minimum.
- **Onboarding/offboarding:**
  - Onboarding: Helps new employees learn all of the facets of their new job.
  - Offboarding: Helps leaving employees learn how to properly leave and potentially return to the company.
- **Permission auditing and review**: Looks at the rights and perms assigned to users.
- **Usage auditing and review**: Logging information on what users do.
- **Time-of-day restrictions**: Certain privileges are permitted or restricted based on the time of day.
- **Recertification**: The action of regaining a certification due to the certification being expired.
- **Standard naming convention**: Allows for the easier identification of resource location and purpose. Reduces the amount of time needed for troubleshooting and training.
- **Account maintenance**: Making sure that accounts have the proper privileges, and unused accounts are deleted. Generally done through scripts to save time and money.
- **Group-based access control**: Every user in a group has the same privileges.
- **Location-based policies**: Grants and denies access based on the user's location.

Account policy enforcement:

- **Credential management**: Stores, manages, and tracks user credentials.
- **GPO (Group Policy Object)/Group policy** a set of rules or policies that can be applied to groups of users or computers in an organization, enabling centralized management and control of these resources. GPOs can be used to enforce security settings, software deployment, and other system configuration settings across an entire network.
- **Acceptable Use Policy (AUP)** is a set of rules and guidelines for the use of an organization's computer network, systems, and services. AUPs typically outline acceptable and unacceptable behaviors and may include consequences for violating the policy.
- **Expiration**: The amount of time that passes before a password is required to be changed.
- **Recovery**: The ability to find lost passwords and usernames in case an employee forgets them.
- **Disablement**: Disabling an account.
  - Disable the Guest account on your systems
- **Lockout**: Prevents login from specific individual after a set of failed login attempts, for a set period of time.
- **Enable CTRL+ALT+DEL** for logging into the system

- **Password history**: Remembers past passwords and prevents the reuse of passwords.
- **Password reuse**: The ability to ever use the same password again.
- **Password length**: The minimum amount of characters that can be used in a password.
- **Default credentialds**: Always require the user to change the default password of the account.
- **Password age**: A policy that sets how long a user can have a password before they are forced to change it.
    - Require that the password is changed frequently (every 90 days)
- **Password complexity**: The enforcing of complex and difficult to guess passwords.
    - Contain uppercase letters, lowercase letters, numbers, special characters, and at least 8 characters or more (preferably 14 or more)

Integrating data and systems with third parties

Risk Awareness is the recognition and understanding of potential threats and vulnerabilities to an organization's assets, including people, systems, and information.

Onboarding and offboarding of business partners refers to the process of bringing a new business partner into the organization and terminating the relationship with an existing business partner.

Interoperability agreements are contracts or agreements between organizations or systems that define how they will exchange information and resources in a secure and reliable manner. These agreements help ensure that systems can communicate and exchange data seamlessly, and are often necessary for organizations that need to exchange sensitive information.

Data backups are copies of data that are created for the purpose of protecting against data loss or corruption.

Data ownership refers to the responsibility and authority over the creation, management, and use of data within an organization.

Compliance and performance standards are requirements and guidelines that organizations must follow to ensure the security, reliability, and performance of their systems and information.

Following security policies and procedures is the adherence to a set of guidelines and protocols that help ensure the security of an organization's information and assets.

5.0 RISK MANAGEMENT

Risk assessments/risk analysis/threat assessments is a process of evaluating potential security threats to an organization. This includes identifying the sources of the threats and the potential impacts of those threats on the organization

Vulnerability assessments is an evaluation of the potential security weaknesses or vulnerabilities in an organization's information systems or networks.

Threat hunting - can involve a variety of activities such as intelligence fusion, combining multiple data sources and threat feeds, and reviewing advisories and bulletins to remain aware of the threat environment for your organization or industry.

Intelligence fusion is the process of collecting and analyzing information from multiple sources to provide a comprehensive view of a particular situation or event. This approach combines information from various sources such as social media, news reports, and government agencies, to provide a more

complete and accurate understanding of the situation. Intelligence fusion is commonly used in law enforcement, military, and intelligence communities.

Proprietary threat intelligence - Proprietary, or closed threat, intelligence is threat intelligence that is not openly available.

ISACs (Information Sharing and Analysis Centers) help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency."

Feedburner is Google's RSS feed management tool, and vertical threat feeds is not an industry term.

STIX and TAXII - The AIS service uses STIX and TAXII. STIX and TAXII are open standards that the Department of Homeland Security started the development of and uses for this type of effort.

A TAXII server is a client that exchanges standardized and anonymized cyber threat intelligence among users. It works as a venue for sharing and collecting Indicators of compromise, which have been anonymized to protect privacy.

Indicators of compromise (IoCs) - There are many indicators of compromise (IoCs), including unusual outbound network traffic, geographical irregularities like logins from a country where the person normally does not work, or increases in database read volumes beyond normal traffic patterns.

End-of-Life (EOL) is a term used to describe the point in time when a product or service is no longer supported by its manufacturer or vendor. This means that no further updates, security patches, or technical support will be provided, leaving the product or service vulnerable to security threats and other issues.

End-of-Support-Life (EOSL) refers to the date when a product or service is no longer supported by the manufacturer or vendor. This means that no further support will be provided, and the product or service may become obsolete or incompatible with other technologies.

Predictive analysis - is analysis work done using datasets to attempt to determine trends and likely attack vectors so that analysts can focus their efforts where they will be most needed and effective.

Threat maps - are often real-time or near real-time visualizations of where threats are coming from and where they are headed to.

Log aggregation and log collectors - Using log aggregation to pull together logs from multiple sources, and performing collection and initial analysis on log collectors can help centralize and handle large log volumes. Capturing packets is useful for network traffic analysis to identify issues or security concerns.

Risk approaches

Risk Avoidance - A strategy that requires stopping the activity that has risk or choosing a less risky alternative.

Risk Transfer - A strategy that passes the risk to a third party.

Risk Mitigation - A strategy that seeks to minimize the risk to an acceptable level.

Risk Acceptance - A strategy that seeks to accept the current level of risk and the costs associated with it if the risk were realized.

Residual Risk - The risk remaining after trying to avoid, transfer, or mitigate the risk.

Control types

Management controls (PEOPLE) refer to the policies, procedures, and practices that are implemented by an organization to manage and control risks. They are typically established by senior management and are designed to provide guidance and direction to the organization on how to address security and risk management issues. Examples of management controls include security policies, incident response plans, and security awareness training programs.

Technical controls (THINGS) refer to the hardware and software solutions that are implemented to protect information systems and data. They are designed to prevent, detect, and respond to security threats. Examples of technical controls include firewalls, intrusion detection systems, encryption, and access controls.

Operational controls = (Management + technical controls) refer to the day-to-day practices and procedures that are used to maintain the security of information systems and data. They are designed to ensure that the technical controls are functioning properly and that the policies and procedures established by management are being followed. Examples of operational controls include change management processes, configuration management, and security monitoring.

Assessment techniques

Baseline reporting: A method that involves collecting information about a system's configuration and status, including hardware and software specifications, as well as its security settings, policies, and procedures. This information is used as a reference point to detect and respond to changes or deviations in the system's state.

Code review: A technique that involves analyzing the source code of an application to identify any security weaknesses, such as buffer overflows, input validation errors, or misconfigurations.

Attack surface review: A method that involves examining the different ways an attacker might be able to access a system or network, including network protocols, ports, services, and applications.

Architecture review: A technique that involves evaluating the design of a system, network, or organization from a security perspective, including its security controls, processes, and policies.

Design review: A method that involves evaluating the design of a system, network, or organization from a security perspective, including its security controls, processes, and policies. This technique is often performed before implementation to identify and address security concerns early in the development process.

Vulnerability Scanning

Nessus, Qualysguard, and AlienVault

Scan, Patch, Scan, ...

Passively test security controls: Uses an automated vulnerability scanner. Observes and reports findings. Does not take down systems, applications, or services, and doesn't disrupt business.

Identify vulnerability: Understanding common attacks and taking inventory of vulnerabilities. Scanners can report: missing updates, misconfigured security settings, and known exploits.

Identify lack of security controls: Vulnerability scanners can identify missing patches or antivirus.

Identify common misconfigurations: Weak passwords, default usernames and passwords, and open ports.

Intrusive scan - attempts to actively exploit vulnerabilities, and thus could possibly cause some disruption of operations. For this reason, it should be conducted outside normal business hours or in a test environment, if it is used at all.

Non-intrusive scan - attempts to identify vulnerabilities without exploiting them. A penetration test actually attempts to breach the network by exploiting vulnerabilities. An audit is primarily a document check. Both intrusive and non-intrusive vulnerability scans can be effective at finding vulnerabilities.

Credentialed vs. non-credentialed

- **Credential Scan:** A vulnerability scan that uses an authorized user's login credentials to test a network, system, or application's security posture. The scan simulates an attack that uses a valid username and password to gain access to the target. This type of scan is used to identify vulnerabilities in systems that are only accessible by authenticated users.
- **Non-Credential Scan:** A vulnerability scan that does not use an authorized user's login credentials. Instead, the scan relies on other methods, such as IP addresses, to identify vulnerabilities in systems, networks, or applications. Non-credential scans can be useful for identifying vulnerabilities in systems that are publicly accessible and can provide a baseline for security posture.

False positive vs false positive

- **False positive**: A result which shows incorrectly that a condition or attribute is present. A false vulnerability.
- **False negative** - occurs with a vulnerability scanning system when a scan is run and an existing issue is not identified. This can be because of a configuration option, a firewall, or other security settings or because the vulnerability scanner is otherwise unable to detect the issue. A missing vulnerability update might be a concern if the problem did not specifically state that the definitions are fully up-to-date.

Penetration Testing

Active reconnaissance vs passive reconnaissance

- **Active reconnaissance**: Is the use of tools to send data to systems and then understanding their responses. Usually starts with various network and vulnerability scanners. Can be incredibly illegal and should not be engaged without being prepared and proper authorization.
- **Passive reconnaissance**: You are not touching any of the target's equipment. Instead you are going through and gathering that is already available. Forums and social media are great sources for gathering information about the company and its employees.

Pivot: In penetration testing it is using a compromised machine to attack other machines on the same network. Attacking and gaining access to an area of lower security in order to be more likely to have a successful attack on an area of greater security. Is also referred to as island hopping.

Initial exploitation (initial access): Usually the hardest part. A vulnerability is taken advantage of to get into the network or system.

Persistence: Installing backdoors or methods to keep access to the host or networks.

Black vs white vs gray box:

- **Black box**: The pentester knows nothing about the network and have no prior knowledge.
- **White box**: The pentester have full knowledge of the configurations allowing you to perform specific tests.

- **Gray box**: Some knowledge of the network; a mix of black and white.

Penetration testing vs. vulnerability scanning

- **Penetration testing** is an active attack on the network to exploit vulnerabilities, can assess potential damages and the potential of the exploits being found. Is done by a human.
- **Vulnerability scans** passively scans and identifies vulnerabilities. Is automated.

SOC Type 2 report is a type of audit report that provides information on a company's internal controls, specifically those related to financial reporting, security, availability, processing integrity, and confidentiality. The report is prepared by an independent auditor and evaluates the effectiveness of the controls over a period of time, typically six months to a year.

Risk assessment evaluation

1. **SLE** (Single loss expectancy): The cost of any single loss.
2. **ARO** (Annual rate of occurrence): Indicates how many times the loss will occur in a year.
3. **ALE** (Annual loss expectancy): Is the value of SLE x ARO.

Annual Loss Expectancy = **Single Loss Expectancy** x **Annual Rate Of Occurence**

4. **Asset value**: Identifies the value of an asset and can include any product, system, resource, or process.
5. **Risk register**: A document listing information about risks.
6. **Likelihood of occurrence**: The probability that something will occur.
7. **Supply chain assessment**: An evaluation of the supply chain needed to produce and sell a product.

Qualitative vs quantitative risk assessments

Qualitative assessment (metoda jakościowa np. scenariusz) is a subjective, non-numeric evaluation of risks and vulnerabilities. It is used to evaluate factors such as the likelihood of a risk occurring, the potential impact of a risk, and the effectiveness of current controls. Qualitative assessments are often performed using qualitative methods such as expert opinion, scenario analysis, or checklists.

Quantitative assessment (metoda ilościowa np. badanie statystyczne), on the other hand, is an objective, numerical evaluation of risks and vulnerabilities. It is used to measure the exact magnitude or probability of a risk and its potential impact. Quantitative assessments are often performed using quantitative methods such as statistical analysis, simulation, or financial modeling.

In general, qualitative assessments provide a broad, high-level view of risks and vulnerabilities, while quantitative assessments provide a more detailed and precise evaluation. Both qualitative and quantitative assessments are important tools in the risk management process and are often used in combination to provide a comprehensive view of risks and vulnerabilities.

Policies, Plans And Procedures - Organizational Security

Agreement types

BPA (Business partners agreement): A written agreement detailing the relationship between business partners including their obligations.

SLA (Service level agreement): An agreement between a company and a vendor that stipulates performance expectations.

ISA (Interconnection security agreement): Specifies technical and security requirements for planning, establishing, maintaining and disconnecting a secure connection between two or more entities.

MOU/MOA (Memorandum of understanding/agreement): Expresses and understanding between two or more parties indicating their intention to work together toward a common goal.

NDA (Non-Disclosure Agreement) is a legal contract that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties.

Privileged user agreement: is a legal agreement that is signed by individuals who are granted privileged access to an organization's information systems or sensitive data. This agreement outlines the responsibilities and obligations of the privileged user, including their access rights, security requirements, and confidentiality obligations.

Document types

Standard operating procedure: A document that provides step-by-step instructions on how to perform common tasks or routine operations.

An annual privacy notice is a document that organizations are required to provide to their customers or clients on an annual basis. This notice outlines the organization's privacy policies and practices, including how personal information is collected, used, and shared. It also informs customers of their privacy rights and how they can exercise them.

Communication plan is a document that outlines the strategy and tactics for communicating with stakeholders during a project or crisis. It typically includes information on the audience, key messages, communication channels, and timing of communication.

IT security frameworks/benchmarks

Sherwood Applied Business Security Architecture (SABSA) is a risk-driven architecture

Control Objectives for Information and Related Technology (COBIT) - A security framework that divides IT into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate

NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)/NIST Risk Management Framework is a set of recommended security and privacy controls for federal information systems and organizations to help meet the requirements set by the Federal Information Security Management Act (FISMA). It provides a list of controls that support the development of secure and resilient federal information systems.

The framework includes six steps:

- categorize the system,
- select security controls,
- implement security controls,
- assess security controls,
- authorize the system,
- monitor security controls.

The RMF is intended to be flexible and adaptable to a wide range of systems and organizations and is designed to help organizations effectively manage cybersecurity risk while balancing the need for security with mission and business requirements.

ITIL (Information Technology Infrastructure Library) is a library of best practices for managing IT services and improving IT support and service levels. One of the main goals of ITIL is to ensure that IT services align with business objectives, even as business objectives change.

GDPR (General Data Protection Regulation): A regulation in the European Union that governs the protection and privacy of personal data for EU citizens.

ISO (International Organization for Standardization) ex. 27000 An independent, non-governmental international organization that develops and publishes standards for various industries, including information security.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements designed to protect credit card data and prevent fraud. PCI DSS applies to any organization that accepts credit card payments and specifies security controls for protecting cardholder data, such as encryption, access controls, and vulnerability management.

ISO 31000 Risk Management Framework – Guidelines, provides principles, a framework and a process for managing risk. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

CIS Benchmarks are a set of cybersecurity best practices and guidelines developed by the Center for Internet Security (CIS) for various technology systems and platforms. CIS Benchmarks provide detailed configuration guidance and recommended security settings to help organizations improve their security posture.

- **The CIS Controls Top 20** is a prioritized set of security best practices developed by the CIS to help organizations improve their cybersecurity posture. The CIS Top 20 includes 20 critical security controls that organizations should implement to protect against common threats.

Service Organization Control 2 (SOC 2) is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA) for evaluating the security, availability, processing integrity, confidentiality, and privacy of cloud-based service providers. SOC 2 reports provide independent assurance of a service provider's security controls and practices.

Personnel management

Separation of duties, Onboarding

Mandatory vacations: A policy that forces employees to take a vacation to deter malicious activity.

Job rotation: A process that ensures employees rotate through different jobs to learn the processes and procedures in each job.

Clean desk: A security policy requiring employees to keep their areas organized and free of papers.

Background checks: A check into a person's history to determine eligibility for a job.

- **Adverse actions**: Actions that denies employment based on the background check.

Exit interviews: An interview conducted with departing employees just before they leave an organization.

Continuing education: Personnel need to regularly receive additional training to ensure they are up to date on current threats, vulns and technologies.

- **Computer-Based Training (CBT)**, is a type of training through a computer or online platform.

Acceptable use policy/rules of behavior (AUP): A policy defining proper system usage and the rules of behavior for employees.

Social media networks/applications ban: People sharing their personal data that can result in inadvertent information disclosure or give attackers information to launch social attacks.

Disaster Recovery And Continuity Of Operation Concepts.

RTO (Recovery time objective): Identifies the maximum amount of time it should take to restore a system after an outage.
RPO (Recovery point objective): Refers to the amount of data you can afford to lose.
MTTF (Mean Time to Failure): average time a system or component is expected to function before failing
MTBF (Mean time between failures): Identifies the average time between failures with the goal of predicting potential outages.
MTTR (Mean time to recover): Identifies the average time it takes to restore/repair a failed system.
Mission-essential functions (MEF): A set of functions that must be continued throughout, or resumed rapidly after a disruption of normal operations.
Impact: The magnitude of harm related to a risk.

- **Life**: The most important consideration.
- **Property**: The risk to buildings and assets.
- **Safety**: Some environments are too dangerous to work.
- **Finance**: The resulting financial cost.
- **Reputation**: An event can cause status or character problems.

Privacy impact assessment (PIA): Attempts to identify potential risks related to the PII by reviewing how the information is handled.
Privacy threshold assessment (PTA): Helps the organization identify PII within a system.

Business continuity concepts

Business Continuity Planning (BCP) refers to the process of developing, implementing, and maintaining strategies and procedures that organizations follow to ensure the availability of critical business functions in the face of adverse events like natural disasters, cyber-attacks, and other disruptions. **The goal of BCP is to minimize downtime and the impact of these events on the organization's operations and reputation.**

Disaster Recovery Plan (DRP) is a subset of BCP and is specifically focused on restoring normal business operations as quickly as possible after a disaster. The DRP outlines the steps and procedures to be taken to get critical systems and functions up and running again in the aftermath of a disaster.
The purpose of a Disaster Response Plan is to ensure that an organization is prepared to respond effectively to a disaster and minimize its impact on the organization's operations, employees, and customers.

Business Impact Analysis (BIA) is the process of evaluating the potential impact of adverse events on critical business functions and systems, and determining which functions and systems are most critical to the survival of the organization. The information gathered during the BIA is used to develop and prioritize the strategies and procedures in the BCP and DRP.

Critical System and Component Identification: process of identifying and prioritizing critical systems and components within an organization's infrastructure that are essential for business operations.

Single point of failure (SPOF) is a part of a system or component that, if it fails, will cause the entire system to fail. SPOFs are a significant risk in organizational systems as they can cause widespread outages or disruptions to business operations.

Succession planning is a process in which an organization identifies and develops potential successors for key leadership positions within the organization. The goal of succession planning is to ensure the smooth transition of leadership and minimize disruption to business operations in the event of a sudden departure of a key leader.

IT contingency planning refers to the process of preparing and implementing plans to help an organization respond to and recover from potential IT disruptions or failures. The goal of IT contingency planning is to minimize downtime and ensure business continuity.

Continuity of operation planning: It focuses on restoring mission-essential functions at a recovery site after a critical outage.

BCP testing refers to the process of evaluating and verifying the effectiveness of a business continuity plan (BCP) through simulation or actual execution of the plan.

Fault tolerance

Fault tolerance is a security measure that ensures that a system remains functional even in the event of a component failure. This is accomplished through redundant components and automatic failover processes.

Server fault tolerance refers to the ability of a server to remain operational in the event of a component failure. This can be achieved through redundancy, load balancing, and failover processes.

Clustering is a technology that enables multiple servers to work together as a single entity, providing increased reliability and scalability. In the event of a server failure, another server can take over its workload.

Active node is a server within a cluster that is currently performing work.

Exercises/tabletop: A discussion-based exercise where participants talk through an event while sitting at a table.

Failover: The process of moving mission-essential functions to the alternate site.

Alternate processing sites: An alternate site that the organization can use after a disaster.

Alternate business practices: The organization can change the business practices after a disaster.

Power supply

Uninterruptible Power Supply (UPS), which is a device used to provide emergency power to a computer, server, or other electronic device in the event of a power outage.

Redundant Power - An enclosure that provides two or more complete power supplies. A redundant power supply mitigates a single point of failure.

Backup Generator - An emergency power system used when there is an outage of the regular electric grid power.

Managed PDU (Power Distribution Unit) is a device that distributes electrical power to multiple devices while providing monitoring, control, and management capabilities. It typically features remote monitoring and control functions through a network interface, allowing administrators to monitor power usage and control individual outlets from a central location. Managed PDUs are commonly used in data centers and

server rooms, where they help to improve power efficiency, reduce downtime, and ensure critical systems remain online.

Errors in power supply:

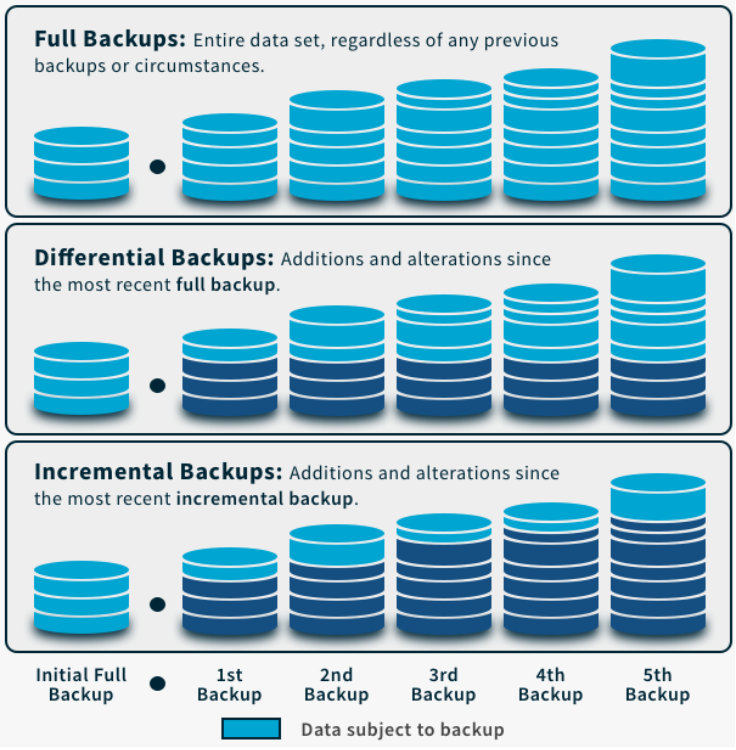
- **Surge** - An unexpected increase in the amount of voltage provided
- **Spike** - A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike
- **Sag** - An unexpected decrease in the amount of voltage provided
- **Brownout** - Occurs when the voltage drops low enough that it typically causes the lights to dim and can cause a computer to shut off
- **Blackout** Occurs when there is a total loss of power for a prolonged period

Backups

dd is a command-line utility for Unix-based operating systems that is used for copying and converting data between disks or files. dd can be used to create backup images, copy data between disks, and perform low-level disk operations.

Recovery sites: An alternate processing site that an organization can user after a disaster.

- **Cold site** - is a location which can be brought online but does not have systems; cold sites typically have access to power and bandwidth, but they need to be fully equipped to operate after a disaster since they are just rented space.
- **Warm sites** - have some or all of the infrastructure and systems, but does not have data.
- **Hot site** - is a fully functional environment with all of the hardware, software, and data needed to operate an organization. They are expensive to maintain and run but are used by organizations that cannot take the risk of downtime. Order of restoration: After the disaster has passed, the least critical functions go to the primary site first.



Backups: Copies of data created to ensure that if the original data is lost or corrupted, it can be restored.

Types:

Full: Backs up all the selected data.

Differential: Backs up all the data that has changed or is different since the last full backup.

Incremental: Backs up all the data that has changed since the last full or incremental backup. **it only backs up changes since the last backup.**

Snapshots: Captures the data at a point in time.

Backup time needed - In general, differential backups take more time than incremental ones to complete. However, when it comes to recovering

backup files, the tides change - differential restores are faster than incremental ones, as you need fewer data pieces to complete the recovery process**.**

From slowest to quickest: Full backup is the slowest because it backs up all data, regardless of whether it has changed since the last backup. Differential backup is faster than a full backup but slower than incremental backup because it backs up all changes since the last full backup. Snapshot is quicker than full backup and differential backup because it only copies the data at a point in time. Incremental backup is the quickest because **it only backs up changes since the last backup**.

Geographic considerations:

- **Off-site backups**: A copy of a backup should be stored in 2a separate location.
- **Distance**: Depends on the organization, the off-site location will be close or far away.
- **Location selection**: Depends on the environmental issues like earthquake zones.
- **Legal implications**: Depends on the data stored, the backup will be protected according to gov laws.
- **Data sovereignty**: The legal implications when data is stored off-site.

Incident Response Concepts

Computer Security Incident Response Team (CSIRT) is a group of cybersecurity professionals responsible for managing, handling, and responding to computer security incidents. CSIRTs may be internal or external to an organization and their main objective is to minimize the damage and impact of cybersecurity incidents by identifying and resolving them quickly.

Disaster Recovery as a Service (DraaS) is a cloud-based service that provides an organization with a remote, secure, and redundant environment for restoring critical IT infrastructure and data in the event of a disaster. DraaS allows organizations to quickly recover from a disaster and maintain business continuity.

Incident response plan (IRP): Provides more detail than the incident response policy.

1. **Documented incident types/category definitions**: Helps employees identify the difference between an event and an actual incident.
2. **Roles and responsibilities**: Many incident response plans identify specific roles for an incident response team along with their responsibilities.
3. **Reporting requirements/escalation**: Depending on the severity of the incident, sec personnel might need to escalate it or notify executives within the company of the incident.
4. **Cyber-incident response teams**: A cyber-incident response team is composed of employees with expertise in different areas.
5. **Exercises**: One method of preparing for incident response is to perform exercises.

Incident response process

1. **Preparation**: This phase occurs before an incident and provides guidance to personnel on how to respond to an incident.
2. **Identification**: All events aren't security incidents so when a potential incident is reported, personnel take the time to verify it is an actual incident.
3. **Containment**: After identifying an incident, sec personnel attempt to isolate or contain it.
4. **Eradication**: After containing the incident, it's often necessary to remove components from the attack.

5. **Recovery**: During the recovery process, admins return all affected systems to normal operation and verify they are operating normally.
6. **Lessons learned**: After personnel handle an incident, sec personnel perform a lessons learned review.

Forensics

The first step in forensics is the recognition that forensics measures need to take place – that a security incident has occurred.

First Responder Responsibilities: taking immediate actions to secure the incident scene, collect evidence, and minimize damage to the system and data during a security incident

Order of volatility: The order in which you should collect evidence.

Cache memory → regular RAM → swap or paging file → hard drive data → logs stored on remote systems → archived media.

Chain of custody: A process that provides assurances that evidence has been controlled and handled properly after collection.

Data acquisition and preservation:

- **Capture system image**: A forensic image of a disk captures the entire contents of the drive.
- **Network traffic and logs**: Helps re-create events leading up to and during the incident.
- **Capture video**: Video surveillance methods are used as a detective control during an investigation.
- **Record time offset**: An offset used by recorders to identify times on recordings.
- **Take hashes**: To provide proof that collected data has retained integrity.
- **Screenshots**: For capturing exactly what a user was doing or specific displays.
- **Witness interviews**: Provide firsthand reports of what happened and when it happened.
- **Live System Image**: a copy of a running operating system and all its data, used for forensic analysis
- **Static System Image**: a copy of a system taken at a specific time, used for offline forensic analysis
- **Creating a Tracking Log**: documenting all actions taken during an incident, including time stamps, details of evidence collected, and the individuals involved
- **Network Traffic and Log Files**: analyzing network traffic and log files to identify any unusual activities or signs of a security breach
- **Big Data Analysis**: using advanced analytics and machine learning techniques to process large volumes of data to identify patterns, trends, and anomalies, used for threat detection and incident response.

Strategic intelligence/counterintelligence gathering: A plan for increasing the amount of data that they collect.

- **Active logging**: This strategy increases the amount of logged data collected on a routine basis.

Track man-hours: Identify how much time and money is needed for a budget request.

Legal Hold is a legal process that requires an organization to preserve relevant data, such as electronic documents or email, for a pending or anticipated legal matter. Legal Hold ensures that data is not destroyed, altered, or deleted before it can be reviewed for legal purposes.

Software

Cuckoo is an open-source automated malware analysis system that can be used to analyze and report on the behavior of suspicious files and URLs. Cuckoo runs the suspicious files and URLs in a sandboxed environment and monitors their behavior to identify potential malicious activity.

Memdump (Memory Dump) is a snapshot of the contents of a computer's memory at a specific point in time. Memdumps are typically used in digital forensics to analyze the contents of a computer's memory for evidence of malicious activity or to recover lost data.

Autopsy is a digital forensics platform that can be used to analyze and investigate digital evidence, such as hard drives, memory dumps, and mobile devices. Autopsy provides a user-friendly interface for digital forensics investigators and includes features such as file recovery, keyword search, and timeline analysis.

Various Types Of Controls

Deterrent: Attempt to prevent incidents by discouraging threats.

Preventive: Attempt to prevent security incidents.

Detective: Attempt to detect when a vulnerability has been exploited.

Corrective: Attempt to reverse the impact of an incident or problem after it has occurred.

Compensating: Alternative controls used when it isn't feasible or possible to use the primary control.

Data Security And Privacy Practices

Data destruction and media sanitization: The organization has to ensure that the devices don't include any data.

- **Burning**: Burn printed materials in an incinerator.
- **Shredding**: Shred papers by passing them through a shredder.
- **Pulping**: An additional step taken after shredding paper.
- **Pulverizing**: The process of physically destroying media to sanitize it.
- **Degaussing**: A very powerful electronic magnet that renders the data on tape and magnetic disks unreadable.
- **Purging**: A general sanitization term indicating that all sensitive data has been removed from a device.
- **Wiping**: The process of completely removing all remnants of data on a disk.

Data sensitivity labeling and handling: Ensures that users know what data they are handling and processing.

- **Confidential**: Very sensitive, must be approved to view.
- **Private**: Internal use only, may require an NDA.
- **Public**: No restrictions on viewing the data.
- **Proprietary**: Is property of an organization.
- **PII (Personally Identifiable Information)** is a personal information that can be used to personally identify an individual.
- **PHI (Personal health information)** is PII that includes health information.

Data roles: An organization often assigns specific roles to some people with specific responsibilities:

- **Owner**: The individual with overall responsibility for the data. CEO or department head.
- **Data custodian/steward**: is responsible for the day-to-day management of data, including its storage, backup, and protection. They are tasked with ensuring that data is kept secure, confidential, and available when needed. Examples of data custodians include IT administrators, database administrators, and system administrators.
- **Data processor**: is responsible for processing data on behalf of a data controller. This may involve tasks such as data entry, data analysis, or data transformation. Data processors are required to follow the instructions of the data controller and to comply with data protection regulations. Examples of data processors include outsourcing service providers or third-party vendors who process data on behalf of an organization.
- **Data controller/privacy officer**: is the person or entity that determines the purposes and means of processing personal data. They are responsible for ensuring that data processing is carried out in compliance with relevant regulations, such as GDPR or CCPA. Examples of data controllers include businesses, government agencies, or non-profit organizations that collect and process personal data.

Data retention: Identifies how long data is retained and sometimes specifies where it is stored.

Legal and compliance: Organizations have a responsibility to follow all laws that apply to them, and ensure that they remain in compliance.

File and folder permissions

File and folder permissions refer to the settings that dictate who can access, modify, or execute files and folders on a computer system. These permissions are used to control user access to specific files or folders and to restrict access to sensitive data:

- **Read permission**
- **Write permission**
- **Execute permission**
- **Full Control permission**

Risk mitigation techniques

Application firewalls, Updates, Secure router configurations, Perform routine audits, Enforce policies and procedures, review of user rights and permissions, Disabling unnecessary ports and services,

CVSS (Common Vulnerability Scoring System) is a framework used to assess and prioritize the severity of security vulnerabilities. The framework assigns a numerical score to each vulnerability based on a variety of factors, including the exploitability of the vulnerability and the potential impact of an attack.

Change Management (CM): process of identifying, documenting, testing, and implementing changes to systems, processes, and configurations in a controlled and systematic manner

Incident Management: process of identifying, responding to, and resolving security incidents to minimize their impact on the organization

Data Loss Prevention (DLP): technologies, tools, and processes used to monitor and protect sensitive data from unauthorized access, theft, or loss.

Segmentation: The process of dividing a network into smaller subnetworks or segments to improve security by limiting access to critical resources and containing potential threats. Segmentation can be achieved through physical separation or logical isolation using firewalls, VLANs, or other network technologies.

Wrappers: A technique that adds an additional layer of security to a software application by encapsulating it with an external program that monitors the behavior of the application and restricts its access to system resources. Wrappers can be used to detect and prevent malware, buffer overflow attacks, or other security threats.

Subnetting: is the process of dividing a larger network into smaller, more manageable sub-networks. Subnetting helps to improve network performance and security by creating smaller, more secure segments of the network. Subnetting is performed by dividing a single IP address range into multiple sub-ranges, each of which is assigned to a different sub-network.

Firmware version control: The practice of managing and tracking changes to firmware, which is the low-level software that controls the hardware in devices such as computers, routers, or printers. Firmware version control is important for maintaining the security and stability of devices, as it allows organizations to apply security patches and updates to fix vulnerabilities and bugs. It also helps ensure that devices are running the correct firmware version and can detect unauthorized changes or tampering.

Defense in depth (security layers/layering) is a security strategy that involves implementing multiple layers of security controls to protect an organization's assets. The idea is to create multiple lines of defense, with each layer providing a separate layer of protection. If one layer is breached, the next layer should provide additional protection, making it more difficult for an attacker to succeed.

Vendor diversity: The practice of implementing security controls from different vendors to increase security. Reduces the impact of company specific vulnerabilities.

Application whitelisting/blacklisting: Protects the system from potentially dangerous applications.

- **Whitelisting**: Applications allowed on the system.
- **Blacklisting**: Applications blocked by the system.

Hardening physical hosts

- Operating system hardening
- OS security settings
- Anti-malware
- Patch management
- Trusted OS
- Applications whitelisting/blacklisting
- Host-based firewalls/intrusion detection systems

Host software baselining refers to the process of establishing a known and trusted configuration for an operating system and software applications installed on a computer.

Mobile device security

GPS, **Remote wiping**, **Full device encryption**, **Disabling unused features, Screen locks, Storage segmentation**, **credentials management, authentication, geotagging,**

Lockout settings: Lockout settings prevent attackers from repeatedly attempting to access a system by locking out the account after a specified number of failed login attempts.

Removable storage: Removable storage refers to any storage device that can be removed from a mobile device, such as an SD card or USB drive. It is important to protect any data stored on removable storage devices, as they can be easily lost or stolen.

Application controls: Application controls limit the access of an application to only the resources and data it needs to function, and prevent the application from accessing sensitive data or resources that it does not need to operate.

Inventory control: Inventory control is the process of keeping track of all mobile devices and their associated hardware and software components, to ensure that all devices are properly accounted for and secured.

Mobile device management (MDM) is a security framework that allows IT administrators to monitor, manage, and secure mobile devices and the data they contain.

Device access control: Device access control ensures that only authorized users can access a mobile device or its data. This can be achieved through authentication mechanisms such as passwords, PINs, or biometrics.

Wireless transmission risks

EMI (Electromagnetic Interference) caused by devices that can corrupt data or prevent data from being transferred.

EMP (Electromagnetic Pulse) a short burst of electromagnetic energy

Radio Frequency Interference (RFI) - A disturbance that can affect electrical circuits, devices, and cables due to AM/FM transmissions or cell towers. RFI causes more problems for wireless networks

Crosstalk - Occurs when a signal transmitted on one copper wire creates an undesired effect on another wire

Data Emanation - The electromagnetic field generated by a network cable or device when transmitting. A Faraday cage can be installed to prevent a room from emanating

Protected Distribution System (PDS) - Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats

Wireless security settings

1. **Cryptographic protocols (marked green are the most secure):**

WPA (Wi-Fi Protected Access): Uses RC4 with TKIP. Was replaced by WPA2. Every packet gets a unique 128-bit encryption key.

WPA2 (Wi-Fi Protected Access v2): Uses CCMP for encryption instead TKIP and AES instead RC4.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): Is based on 128-bit AES is more secure than TKIP. Was advanced for its time.

TKIP (Temporal Key Integrity Protocol): Protocol that mixes a root key with an initialization vector, a new key for each packet. Prevents replay attacks and protects against tampering.

WPA3 (Wi-Fi Protected Access 3) is the latest Wi-Fi security protocol that was introduced as a successor to WPA2. It was designed to address some of the vulnerabilities and weaknesses found in the previous Wi-Fi security standards. WPA3 provides improved security for Wi-Fi networks by implementing stronger encryption and authentication protocols.

2. **Authentication protocols:**

EAP (Extensible Authentication Protocol): Is an authentication framework that provides general guidance for authentication methods.

Protected Extensible Authentication Protocol (PEAP), is a security protocol used in wireless networks to authenticate users and provide encryption for network traffic. PEAP is designed to protect against various types of attacks, including man-in-the-middle attacks and credential theft.

EAP-FAST (EAP Flexible Authentication with Secure Tunneling): A Cisco-designed replacement for Lightweight EAP, supports certificates but are not required.

EAP-TLS (EAP Transport Layer Security): This is one of the most secure EAP standards and is widely implemented on many networks. It uses PKI, so certificates are required on the 802.1x server and on the clients.

EAP-TTLS (EAP Tunneled Transport Layer Security): Allows for systems to use older authentication methods such as PAP within a TLS tunnel. Certificate is required on the 802.1x server but not on the clients.

IEEE 802.1x: An authentication protocol used in VPNs, wired and wireless networks. In VPNs it is used as a RADIUS server, wired use it as a port-based authentication, and wireless use it in Enterprise mode. Can be used with certificate-based authentication.

RADIUS Federation: Members of one organization can authenticate to the network of another network using their normal credentials. Uses 802.1X as authentication method.

Z-Wave is a wireless communication protocol used in smart home devices. Z-Wave compatibility refers to the ability of devices to communicate with each other using the Z-Wave protocol. To ensure compatibility, Z-Wave devices must use the same frequency and comply with the Z-Wave standard.

ZigBee is a wireless communication protocol used in smart home devices. ZigBee configuration refers to the process of setting up and configuring ZigBee devices to communicate with each other. This involves configuring the devices with the appropriate settings and network information, such as the network ID, channel, and security settings.

3. **Methods:**

PSK vs. Enterprise

- **PSK** (Pre-Shared Key): Uses WPA2 encryption along with a key that everyone needs to know to access the network.
- **Enterprise**: Users to authenticate using a username and password, and uses 802.1X to provide authentication, server handles distribution of keys/certificates.

WPS: Allows users to easily configure a wireless network, often by using only a PIN. Are susceptible to brute force attacks because they can discover the PIN.

Captive portals: Forces clients using a web browser to complete a task before being able to access the network.

6.0 CRYPTOGRAPHY

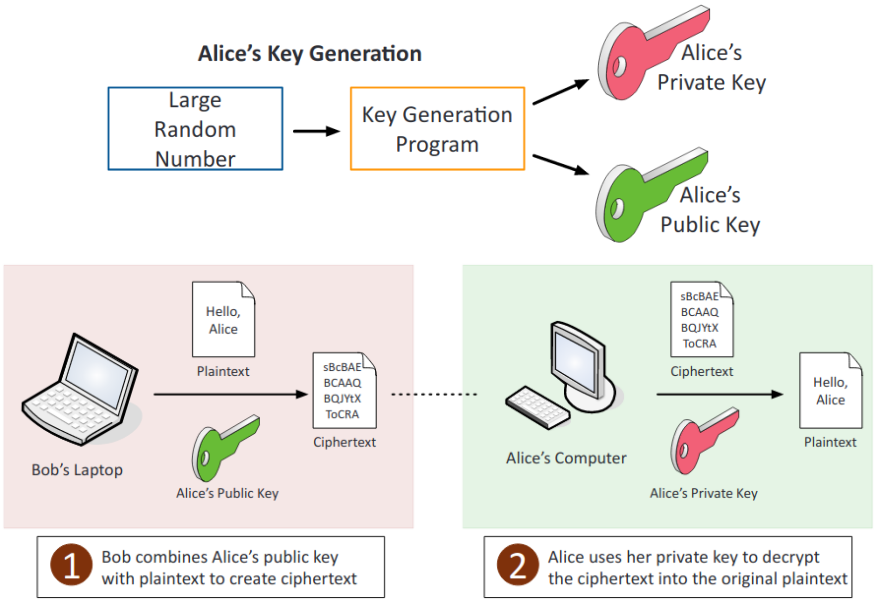
The greates vulnerability in any cryptographic implementation tends to be the key

Hashing services are cryptographic functions that generate a fixed-length, unique digital representation of data. This process involves passing the data through a hashing algorithm, which then produces a hash value or message digest that is typically a fixed size.

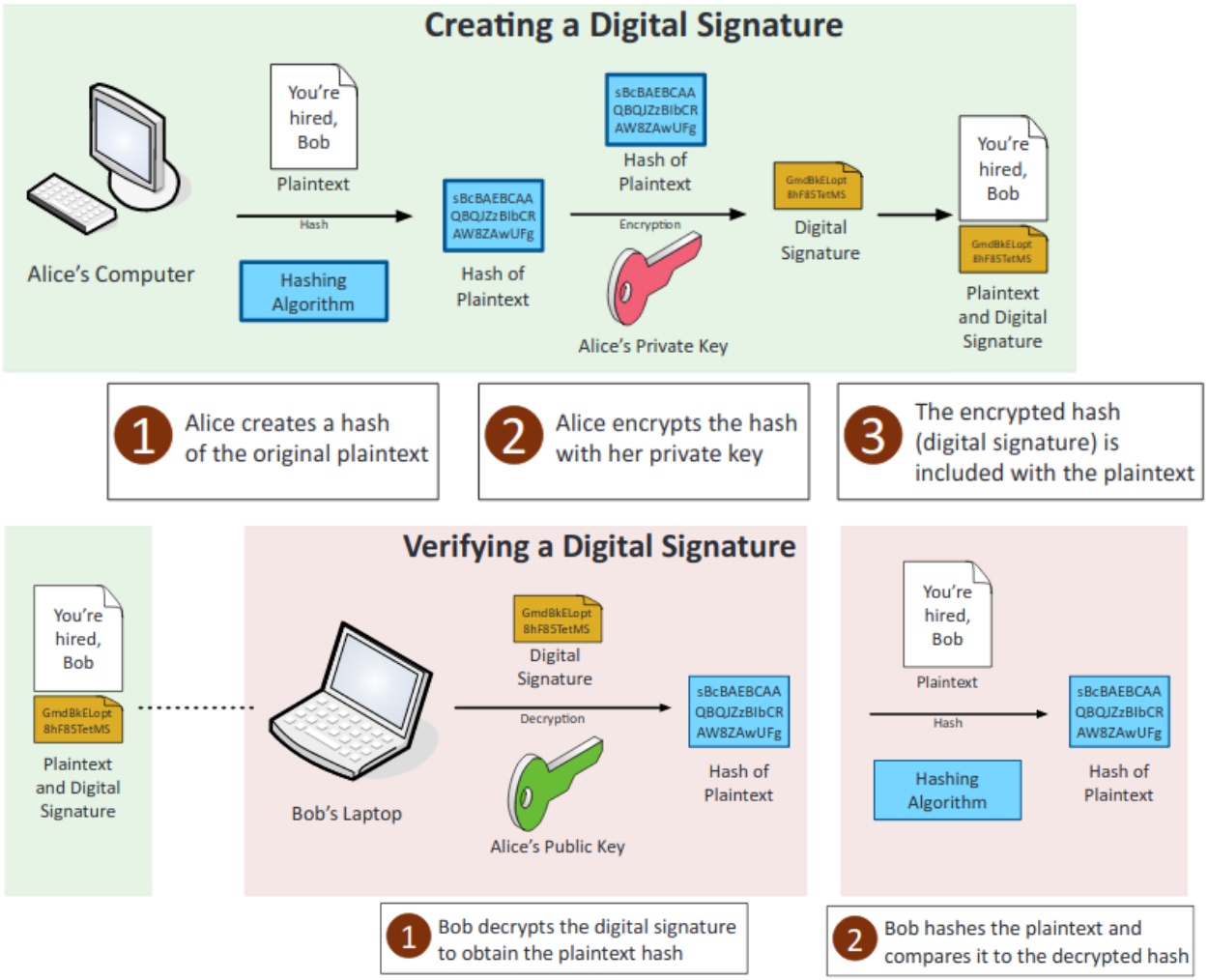
Ciphertext: An encrypted message.
Cipher: The algorithm used to encrypt or decrypt.
Hashing: An algorithm that creates a unique one-way encryption, not plaintext.
Key exchange is the process of securely exchanging cryptographic keys between two parties.

Both symmetric and asymmetric encryption have their uses and are important in modern security practices. Symmetric encryption is often used for encrypting large amounts of data quickly and efficiently, while asymmetric encryption is often used for secure communication between two parties without the need to exchange a secret key.

Symmetric algorithms: A shared secret key used by the sender and receiver to encrypt and decrypt.
Asymmetric algorithms: There is a shared public key and a private secret key. Public key encrypts and the private key decrypts, private key to sign and public key verify.



IV (Initialization Vector): A random value used with an encryption key.
Nonce: One-time use random value used for authentication.
Digital signatures: Provides integrity, authentication and non-repudiation, verifies that the original sender is actually the one who sent it. This can be done through asymmetric encryption, where there is a hash message then they will encrypt the hash using their private key, creating a digital signature that can only originate from them. To verify, the signature is decrypted with the public key, and the message is then hashed. If the two hashes match, then the digital signature is valid.



Diffusion: Changing one character causes the plaintext to drastically change the outputted cipher.

Confusion: The cipher doesn't look anything like the plain text.

Collision: Two completely different pieces of data have the exact same hash.

Steganography: Hides messages or code inside of an image or another type of data. Impossible to decipher without the correct tools.

Session keys: Symmetric keys used to provide a secure and fast online connection. The server's public key is paired with a random key to produce a symmetric key, that the server uses to encrypt and the user to decrypt.

Ephemeral key: A key that is generated for a single session or transaction and is then discarded. Ephemeral keys are used to provide forward secrecy and reduce the risk of data compromise if a long-term key is compromised.

Secret algorithm: Is a symmetric encryption. Uses the same key for the sender to encrypt and the receiver to decrypt.

Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without first decrypting it. This means that sensitive data can be kept encrypted even while being processed, reducing the risk of data breaches and improving privacy. Homomorphic encryption has applications in areas such as secure cloud computing, financial analysis, and machine learning, where privacy and security are paramount.

Data state:

- **Data-in-transit**: Data being transmitted over a network. Should be encrypted using TLS and IPSec.

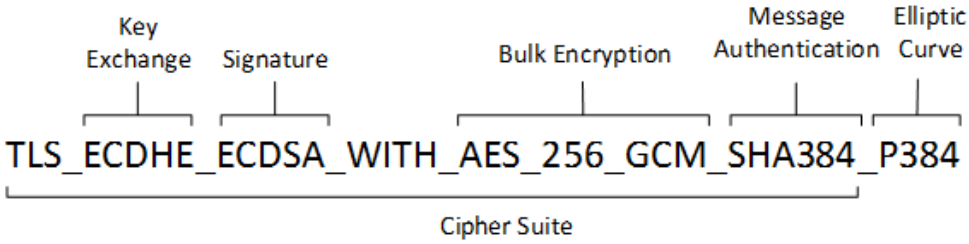
- **Data-at-rest**: Data in a storage device.
- **Data-in-use**: Data being ran through RAM or CPU, is almost always decrypted to make it easier to use.

Random/pseudo-random generation: Used to create random keys and salts, a computer is never truly random, so it relies on outside factors such as user input to create a more random number.

Perfect forward secrecy (PFS): Prevents point of failure where a stolen private key can decrypt all connections by generating a new key each session. Protects past sessions against future compromises of secret keys.

Security through obscurity: Relying on secrecy to protect and secure data.

Cipher suites: A set of information that helps determine how your web server will communicate secure data over HTTPS.



- **Key exchange algorithms**: Protect information required to create shared keys. They are asymmetric and perform well for relatively small amounts of data.
- **Signature**: The client checks the authenticity of the certificate being presented by running a series of checks.
- **Bulk encryption**: What will be used for the symmetric encryption that will occur during the HTTPS connection. (Block or Stream ciphers)
- **Message authentication**: Generate message hashes and signatures that ensure the integrity of a message.

Cryptography algorithms

Symmetric algorithms (marked green are the most secure):

AES (Advanced Encryption Standard): Symmetric, block cipher with 128-bit blocks, key sizes of 128-bit, 192-bit and 256-bit. It utilizes the Rijndael algorithm and is the U.S. government standard for the secure exchange of sensitive but unclassified data. It is also the encryption standard used today with WPA2.

DES (Data Encryption Standard): Symmetric, was common until replaced by AES, the block cipher is 64-bit and the key is 56-bit (very small), this means it can easily be brute forced.

3DES: Symmetric, very secure and upgrade over DES with three separate keys and three passes over data. Not used in modern day either.

RC4 (Rivest Cipher 4): Symmetric, part of the original WEP standard with SSL, removed from TLS, key sizes of 40-bit to 2048-bit. Deprecated from biased output.

Blowfish: Symmetric, fast and has variable key-lengths from 1-bit to 448-bits, uses 64-bit block cipher. Not limited by patents.

Twofish: Symmetric, uses a very complex key structure up to 256-bits but still similar to predecessor, works using 128-bit blocks. Again, not limited by patents.

Asymmetric algorithms

Rivest, Shamir, Adleman (RSA): First practical use of public key cryptography, uses large prime numbers as the basis for encryption. Encrypt/decrypt digital signatures.

DSA (Digital Signature Algorithm): A standard for digital signatures. Modifies Diffie-Hellman for use in digial signatures. Combines with elliptic curves to create **ECDSA**.

Diffie-Hellman: An asymmetric standard for exchanging keys. Primarily used to send private keys over public (unsecured) networks.

- **Groups**: Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.
- **DHE** (Diffie-Hellman Ephemeral): A Diffie-Hellman key exchange that uses different keys.
- **ECDHE** (Elliptic Curve Diffie-Hellman Ephemeral): Key agreement protocol that allows 2 parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. **They are both used for Perfect Foward Secrecy.**

Elliptic curve cryptography (ECC): Asymmetric, uses smaller key sizes and curve algorithms to secure data, useful in portable devices because it uses less CPU power. Used for encryption, digital signatures, pseudo-random generators and more. Great for low powered machines. Uses curves for encryption instead of large prime numbers.

PGP (Pretty Good Privacy): Asymmetric, used by many for emails and is used by IDEA algorithm. Owned by Symantec.

GPG (GNU Privacy Guard): A free, open-source version of PGP that provides equivalent encryption and authentication services.

Hashing algorithms

MD5 (Message-Digest Algorithm v5): Hashing algorithm, 128-bit hash with strong security, collision was found in 1996 so it is not used as much nowadays.

SHA (Secure Hash Algorithm): Hashing algorithm, one-way 160-bit hash value with encryption protocol. Standard hash algorithm today, went from SHA-1 (160-bit digest, deprecated) to SHA-2 (512-bit digest, still used). Developed by NSA.

HMAC (Hash-Based Message Authentication Code): Hashing algorithm that combines itself with a symmetric key. Provides data integrity as well as authenticity, but is faster than asymmetric encryption. Used in network encryption protocols.

Methods of encrypting data

Stream cipher is an encryption algorithm that encrypts data one bit or byte at a time, whereas a block cipher encrypts data in fixed-size blocks, typically 64 or 128 bits at a time. Stream ciphers are typically faster and more efficient for encrypting real-time communication, such as video or voice, because they encrypt data as it is being transmitted. However, they can be more susceptible to certain types of attacks, such as a known plaintext attack.

Block ciphers are generally considered more secure than stream ciphers because they are less susceptible to known plaintext attacks and provide stronger encryption of the data. However, they can be less efficient

than stream ciphers for real-time communication. Block ciphers are commonly used for encrypting data at rest, such as in databases or files.

- **CBC** (Cipher Block Chaining): Symmetric, uses IV for randomization. Encryption that is dependent on the block before it. Slow.
- **GCM** (Galois Counter Mode): Encryption with authentication as part of the block mode. Very efficient encryption and authentication. Used by many and commonly used in packetized data. Provides data authenticity/integrity, hashes as well. Widely used.
- **ECB** (Electronic Code Book): The simplest encryption mode, each block is encrypted with the same key, not recommended.
- **CTR** (Counter Mode): Converts block into stream, uses IV. Widely used.

Hash-based Message Authentication Code (HMAC) is a type of message authentication code (MAC) that involves the use of a cryptographic hash function in combination with a secret key. HMAC is used to verify both the integrity and authenticity of a message, ensuring that it has not been tampered with or altered in any way.

HMAC works by taking a message and a secret key as input, and then using a cryptographic hash function to produce a fixed-length output, or digest. This digest is then appended to the message, and the entire message is sent to the receiver. The receiver can then use the same cryptographic hash function and the same secret key to produce a digest of the received message. If the received digest matches the calculated digest, then the message is considered authentic and has not been altered.
HMAC is widely used in a variety of applications, including secure communications, message authentication, and digital signatures. It is considered to be a strong and reliable authentication mechanism, and is used in many security protocols and applications.
RIPEMD (RACE Integrity Primitives Evaluation Message Digest): Hashing algorithm that is based on MD4, collisions were found so it now exists in versions of 160-bits, 256-bits, and 320-bits.

Increasing hash security

Transport encryption

- HTTPS
- SSL/TLS
- S/MIME
- Ipsec

High data entropy refers to the unpredictability and randomness of data used as input to a cryptographic system. The higher the entropy, the more difficult it is for an attacker to guess the input data, thereby increasing the cryptographic security of the system.
Obfuscation: Taking something and making it difficult for a human to understand, however it is not impossible to convert it back to the original form.
Key stretching: Hashing a password, and then hashing that hashed value. Protects a weak password from brute force attacks.
Key strength: Larger keys and more bits are signs of better encryption and stronger keys.
Implementation vs. algorithm selection:

- **Crypto service provider**: A library of cryptographic standards and algorithms.
- **Crypto modules**: Hardware, firmware or software that provides the hash, HMAC, cipher, decipher, sign, and verify methods.
    - **Bcrypt**: Key Stretching that helps protect passwords by repeating Blowfish cipher.
    - **PBKDF2** (Password-Based Key Derivation Function 2): Key Stretching, applies RSA function to password to create stronger key.

Salt: The adding of input to random data to function to make it more complicated. A small piece of data added to the end of a password when creating a hash.

Modern cryptography requirements

- **Low power devices**: Smaller symmetric key sizes. Use of elliptic curve cryptography for asymmetric encryption. Mobile phones and portable devices.
- **Low latency**: Low amount of time occurs between input and output. Symmetric encryption and smaller key sizes.
- **High resiliency**: Larger key sizes and encryption algorithm quality.
- **Supporting confidentiality**: Secrecy and privacy. Encryption on file, drive or email level.
- **Supporting integrity**: Preventing modification of data and validating contents with hashes.
- **Supporting obfuscation**: Modern malware. Encrypted data hides the active malware code and decryption occurs during execution.
- **Supporting authentication**: Password hashing and protecting the original password.
- **Supporting non-repudiation**: Confirm the authenticity of data. Digital signature provides both integrity and non-reputdiation.
- **Resource vs. security constraints**: Limitations in providing strong cryptography due to the amount of available resources (time and energy) vs the security provided by cryptography.

7.0 PUBLIC KEY INFRASTRUCTURE (PKI)

Entities

Public Key Infrastructure (PKI) is a system of digital certificates, public key encryption, and other cryptographic protocols that enable secure communication over a network.

Public CA (Certificate Authority) is an organization that issues digital certificates for use in a PKI. It is a trusted third party that verifies the identity of a certificate holder and signs and issues the certificate.

Private CA is an internal CA that an organization uses to issue digital certificates within its own environment. It is not publicly trusted, and its certificates are only recognized by the organization.

Intermediate CA (Intermediate Certificate Authority): An entity that processes the CSR and verifies the authenticity of the user on behalf of a CA.
Recovery agent is a designated individual or entity that can perform a recovery of a user's private key in case it is lost, damaged or compromised. The recovery agent is responsible for verifying the user's identity and authenticating the request before providing access to the private key.

There are different levels of certificate authorities, including **root CAs, intermediate CAs, and issuing CAs**. Root CAs are at the top of the hierarchy and are responsible for signing and issuing intermediate CAs. Intermediate CAs, in turn, issue digital certificates to end entities. Issuing CAs are responsible for issuing certificates to individual users or devices.

Web of Trust - A decentralized trust model that addresses issues associated with the public authentication of public keys within a CA-based PKI system

- A peer-to-peer model
- Certificates are created as self-signed certificates
- Pretty Good Privacy (PGP) is a web of trust

Certificates specification

Components:

Certificate: Digitally signed statement that associates a public key to the corresponding private key.
Public key: A key that is provided by the sender, used by anyone to encrypt with asymmetric.
Private key: Key used to decrypt a message, only used by the person opening the message.
Object identifiers (OID): A serial number that authenticates a certificate.

Concepts:

Online vs. offline CA:

Online CA: Is directly connected to a network, most common.
Offline CA: Is not directly connected to a network, often used for root certificates.

Stapling: Combining related items in order to reduce communication steps. The device that holds the certificate will also be the one to provide status of any revocation.

OCSP Stapling - Allows the certificate holder to get the OCSP record from the server at regular intervals and include it as part of the SSL or TLS handshake

The Online Certificate Status Protocol (OCSP) is a protocol used to check the status of a digital certificate in real-time. When a digital certificate is presented for authentication, the OCSP client sends a request to the OCSP server to verify the status of the certificate. The server responds with the current status of the certificate, allowing the client to make an informed decision about whether to accept or reject the certificate.

Pinning: The application has hard-coded the server's certificate into the application itself.

Public Key Pinning - Allows an HTTPS website to resist impersonation attacks by presenting a set of trusted public keys to the user's web browser as part of the HTTP header

Trust model: A complex structure of: systems, personnel, applications, protocols, technologies, and policies working together to provide protection.

Key escrow: A process in which a copy of an encryption key is securely stored by a third party, who can then retrieve the key if necessary. This is often used in situations where data needs to be recovered, even if the original key owner is unavailable.

Certificate chaining: Certificates are handled by a chain of trust, the trust anchor for the digital cert is the root CA.

Types of certificates:

Wildcard: A Certificate that can be used with multiple subdomains of a given domain, by covering the all subordinate certificates to the root.

SAN (Subject Alternative Name): The certificate has several uses, allows a certificate to be valid for multiple domains using multiple names.

Code signing: Digitally signs written application code and makes sure that it adheres to policy restriction and usage.

Self-signed: The root CA creates its own certificate.

Machine/computer: Certificates that are assigned to a specific machine.

Email: Secures emails, is used by S/MIME.

User: Often for authentication or to access resources.

Root: Used for root authorities, they usually are self-signed.

Domain validation: Provides a secure communication with a specific domain and provides TLS, this is the most common form of certificate.

Extended validation: Are more secure because they require more validation from the certification holder.

Formats of certificates

1. **X.509:** This is the most widely used format for digital certificates, including CA certificates. It is a standard defined by the International Telecommunication Union (ITU) and widely adopted by the industry. X.509 certificates include a range of information about the certificate holder, such as the public key, validity period, issuer information, and digital signature.
2. **PKCS#7**: This is a format defined by the Public-Key Cryptography Standards (PKCS) developed by RSA Security. It is a binary format used to bundle one or more X.509 certificates and their associated private keys into a single file. PKCS#7 is often used for secure email and document signing.

Extensions of files

DER (Distinguished Encoding Rules): Are common and designed for X.509 certificates, they are used to extend binary encoded certificates. Cannot be edited by a plain text editor. Used with Java commonly.

PEM (Privacy Enhanced Mail): Most common format in which certificates are issued. Multiple certificates and the private key can be included in one file. The file is encoded ASCII. PEM file extensions include .pem, .crt, .cer, and .key. Apache servers typically use PEM-format files.

PFX: A precursor to P12, has the same usage. Administrators often use this to format on Windows to import and export certificates.

CER (Certificate File): May be encoded as binary DER or as ASCII PEM.

P12: Is a PFX extension used in windows.

PKCS #12 (Public Key Cryptography Standards #12): Is part of the RFC standard. Stores many types of certificates and can be password protected.

RFC (Remote Function Call): A formal document describes the specifications for a particular technology, was drafted by the Internet Engineering Task Force.

P7B: Is stored in Base64 ASCII, containing certificates and chains but not the private key.

Responsibilites of CA

1. Verification of identity: A CA is responsible for verifying the identity of the person or organization requesting a digital certificate.
2. Issuance of certificates: Once the identity has been verified, the CA issues a digital certificate containing the public key of the certificate holder along with other information.
3. Revocation of certificates: If a certificate has been compromised or is no longer valid, the CA revokes the certificate and publishes a Certificate Revocation List (CRL) containing the revoked certificates.
4. Management of certificate status: The Online Certificate Status Protocol (OCSP) is used to verify the status of a digital certificate in real-time. A CA must ensure that OCSP servers are available to provide certificate status information when required.
5. Renewal of certificates: Digital certificates have a finite lifespan and must be renewed periodically. The CA is responsible for managing the renewal process.
6. Key escrow: In some cases, a CA may be responsible for securely storing private keys associated with digital certificates.
7. Compliance with policies and regulations: A CA must comply with industry standards, policies, and regulations to ensure the security and integrity of the digital certificates it issues.

Actions

A Certificate Signing Request (CSR) is a request for a digital certificate that is sent to a CA. The CSR includes information about the identity of the certificate holder, along with the public key that will be included in the digital certificate. The CA uses the information in the CSR to verify the identity of the certificate holder before issuing a digital certificate.

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by a CA before their expiration date. The CRL is published by the CA and is used by certificate holders to check the validity of a digital certificate.

Registration refers to the process of requesting and obtaining a digital certificate from a certificate authority. The registration process typically involves the submission of a certificate signing request (CSR) which contains the public key and other identifying information of the requesting entity. The certificate authority verifies the information and issues a digital certificate that binds the public key to the identity of the requester.

8.0 UNASSIGNED

Content Management System (CMS) is a software application that allows users to create, manage, and publish digital content, typically on websites, without requiring specialized technical knowledge.

Border Gateway Protocol (BGP) is a routing protocol used in large-scale networks, such as the Internet. BGP is used to exchange routing information between different autonomous systems (ASes) and is essential for enabling the global reachability of the Internet.

Network interface card teaming (NIC teaming) is a technology used to combine multiple network interface cards into a single logical interface. This provides increased bandwidth and redundancy, as well as improved load balancing and failover capabilities.