**1.0 Threats, Attacks, and Vulnerabilities (24%)**

**Information Security** - Act of protecting data and information from unauthorised access, unlawful modification and disruption, disclosure, corruption, and destruction - **protecting the DATA**

**Information Systems Security** - Act of protecting the systems that hold and process our critical data - **protecting the SYSTEMS**

**CIA Triad - Confidentiality, Integrity, Availability**

**Confidentiality - (encryption)** information has not been disclosed to unauthorised people

**Integrity - (hashing)** information has not been modified or altered without proper authorisation

**Availability - (redundancy)** information is able to be stored, accessed, and protected at all times

**1.1 Compare and contrast different types of social engineering techniques.**

**• Phishing**

Attempt to fraudulently obtain information from a user, mainly **email**. Works really well lol.

**• Spear phishing**

Targeted phishing using data that is specific to you.

**• Whaling**

Spear phishing against high-value targets e.g. CEO, CISO, CFO etc.

**• Smishing**

Phishing via SMS ‘royal mail missing parcel’ etc. - can either take your details for credit card fraud, or to further target you with vishing or spear-phishing, or to install malware.

**• Vishing**

Phishing via phone calls (voice phishing).

**• Spam**

Abuses electronic messaging, often to advertise. Spammers often exploit a company’s **open mail relays** to send their messages. 2003 CAN-SPAM Act, you could get investigated by FTC.

**• Spam over instant messaging (SPIM) (IM Spam)**

Facebook chat, game chat room etc.

**• Dumpster diving**

Looking for discarded information in waste containers.

**• Shoulder surfing**

Literally looking over someone’s shoulder to find out information, direct observation.

**• Eavesdropping**

Listening in on conversations.

**• Baiting**

Leave behind a USB, CD etc. to get people to put it into their machine.

**• Pharming**

Occurs when an attacker redirects one website’s traffic to another website that is bogus or malicious.

**• Tailgating/piggybacking**

Follow someone into a secure area, ‘hold the door for me I forgot my card’

**• Eliciting information**

Having a regular conversation but have them divulge important information.

**• Prepending**

Trick users into entering their username and passwords by adding an invisible string before the weblink URL they click. The prepended string (**e.g. data:text**) converts the link into a Data URI (or Data URL) that embeds small files inline of documents.

**• Identity fraud**

If they can take over your phone number they can take over all your accounts that use that phone number for 2FA. You can get around this by either never posting your phone number and using a call forwarding service like Google Voice, or using a 2FA app like Okta or Google Authenticator which does not use the phone number.

**• Invoice scams**

A scam in which a person is tricked into paying for a fake invoice for a product or service that they did not order.

**• Credential harvesting**

Simply means getting hold of users’ credentials - usernames and passwords.

**• Reconnaissance**

Finding out information before an attempted attack.

**• Hoax**

Social engineering trick, make them believe something true that is false and vice versa e.g. pretends you have a virus so you call them up to lose money/buy their product/install their adware etc.

**• Impersonation**

**Identity** **theft** where you pretend to be someone else.

**• Diversion Theft**

Redirecting a package to intercept it.

**• Watering hole attack**

Takes advantage of people’s habits, malware targets websites that people go to all the time e.g. websites that you use all the time for work, Facebook/Google etc.

**• Typosquatting**

Slightly different spelled domain that takes advantage of people not reading every character precisely of a url. Used in watering hole attacks.

**• Pretexting**

Method of inventing a scenario to convince victims to divulge information they should not divulge.

**• Influence campaigns aka influence operations**

Collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent - take information and use it against someone.

**- Hybrid warfare**

Military strategy which employs political warfare and blends conventional warfare, irregular warfare, and cyberwarfare with other influencing methods such as fake news, diplomacy, and foreign electoral intervention.

**- Social media**

‘Changing the narrative’ around how people think and act e.g. Russians 2016 US elections.

**• Principles (reasons for effectiveness)**

**- Authority**

People are more willing to comply if they think it is coming from someone in authority e.g. a boss, a client, the government, the police. Recognisable brand names e.g. your bank.

**- Intimidation**

Threats or demands to intimidate someone.

**- Scarcity**

FOMO e.g. limited stock offers, only 3 left.

**- Familiarity**

**- Likeability**

Social engineers are very likeable, attempt to find common ground and shared interests with their target. Friendly, attractive.

**- Trust**

Relates to many of the others e.g. authority, familiarity, consensus

**- Social Proof**

**- Consensus**

People are more likely to click on a link if others have seen it and clicked on it e.g. your friends, other internet users.

**- Urgency**

Everyone is in a rush, take advantage of that. Bypass processes. If you feel pressure, its urgency.

**1.2 Given a scenario, analyze potential indicators to determine the type of attack.**

**• Malware**

Malicious Software designed to infiltrate a computer system and possibly change it without the user’s knowledge or consent

**- Virus**

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

**- Boot sector Virus**

Stored in the first sector of a hard drive and loaded up into memory upon boot up

**- Macros Virus**

Virus embedded into a document and is executed when the document is opened by the user e.g. excel, word, powerpoint

**- Program Virus**

Infects an executable or application

**- Multipartite Virus**

Virus that combines boot and program viruses to first attach to the boot sector and system files before attacking other files on the computer

**- Encrypted Virus**

Encrypted to avoid detection by antivirus software

**- Polymorphic Virus**

Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection

**- Metamorphic Virus**

Advanced version of a polymorphic virus, can rewrite itself entirely before it attempts to infect a file

**- Stealth Virus**

Category of virus that protects itself (encryption, polymorphic, metamorphic)

**- Armored Virus**

Virus with a layer of protection to confuse a person or program analysing it

**- Hoax Virus**

Social engineering trick, pretends you have a virus so you call them up to lose money/buy their product/install their adware etc.

**- Ransomware**

Uses a vulnerability in your software to access your system, takes control of your computer or encrypts files until ransom is received.

**- Trojans**

Disguised as a piece of harmless or desirable software. Performs desired functions as well as malicious ones.

**- Remote access Trojan (RAT)**

Most commonly used type of trojan. Provides the attacker with remote control of a victim’s computer.

**- Worms**

Like a virus, **but is able to self-replicate and spread without user action** e.g. can hunt for a vulnerability across the network/internet and exploit every instance of that vulnerability. Worms can cause disruption to normal network traffic and computing activities. **Spreading and replicating fast, using CPU, memory, bandwidth etc.** Can spread far and wide over the internet.

**Dropper or downloader**, stage 1 dropper - malware designed to install or run other types of malware embedded in a payload on an infected host. Drops a very small piece of shell code onto a machine that then downloads the rest of the code from a remote system.

**Downloader** - a piece of code that connects to the internet to retrieve additional tools after the initial infection by a dropper

**Shellcode** - any lightweight code that is designed to run an exploit on the target, which may include any type of code format from scripting languages to binary code

**Maintain access** - dropper downloads e.g. RAT and gives attacker C2 over the machine.

**Strengthen access** - infect other systems, find higher value targets, lateral movement, privilege escalation

**Actions on objectives** - copying, stealing files, encrypting files etc.

**Concealment** - cover their own tracks, deleting logs etc.

**- Potentially unwanted programs (PUPs)**

Companies often bundle a wanted program download with a wrapper application and may offer to install an unwanted application, and in some cases without providing a clear opt-out method. E.g. when you install a web browser and it comes bundled with the Ask Jeeves search bar.

**- Fileless virus**

Malware is executed as a script or small piece of shell code that creates a process in system memory, or temporarily creates a file that runs and then deletes itself. To avoid detection by signature-based security software that looks at the file system i.e. NOT creating virus.exe and running that constantly - old style. Also called a **dropper** or downloader.

**- Command and control C2**

Server controlled by an attacker that can send commands remotely to infected machines

**- Bots / botnet / zombie computers**

A collection of compromised computers under the control of a master node (Command & Control C2 Server). Good for anything requiring a lot of processing power. Can attack victims through zombie computers so it looks as though the zombie is committing the attack, commit DDoS attacks, or run cryptomining software.

**- Crypto-malware/cryptominer**

Common use of a **botnet** - mines cryptocurrency using the infected machine’s resources.

**- Cryptojacking**

Uses JavaScript to mine crypto so long as the infected webpage is kept open, if the webpage is closed, the browser returns to normal.

**- Backdoor**

Used to bypass normal security and authentication functions. Remote Access Trojan RAT acts like a backdoor to maintain persistent access.

**- Logic bombs**

Malicious code that has been inserted inside a program and will execute only when certain conditions have been met e.g. certain datetime (time bomb), when an employee gets fired

**- Easter Egg**

Harmless secret joke code, issue is that the code is often not tested for security as only a couple of people know about it

**- Spyware**

Gathers information about the user without their consent.

**- Adware**

Gathers data on you to target ads with the ad commissions being sent to the attacker.

**- Keyloggers**

Captures keystrokes and/or screenshots and sends them to the attacker.

**- Rootkit**

Designed to gain administrative level control over a system without detection. Ring 0 (kernel all hardware/software operations permitted) or ring 1 (admin) level-permissions. Can be embedded extremely deeply so even the operating system cannot possibly detect it. Often the only way to find them is to boot into the machine with an external device and scan it.

**- Grayware/Jokeware**

Neither benign nor malicious and tends to behave improperly without serious consequences. Sort of gimmicky joke things that annoy you.

**• Password attacks**

**- Spraying**

Trying the **same password on different usernames** (this can avoid lockouts on the same account)

**- Dictionary**

Trying the **most common passwords from a dictionary** of passwords

**- Credential Stuffing**

Trying the **same credentials on different websites** e.g. after data breach, and people reuse passwords across different sites. Prevent by not reusing passwords.

**- Brute force**

**-- Offline**

Trying to crack the hashes offline (e.g. using rainbow tables)

**-- Online**

Trying multiple passwords in the online form - can be blocked with timeouts (number/rate of logins e.g. block after 3 fails) and by looking at the logs to see what is occurring.

**- Rainbow table**

**Dictionary of existing pre-computed hashes**, prevent with: salted hash

**- Plaintext/unencrypted**

Passwords used that were stored unencrypted or stolen from browser cookies.

**- Broken authentication**

E.g. weak password credentials, weak password reset methods (e.g. what is your birthday, where were you born), credential exposure - poor coding exposes credentials, session hijacking - poor coding.

**- Rubber Hose Attack**

Threat or use of violence against the person who knows the password.

**• Physical attacks**

**- Malicious Universal Serial Bus (USB) cable**

USB cable with malware in it.

**- Malicious flash drive**

Dropped somewhere nearby e.g. the car park with the hope that an employee will plug it into their computer.

**- Card cloning / Skimming**

Making an unauthorised copy of a credit card.

**• Adversarial artificial intelligence (AI)**

Machine learning is a component of AI that develops strategies for solving tasks after being **given a training set.** **The human** **determines** factors and the **machine** **classifies factors.**

Deep learning = ML without explicit instructions. **The machine determines and classifies factors.** UsesArtificial Neural Network (ANN) - algorithmic design that functions like a brain to understand the world.

**- Tainted training data for machine learning (ML)**

Only as good as the data you feed it, garbage in, garbage out (racist parties).

**- Security of machine learning algorithms**

**• Supply-chain attacks**

Device compromised via supply chain e.g. hardware tampered with in factory/en route, or third-party software updates hijacked with malware

**• Cloud-based vs. on-premises attacks**

**• Cryptographic attacks**

**- Birthday**

Technique used by an attacker to find two different messages that have the same identical hash digest.

**- Collision**

Two different inputs provide hashes that match, but shouldn’t.

**- Downgrade**

Attack on SSL/TLS where a protocol is tricked into using a lower quality version of itself instead of a higher quality version e.g. TLS 1.0 instead of TLS 1.3. Can configure a web server to not support downgrades.

**• Living Off the Land**

Exploit technique that uses standard system tools and packages to perform intrusions. Much more difficult to detect.

**1.3 Given a scenario, analyze potential indicators associated with application attacks.**

**• Active Interception**

Occurs when a computer is placed between the sender and receiver and is able to capture or modify the traffic between them

**• Privilege escalation**

Occurs when attacker can exploit a design flaw or bug in a system to gain access to a resource that a normal user is not able to access, get admin/root access

**• Cross-site scripting**

Attacker embeds malicious scripting commands on a trusted website. The victim is the user, not the web server.

**Stored/Persistent** - attempts to get data provided by the attacker to be saved on the web server by the victim, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing.

**Reflected** - attempts to have a non-persistent effect activated by a victim clicking a link on the site.

**DOM-based (client-side attack)** - attempts to exploit the victim’s web browser.

**Prevent with:** output encoding and proper input validation

**• Injections**

**- Code Injection**

The exploitation of a computer bug that is caused by processing invalid data without **input validation**. The injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution.

**- Structured query language (SQL)**

Attack consisting of the insertion or injection of an SQL query via input data from the client to a web app. **Prevent with: input validation** and least privilege. **On the exam = `OR 1=1; or anything else that always returns True.**

**- Dynamic-link library (DLL)**

Rootkits use this. Malicious code inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime.

**- Lightweight Directory Access Protocol (LDAP)**

**- Extensible Markup Language (XML) - injection, vulnerabilities, exploitation**

XML data submitted without encryption or **input validation** is vulnerable to spoofing, request forgery, and injection of arbitrary code.

**XML Bomb (Billion Laughs Attack)** - XML encodes entities that expand to exponential sizes, consuming memory on the host and potentially crashing it. Type of DoS attack.

**XML External Entity (XXE)** - attack that embeds a request for a local resource (like a file).

XML can name the tags whatever you want, unlike HTML. **On the exam for the close tag /> syntax.**

**• Pointer/object dereference**

Software vulnerability that occurs when the code attempts to remove the relationship between a pointer and the thing it points to.

**• Directory traversal**

Method of accessing unauthorised directories by moving through the directory structure on a remote server = **../../../../ on the exam.**

**• Arbitrary Code Execution / Remote Code Execution**

Arbitrary is where an attacker can run code on a victim’s computer (could be in real life), remote is a subset where the attacker is in a remote location.

**• Buffer overflows**

When a process stores data outside the memory range allocated by the developer. Attacker puts more memory into a buffer than it is designed to hold. Trying to overwrite the return pointer to point to malicious code.

Buffer - temporary storage area to store data.

85% of data breaches are caused by buffer overflows as the initial attack vector.

Stack - reserved area of memory where the program saves the return address when a function call instruction is received.

**Smash the Stack** - occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attacker’s code to run - **‘NOP Slide’**

**Address Space Layout Randomisation (ASLR)** - method used by programmers to randomly arrange the different address spaces used by a program or process to prevent buffer overflow exploits.

**• Race conditions**

Software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those **events fail to execute in the order and timing intended** by the developer. Computer is trying to race itself. Threads trying to write a location at the same time. Difficult to detect - 2016 ‘Dirty Cow (copy on write)’ local privilege escalation bug - didn’t leave anything in logs. Can also be used against databases and file systems.

**Prevent with:**

Develop apps to **not process things sequentially** if possible - parallel processing

**Locking mechanism** to provide app with exclusive access e.g. when you buy a ticket it reserves it for a few min. Also works with shared use of databases/cloud apps.

**- Time of check to time of use (TOCTTOU)**

Potential vulnerability that occurs when there is a change between when an app checked a resource and when the app used the resource e.g. eCommerce store checks the items when you pay, not just when you put them in your cart.

**• Error handling**

**• Improper input handling**

**• Replay attack**

Network-based attack where a valid data transmission is maliciously rebroadcast, repeated, or delayed. Works well with authenticating with WAPs. Prevent with: MFA

**- Session replays**

**• Integer overflow**

**• Request forgeries**

**- Server-side**

**- Cross-site (XSRF / CSRF)**

When an attacker forces a user to execute actions on a web server for which they are already authenticated e.g. you login to a bank, then code is executed.

**Prevent with:** captchas, tokens, encryption, XML file scanning, cookie verification.

**• Application programming interface (API) attacks**

**• Resource exhaustion**

**• Memory leak**

**• Secure Sockets Layer (SSL) stripping**

**• Driver manipulation**

Rootkits use this. Attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level.

**- Shimming**

Piece of software that is placed between two components to intercept calls and redirect them e.g. between DLL and Windows OS - this is how Windows Compatibility Mode works and can be used to attack.

**- Refactoring**

Changes the code every time the malware is downloaded - either add and remove code, or reorder, rewrite how the code works, means that virus signatures and hashes will not work as well.

**• Pass the hash**

Technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LM hash instead of requiring the associated plaintext password. **Hash is functionally equivalent to the underlying password.** Difficult to defend against. Only use trusted OS - patch/update workstations, use MFA, use least privilege.

Mimikatz - penetration testing tool used to automate the harvesting of hashes and perform the attack,

**1.4 Given a scenario, analyze potential indicators associated with network attacks.**

**• Wireless**

**- Evil twin**

Rogue, counterfeit WAP with the same SSID as your valid one.

**- Rogue access point**

Unauthorised WAP or wireless router on your network, decreases security. Prevent with: MAC filtering, NAC.

**- Bluesnarfing**

**Taking data.** Unauthorised access of information from a wireless device over a Bluetooth detection.

**- Bluejacking**

**Send (unwanted) data.** Sending of unsolicited messages to Bluetooth enabled devices e.g. if your car is in pairing mode, someone else could pair, or if your phone is in discover mode someone could drop random texts/images onto your phone (AirDrop on iPhone)

Don’t use the default pairing key (e.g. 0000). Turn off when not needed.

**- Disassociation**

Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects

**- Jamming**

Intentional radio frequency interference targeting your wireless network to cause a DoS.

**- Radio frequency identification (RFID)**

Devices use a radio frequency signal to transmit identifying information about the device or token holder e.g. ID cards - **10cm to 200m depending on device**, eavesdropping possible.

**- Near-field communication (NFC)**

Allows two devices to transmit information when they are within close range **4cm** through automated pairing and transmission e.g. Apple Pay

**- Initialization vector (IV)**

WEP has 24-bit IV and is easy to crack

**• Hijacking**

Exploitation of a computer session in an attempt to gain unauthorised access to data, services, or other resources on a computer or server

**Session theft -** attacker guesses the session ID for a web session, enabling them to takeover the already authorised session of the client

**Clickjacking -** uses multiple transparent layers to click a user into clicking on a button or link on a page when they were meaning to click on the actual page

**TCP/IP Hijacking** attacker takes over a TCP session between two computers without the need of a cookie or other host access - only authenticate at the beginning handshake

**Blind hijacking -** attacker blindly injects data into the communication stream without being able to see if it is successful or not

**• On-path attack (previously known as man-in-the-middle attack/man-in-the-browser attack)**

Attack that causes data to flow through the attacker’s computer where they can intercept or manipulate the data

**Browser** - trojan infects a vulnerable web browser and modifies web pages and transactions being done only in the browser. Intercepts API calls between the browser process and its DLLs.

**• Layer 2 attacks**

**- Media access control (MAC) flooding**

Attempt to overwhelm the limited switch memory set aside to store the MAC addresses for each port. Content Addressable Memory (CAM Table) - switches can **fail-open** when flooded and begin to act like a hub.

**- MAC spoofing / cloning**

Occurs when an attacker masks their own MAC address to pretend they have the MAC address of another device. Can overcome MAC filtering rules. Prevent with: authentication.

**- Address Resolution Protocol (ARP) poisoning**

**ARP** - protocol for mapping an IP address to a MAC address that is recognised in the local network - **‘DNS for MAC addresses’**

**Poisoning** - diverting traffic from the originally intended host to the attack instead by altering the ARP table, combined with MAC spoofing.

Prevent with: VLAN segmentation, DHCP snooping, limit static MAC addresses accepted, limit duration of ARP entry on hosts, conduct ARP inspection

**- Physical tampering**

Attackers can physically attack the **management port** of the switch by plugging their computer in. Switch be physically locked away.

**• Domain name system (DNS)**

**- Domain hijacking**

**- DNS poisoning**

Occurs when the name resolution information is modified in the DNS server’s cache. Redirects clients to malicious sites. Often occurs on internal DNS servers after an attack has gained access.

**- Uniform Resource Locator (URL) redirection**

**- Domain reputation**

**- Altered hosts file**

When an attacker modifies the host file on the individual machine itself to have the client bypass the DNS server and redirects them to a malicious website. Set host file to read-only.

**- Unauthorized zone transfer**

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

**- Domain name kiting**

Attack that exploits a process in the way a domain name is registered so that the domain name is kept in limbo and cannot be registered by an authenticated buyer - you have a 5 day window to register it, but you can delete and readd and the 5 days starts again.

**• Denial-of-service (DoS)**

**Flood Attacks** - attempts to send more packers to a single server or host than it can handle.

**Ping Flood -** attempts to flood the server by sending too many ICMP echo request packets (pings) - many organisations block pings

**Smurf Attack -** attacker sends a ping to subnet broadcast address and devices reply to a spoofed IP (victim’s server) using up bandwidth and processing power. Send ping with spoofed IP of victim’s server to subnet broadcast address, this will mean every device on the network will echo reply to that spoofed IP, causing a huge amount of traffic - amplifies an attack.

**Fraggle Attack -** attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets (older attacker, probably blocked)

**UDP Flood -** similar to Fraggle attack but uses different ports

**SYN Flood** - attacker initiates multiple TCP sessions with spoofed IPs but never completes the 3-way handshake. Send SYN requests with spoofed IPs to server, server will then send SYN ACK to spoofed IPs but these spoofed IPs won’t respond, as they were not expecting anything, so these open, incomplete TCP 3-way handshakes will use up server resources. Prevent with: flood guards (blocks request at network boundary), time outs (if incomplete about 10-30s), and IPS (can respond and stop).

**XMAS Attack** - sets the FIN, PSH, and URG flags to true inside a TCP packet, causes device to crash or reboot as packet in non-standard format. Many modern routers will drop these packets.

**Ping of Death -** sends an oversized and malformed ping packet. One of the first DoS’s. Modern routers will ignore this.

**Teardrop Attack -** breaks apart packets into IP fragments, modifies them with overlapping and oversized payloads, and sends them to a victim machine. Enough teardrops form a puddle.

**Permanent DoS PDoS -** exploits a security flaw to permanently break a networking device by reflashing its firmware, rebooting does not fix.

**Fork Bomb -** creates a large number of processes to use up the available processing power of a computer. Expands inside the cache of the processor of the server being attacked.

**On the exam -** any attack that means a server cannot provide to its users, is a DoS.

**• Distributed denial-of-service (DDoS)**

**Botnet** - many machines target a single victim and attack at the exact same time. Send requests to overwhelm the victim machine and disrupt/degrade its service.

**DNS Amplification attack -** attack which relies on the large amount of DNS information that is sent in response to a spoofed query on behalf of the victim server - small packet to send request for information, a lot of data is returned (50x more)

**Stopping a DDoS**: DNS sinkhole, IPS, cloud providers e.g. CloudFlare that does the elastic cloud scaling for you.

**- Network**

**- Application**

**- Operational technology (OT)**

**• Malicious code or script execution**

**- PowerShell**

**- Python**

**- Bash**

**- Macros**

Can disable macros in Office to prevent viruses.

**- Visual Basic for Applications (VBA)**

**1.5 Explain different threat actors, vectors, and intelligence sources.**

**• Actors and threats**

**- Advanced persistent threat (APT)**

Highly-trained and well-funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal. Very quiet and sneaky inside a network.

**- Insider threats**

Employees - malicious, incompetent, accidents

**- State actors**

Intelligence agencies - CIA/NSA, GCHQ, Mossad/Unit 8200 (Israel), FAPSI/FSB/SVR/GRU (Russia), PLA/MSS (China), RGB/MSS (North Korea), MIS (Iran)

**- Hacktivists**

Driven by a cause, social change, political agendas, terrorism e.g. Anonymous

**- Script kiddies**

Opposite of elite - they just use programs and tools that other people create. ‘Baby hackers’.

**- Criminal syndicates aka organised crime**

Well-funded and highly sophisticated, mainly for financial gain

**- Hackers**

**Elite -** hackers who find and exploit vulnerabilities before anyone else does. They create the tools that are being used by everyone else (1 in 10,000 are elite). Either white hat elite or black hat elite - refers to skill level not their allegiance.

**-- Authorized**

**White Hat (ethical hacker, penetration tester)** - non-malicious hackers who attempt to break into a company’s systems at their request

**-- Unauthorized**

**Black Hat -** malicious hackers who try to break into computer systems and networks without authorisation or permission

**Grey Hat -** no affiliation to a company, attempts to break into a network but risks the law by doing so. May just be doing it for the sake of it, motives less clear, neither malicious nor non-malicious. May tell the company what they did so they can improve their security.

**-- Semi-authorized**

**Blue Hat -** attempting to hack into a company’s network but not employed by that company. **‘Bug bounty’** **programs.**

**- Shadow IT**

**- Competitors**

**• Attributes of actors**

**- Internal/external**

**- Level of sophistication/capability**

Script kiddie -> hacktivist -> organised crime -> APT

**- Resources/funding**

**- Intent/motivation**

**• Threat Vectors**

Method used by an attacker to access a victim’s machine. How we get to the machine itself.

**Attack vector -** method used by an attacker to gain access to a victim’s machine in order to infect it with malware. How we get to the machine AND how we’re going to infect it.

**- Direct access**

**- Wireless**

Wired is always more secure than wireless as it has a significantly smaller attack surface with less attack vectors.

**- Email**

**- Supply chain**

**- Social media**

**- Removable media**

CD, USB Stick - left lying around infected with malware

Removal Media Controls - inside group policies on Windows - deny read access from USBs to prevent malware being uploaded, or deny write access to CDs so data cannot be exfiltrated.

**- Cloud**

**• Threat intelligence sources**

**Timeliness** - property of an intelligence source that ensures it is up to date - intelligence expires

**Relevancy -** property of an intelligence source that ensures it matches the use cases intended for it e.g. we don’t care about vulnerabilities for tech I don’t use - what affects me and my organisation?

**Accuracy -** property of an intelligence source that ensures it produces effective results - needs to be true, remove false positives

**Confidence levels -** property of an intelligence source that ensures it produces qualified statements about reliability

**NATO Admiralty Scale -** for assessing reliability of threat intelligence (e.g. used by MISP)

**Source Reliability - A - Reliable**, no doubt of authenticity, trustworthiness, or competence, **B - Usually Reliable**, minor doubt, **C - Fairly Reliable**, doubt, **D - Not Usually Reliable**, significant doubt but had provided reliable information in the past, **E - Unreliable**, lacking, history of invalid information, **F - Cannot be Judged**, no basis for evaluating yet

**Information Content - 1 - Confirmed**, confirmed by other sources, logical in itself, consistent with other information, **2 - Probably True**, not confirmed, logical, consistent, **3 - Possibly True,** not confirmed, reasonably logical, agrees with some other information, **4 - Doubtfully True,** not confirmed, not logical, no other information to compare to, **5 - Improbable**, not confirmed, not logical, contradicted by other information **6 - Cannot be Judged,** no basis for evaluating yet

**Explicit vs Implicit knowledge** - threat intelligence is explicit, cyber-security professionals have implicit knowledge when they know ‘something is wrong’

**- Open-source intelligence (OSINT)**

Methods of obtaining information about a person or organisation through public records, websites, and social media

Data available without a subscription, may include threat feeds similar to the commercial providers and may contain reputation lists and malware signature databases

**- Proprietary**

Commercial service offering, access to updates and research is subject to a subscription fee - could just be repackaged OSINT data, but could be closed-source data too. Just means you have to pay.

**-Closed**

Data that is provided from provider’s own research and analysis efforts, such as data from honeynets that they operate, plus information mined from its customers’ systems

**- Vulnerability databases**

**NIST NVD - National Vulnerability Database**

**- Public/private information-sharing centers**

**US-CERT - Computer Emergency Readiness Team** - responsible for analysing and reducing cyber-threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

**UK-NCSC - National Cyber Security Centre**

**AT&T Security (OTX - AlienVault)**

**MISP - Malware Information Sharing Project**

**VirusTotal -** file upload service, public repository

**SpamHaus**

**SANS ISC Suspicious Domains**

**- Dark web**

**- Indicators of compromise**

-Computer acting strangely = malware

-Computer runs slower than normal - malware is using all your resources

-Computer starts locking up or stops responding frequently, virus overwriting critical system files (possibly by accident)

-Computer restarts or crashes a lot

-Hard drive, files, or applications are no longer accessible - malware is changing permissions

-Computer makes strange noises

-Unusual error messages displayed

-Display looks strange

-Jumbled printouts

-New desktop icons or appear or disappear

-Double file extensions such as textfile.txt.exe

-Antivirus software does not run, malware shuts it down

-New files and folders have been created or are missing/corrupted

-System Restore will not function

**- Automated Indicator Sharing (AIS)**

**-- Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)**

**- Predictive analysis**

**- Threat maps**

**- File/code repositories**

**• Research sources**

**- Vendor websites**

**- Vulnerability feeds**

**- Conferences**

**- Academic journals**

**- Request for comments (RFC)**

**- Local industry groups**

**- Social media**

**- Threat feeds**

**- Adversary tactics, techniques, and procedures (TTP)**

**1.6 Explain the security concerns associated with various types of vulnerabilities.**

**• Cloud-based vs. on-premises vulnerabilities**

**• Zero-day**

Attack against a vulnerability that is unknown to the original developer or manufacturer, the time between discovery and use in the wild is ‘zero days’.

**• Weak configurations**

Any program that uses ineffective credentials or configurations, or one in which the defaults have not been changed for security. Can read/write to too many folders.

**Prevent with: scripted installations and baseline configuration templates.**

**- Open permissions**

Make sure the correct users can read/write/execute the correct files

**- Insecure root accounts**

**- Errors**

**- Weak encryption**

Use the most modern and powerful algorithms e.g. AES over DES

**- Unsecure protocols**

E.g. HTTP vs HTTPS, telnet vs SSH - use the encrypted one

**- Default settings**

Does this program really need to run as root/admin?

**- Open ports and services**

Close ports and shutdown services that are not being used.

**• Third-party risks**

**- Vendor management**

**-- System integration**

**-- Lack of vendor support**

**- Supply chain**

**- Outsourced code development**

**- Data storage**

**• Improper or weak patch management**

**- Firmware**

**- Operating system (OS)**

**- Applications**

**• Legacy platforms**

**• Impacts**

**- Data loss**

**- Data breaches**

**- Data exfiltration**

**- Identity theft**

**- Financial**

**- Reputation**

**- Availability loss**

**1.7 Summarize the techniques used in security assessments.**

**Security Assessment** - verify that the organisation’s security posture is designed and configured properly to help thwart different types of attacks.

**Active Assessments** - utilise more intrusive techniques like scanning, hands-on testing, and probing of the network to determine vulnerabilities

**Passive Assessment** - utilises open source information, passive collection and analysis of network data, and other unobtrusive methods without making direct contact with the targeted systems - limits to what you can find.

**• Threat hunting**

Cyber-security technique designed to **detect the presence of threats that have not been discovered by normal security monitoring**

Proactive as opposed to reactive. Potentially less disruptive than penetration testing - analysing data within the systems we have

Establish a hypothesis - derived from the threat modelling we have done, and is based on potential events and with higher likelihood and higher impact

Who might want to harm us? And how might they be able to do that? Analyse our threat intelligence to work this out.

Profile threat actors and activities - create scenarios that show how a prospective attacker might attempt an intrusion and what their objectives might be - who are they? What TTPs? What systems will they attack?

Threat hunting relies on the use of the tools developed for regular security monitoring and incident response

Logs, process information, SIEM data for correlation

Have to assume that the existing rules have **failed** when we are threat hunting - looking for things that haven’t been detected yet - it is challenging and difficult

Analyse network traffic, outbound traffic to suspicious domains or C2 servers? Analyses executable process list, what is being run? Analyse other infected hosts, any similarities between them? Identify how the malicious process was executed, how to stop in future?

Consumes a lot of resources and time, but is useful:

-Improve detection capabilities

-Integrate Intelligence

-Reduce attack surface

-Block attack vectors

-Identify critical assets

**- Intelligence fusion**

**- Threat feeds**

**- Advisories and bulletins**

**- Maneuver**

**• Vulnerability scans**

1. What is the **value** of the information?
2. What **threats** are we facing?
3. What **mitigations** could be deployed?
4. Define the desired state of security
5. Create a baseline
6. Prioritise the vulnerabilities
7. Mitigate vulnerabilities
8. Monitor the network and systems

**Scan - Patch - Scan**

**- False positives**

**- False negatives**

**- Log reviews**

**- Credentialed vs. non-credentialed**

Credentialed - given username and login - you see what an admin sees

Non-credentialed - you see what an attacker sees

**- Intrusive vs. non-intrusive**

**- Application**

**- Web application**

**- Network**

**- Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)**

**- Configuration review**

**- OVAL Open Vulnerability and Assessment Language**

Standard designed to regulate the transfer of secure public information across networks and the Internet utilising any security tools and services available. Has a language and an interpreter. XML schema allows it to be shared amongst multiple vulnerability assessment and management tools. Interpreter checks that it complies.

**• Syslog/Security information and event management (SIEM)**

Provides real-time analysis of security alerts generated by network hardware and applications. Software/hardware/MSSP. Splunk, ELK/Elastic Stack, ArcSight, QRadar, AlienVault/OSSIM, Graylog

-**Splunk** - big data info gathering and analysis tool that can import machine-generated data via connector visibility add-on. Can connect many data systems together. Search processing language. On-prem or cloud-based.

**-ELK/ELastic Stack** - collection of free and open-source SIEM tools that provide storage, search, and analysis functions. Made up of 1. Elasticsearch (query/analytics), Logstash (log collection/normalisation), 3. Kibana (visualisation), 4. Beats (endpoint collection agents). Beats installed on different servers and data goes either to Logstash to be parsed then sent to Elastic, or goes straight to Elastic, then visualises the data in Kibana. On-prem/cloud-based.

-**ArcSight -** SIEM log management and analytics software that can be used for compliance reporting for legislation and regulations like HIPAA, SOX, and PCI DSS

**-Qradar -** SIEM log management, analytics, and compliance reporting platform by IBM.

**-AlienVault/OSSIM (Open-Source Security Information Management) -** SIEM solution originally developed by AlienVault now owned by AT&T and rebranded as **AT&T Cybersecurity.** OSSIM can integrate other open source tools and provides integrated webadmin tools to manage the whole security environment.

-**Graylog -** open-source SIEM with an enterprise version focused on compliance and supporting IT operations and DevOps.

-Log all relevant events and filter irrelevant data

-Establish and document scope of events

-Develop use cases to define a threat

-Plan incident response for an event

-Establish a ticketing process to track events

-Schedule regular threat hunting.

-Provide auditors and analysts and evidence trail.

**- Review reports**

**- Packet capture**

**- Data inputs**

**- User behavior analysis**

**- Sentiment analysis**

**- Security monitoring**

**- Log aggregation**

**- Log collectors**

**• Security orchestration, automation, and response (SOAR)**

A class of security tools that facilitate incident response, threat hunting, and security configurations by orchestrating automated runbooks and delivering data enrichment.

‘SIEM 2.0’ - next-gen SIEM. Security information and event monitoring system with an integrated SOAR. Mainly used for **incident response**.

Scan security/threat data - analyse with machine learning - automate data enrichment - provision new resources e.g. accounts, VMs + delete/modify them.

**1.8 Explain the techniques used in penetration testing.**

**• Penetration testing**

Looks at a network’s vulnerabilities from the outside - simulates an attack on the system and performs it in real life.

-Test the system to discover vulnerabilities and prove security controls work

-Examine the system to identify any logical weaknesses

-Interview personnel to gather information

1. Get permission and document info
2. Conduct recon
3. Enumerate the targets
4. Exploit the targets
5. Document the results

Can also simulate an insider threat

**- Known environment - white box**

Full knowledge of the environment

**- Unknown environment - black box**

Zero knowledge of the environment

**- Partially known environment - grey box**

Some knowledge of the environment

**- Rules of engagement**

**- Lateral movement**

**- Privilege escalation**

**- Persistence**

Ability of attacker to maintain a foothold inside the compromised network

**- Cleanup**

**- Bug bounty**

**- Pivoting**

Attacker moves onto another workstation or account

**• Passive and active reconnaissance**

**- Drones**

**- War driving / war flying**

Driving/flying around looking for open WiFi networks.

**- War dialing**

Pinging every IP address in a range to look for active hosts.

**- War chalking**

Physically draw info about found networks - two open halves, one closed circle, or closed circle with password

**- Footprinting**

**- OSINT**

**• Exercise types**

**- Tabletop Exercises (TTX)**

Uses an incident scenario against a framework of controls or a red team **Discussion** of simulated emergency situations and security incidents.

**- Red-team**

Hostile/attacking team, the hackers

**- Blue-team**

Defensive team, sysadmins, cyber security analysts

**- White-team**

Administer, evaluate and supervise - ‘referees’

**- Purple-team**

Red and blue teams work together in a feedback loop.

**- Yellow-team**

Builds the environment that will be used in the exercise

**2.0 Architecture and Design (21%)**

**2.1 Explain the importance of security concepts in an enterprise environment.**

**• Configuration management**

**- Diagrams**

**- Baseline configuration**

All new machines are set up with a baseline image of the OS, necessary installed programs, policy settings, user settings etc.

**- Standard naming conventions**

**- Internet protocol (IP) schema**

**- Group Policy**

A set of rules or policies that can be applied to a set of users or computer accounts within the operating system. In Windows, run gpedit in Run. Things like password complexity, account lockout policies, software restrictions, application restrictions. AD has a more advanced version.

Loading different Group Policy Objectives (GPOs) helps to harden the operating system.

**• Data sovereignty**

**• Data protection**

**- Data loss prevention (DLP)**

**- Masking**

**- Encryption**

**- At rest**

**- In transit/motion**

**- In processing**

**- Tokenization**

**- Rights management**

**• Geographical considerations**

**• Response and recovery controls**

**• Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection**

Cryptographic protocols that provide secure internet communications for web browsing, instant messaging, email, VoIP etc. SSL deprecated, last updated in 1996.

**• Hashing**

**• API considerations**

**• Site resiliency**

Hot = expensive, cold = cheap.

**- Hot site**

Near duplicate, can be up and running in **minutes**.

**- Warm site**

Tech stuff like computers and servers, needs config, **hours** before they can start working

**- Cold site**

No tech beyond cables and phones, need computers and servers, **days** to get online.

**• Deception and disruption**

Used to attract and trap potential attackers. Used by security researchers to learn TTPs.

**- Honeypots, honeyfiles**

A single computer (or file/files, or IP range) that might be attractive to an attacker.

**- honeynets**

Group of computers, servers, networks used to attract an attacker. When you need a bigger honeypot.

**- Fake telemetry**

**- DNS sinkhole / blackhole**

DDoS - identifies any attacking IP address and routes all their traffic to a non-existent server through the null interface.

**2.2 Summarize virtualization and cloud computing concepts.**

**• Cloud models**

Benefits: Decreased cost, increased availability, unlimited elasticity

Downsides: many of the issues from physical servers happen on the cloud too, cloud does not magically fix all your problems.

Hyperconvergence - allows providers to fully integrate the storage, network, and servers

**Logs** - make sure they are copied to non-elastic storage so they are not lost.

**Buckets/Blobs** - cloud storage containers. Access control is administered through container policies, IAM authorisation, and object ACLs. Incorrect permissions can be a problem, set to default. **CORS (Cross Origin Resource Sharing)** - content delivery network policy that instructs the browser to treat requests from nominated domains as safe, weak CORS exposes the site to vulnerabilities like XSS.

**- Software as a service (SaaS)**

Provides all the hardware, operating system, software, and applications needed for a complete service to be delivered e.g. Office 365, DealCloud, Recorded Future - **providing the software**

**- Platform as a service (PaaS)**

Provide your organisation with the hardware and software needed for a specific service to operate e.g. Heroku, AWS Elastic Beanstalk **OS platform to** **run software you already have**

**- Infrastructure as a service (IaaS)**

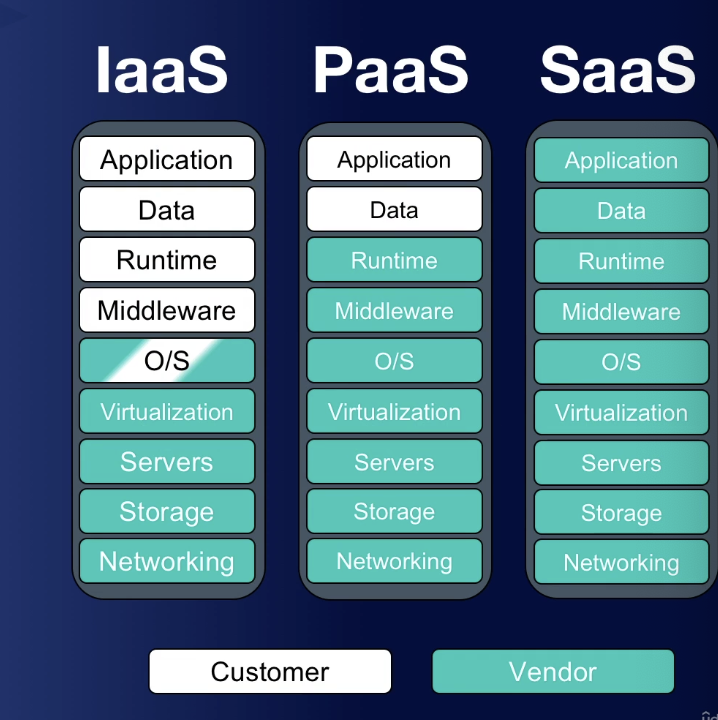
Provides all the hardware, operating system, backend software needed **to run a server in order to develop your own SaaS** e.g. Rackspace, DigitalOcean, AWS

**- Security as a service (SECaaS)**

Provides your organisation with various security services without the need to maintain cybersecurity staff e.g. anti-malware, anti-spam however need internet connection

Cloud-based vulnerability scans can better provide the attacker’s perspective. MSSP.

**- Anything as a service (XaaS)**



**- Public**

Service provider makes resources available to the end user over the internet: Google Cloud, Azure, AWS. Cheapest.

**- Private**

Company creates its own cloud environment that only it can utilise as an internal enterprise resource. Responsible for design, implementation, management of the system and servers. US Government cloud - when security is more important than cost.

**- Hybrid**

Combo of public and private. Need strict rules for what is allowed in which part.

**- Community**

Resources and costs are shared among several different organisations who have common service needs e.g. local banks - like combining multiple private clouds.

**• Cloud service providers**

**• Managed service provider (MSP)/managed security service provider (MSSP)**

**• On-premises vs. off-premises**

On-premises, maintained locally, responsible for everything, you own it including the hardware, expensive. Many softwares can be both cloud-based and on-premise. Off-premises is a lot cheaper and requires less support, but is less secure - also better for AI and ML.

Consider compliance or regulatory limitations of storing data in a cloud-based security solution e.g. transferring data over borders.

Be aware of possible vendor lock in - where you have so much data that it’s too expensive to move.

**• Fog computing**

**• Edge computing**

**• Thin client**

**• Containers**

**• Microservices/API**

Allows for automated administration and management of cloud policies. REST or SOAP.

Integration between lots of different cloud services.

**Insecure API** - you MUST use HTTPS. Must perform input validation. Error handling and sanitised error messages. Implement throttling/rate-limiting to prevent a DoS.

**API key management** - need to use secure authentication and authorisation such as SAML or OAuth/OIDC before accessing data. Do not hardcode or embed key into source code. Delete unnecessary keys, regenerate keys when moving into prod.

**• Infrastructure as code (IaC)**

**Provisioning architecture in which deployment of resources is performed by scripted automation and orchestration.** Allows for the use of scripted approaches to provisioning infrastructure on the cloud. Need 3 things - security templates, scripts, and security policies.

**Snowflake system** - a system that is different in its configuration compared to a standard template within an infrastructure as code architecture. Wrecks IaC and orchestration. Lack of consistency can cause security problems. Eliminate them.

**Idempotence** - a property of IaC that an automation or orchestration action always produces the same result, regardless of the component’s previous state. Can easily generate consistent builds.

**- Software-defined networking (SDN)**

**- Software-defined visibility (SDV)**

**• Serverless architecture**

**FaaS - Function as a Service** - a cloud service model that supports serverless software architecture by provisioning runtime containers in which code is executed in a particular programming language e.g. **AWS Lambda**, Azure Functions

**Serverless** - software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances - everything is developed as a function or microservice. No need for servers, you only pay for the time you use, insanely cheap. No patching. No admin. No file system monitoring. Netflix uses serverless AWS Lambda.

Need to ensure that the clients accessing the services have not been compromised, means there is a lot more code reviewing to check it is secure.

**• Services integration**

**• Resource policies**

**• Transit gateway**

**• Virtualization**

Virtual Machine is a container for an emulated computer that runs an entire OS.

System Virtual Machine - complete platform designed to replace an entire physical computer and includes a full desktop/server OS.

Processor Virtual Machine - designed to run only a single process or application like a virtualized web browser or a simple web server.

Reduces the physical requirements for data centres.

**Hypervisor** - manages the distribution of the physical resources of a host machine (server) to the virtual machines being run (guests).

**Type I** - ‘bare metal’, runs directly on host hardware e.g. Hyper-V.

**Type II** - runs on the OS e.g. VirtualBox, VMWare.

**Application containerization** - A single operating system kernel is shared across multiple virtual machines but each virtual machine receives its own user space for programs and data. Rapid and efficient deployment of distributed apps, more efficient than Type I and Type II e.g. Docker

Elasticity - can scale up and down very easily. However this can leave behind **data remnants** that exist as deleted files on a cloud-based server after deprovisioning of a virtual machine.

**Live migration** - when you move a VM between physical servers, vulnerable to MitM attack.

VMs need AV and firewalls too. Limit connections between VM and host. Remove unnecessary virtual hardware. Keep patched and up to date.

**- Virtual machine (VM) sprawl avoidance**

Occurs when VMs are created, used, and deployed, without proper management or oversight by the system admins. Easy to lose track of them as it is just a file on a server. Need to encrypt VM files.

**- VM escape protection**

VMs are separate from each other by default. However if an attacker can interact with the hypervisor then they can escape into a different VM. DO NOT connect the VM to your host machine’s folders.

**2.3 Summarize secure application development, deployment, and automation concepts.**

**• Software Development Lifecycle (SDLC)**

Waterfall model

Planning and Analysis - requirements gathering

Software/Systems Design

Implementation - writing the code

Testing

Integration - connecting different applications together

Deployment

Maintenance - including retirement

Agile model - sprints, smaller releases more often

DevOps - dev and ops integrated to get product out quicker

**• Testing**

**Black-box testing** - when a tester is not provided with **any information** about the system or program prior to conducting the test

**White-box testing** - tester is given full details of a system including source code, diagrams etc.

**Grey-box testing** - tester is given some details e.g. user access but not admin.

Runtime error - error when the program is running

Compile-time / syntax error - fails to run, caused by errors in the source code

Structured Exception Handling (SEH) - provides control over what the application should do when faced with a runtime or syntax error

**• Environment**

**- Development**

**- Test**

**- Staging**

**- Production**

**- Quality assurance (QA)**

**• Provisioning and deprovisioning**

**• Integrity measurement**

**• Secure coding techniques**

**- Normalization**

**- Stored procedures**

**- Obfuscation/camouflage**

**- Code reuse/dead code**

Copy and pasting code - from the same app, diff app, and from stack overflow - you haven’t checked if it is secure.

**- Server-side vs. client-side execution and validation**

**- Memory management**

**- Use of third-party libraries and software development kits (SDKs)**

Should rely on trusted and up to date SDKs and third-party libraries. You don’t know if it’s secure otherwise.

**- Data exposure**

**• Open Web Application Security Project (OWASP)**

**• Software diversity**

**- Compiler**

**- Binary**

**• Automation/scripting**

**Orchestration** - the automation of automations

Resource orchestration - space and resources, e.g. EC2

Workload orchestration - managing apps

Service orchestration - working on the services themselves

Third-party orchestration - prevents vendor lock-in

**- Automated courses of action**

**- Continuous monitoring**

Technique of constantly evaluating an environment for changes so that new risks may be more quickly detected

**- Continuous validation**

Involves parallel software testing methodologies in which the internal structure and design of an item are being tested. White and black box testing focuses on all those areas in the code where bugs and problems have occurred to help the dev team remove them as quickly as possible.

**- (CI/CD)**

Used to do everything linearly - waterfall model. Now we try to speed things up. Common Source Repository.

**- Continuous integration**

Dev method where code updates are tested and committed to a dev server/repo rapidly (multiple times a day). Detects and resolves code conflicts early and often.

**- Continuous delivery**

Dev method where app and platform requirements are frequently tested and validated for immediate availability. Automated testing of code **in order to get it ready for release, not released.**

**- Continuous deployment**

Dev method where app and platform updates are **released** to production rapidly.

**- DevOps**

Combines software dev and system ops (people who support) into one by integrating the two within the company.

**- DevSecOps**

Also includes security to make sure code is secure. ‘Shift-left’ mindset. Shift security to be earlier in the life cycle. Integrates security from the beginning. Test during and after development. Automate compliance checks.

**• Elasticity**

Would not be possible with orchestration (automation of automations).

**• Scalability**

**• Version control**

**2.4 Summarize authentication and authorization design concepts.**

**• Authentication methods**

**- Directory services**

**- Federation - Federated Identity Management (FIdM)**

A single identity is created for a user and shared with all of the organisations in a federation e.g. you can use Google/Apple/Microsoft/Facebook account to login to websites not owned by those companies

**Cross-certification/Web of Trust** - utilises a web of trust between organisations where each one certifies the other in the federation - good for small number of orgs (5-10 max)

**Trusted Third-Party/Bridge -** Orgs are able to place their trust in a single third-party. More efficient than cross-certification.

**- Attestation**

**- Technologies**

**-- Time-based one-time password (TOTP)**

Password is computed from shared secret and current time

**-- HMAC-based one-time password (HOTP)**

Password is computed from a shared secret and is synchronised between the client and server, changes when used

**-- Short message service (SMS)**

**-- Token key**

**-- Static codes**

**-- Authentication applications**

**-- Push notifications**

**-- Phone call**

**- Smart card authentication**

**• Biometrics**

**- Fingerprint**

**- Retina**

**- Iris**

**- Facial**

**- Voice**

**- Vein**

**- Gait analysis**

**- Efficacy rates**

**- False acceptance**

**- False rejection**

**- Crossover error rate**

**• Multifactor authentication (MFA) factors and attributes**

You need at least two of the below 5 attributes to be considered MFA - even if it is multiple elements of the same type, **this is still considered single-factor e.g. username/password**

**- Factors**

**-- Something you know**

Password, username, mother’s maiden name, social security number, place/date of birth

**-- Something you have**

Driver’s licence, passport, credit card, token device, smart card, usb dongle, cell phone

**-- Something you are**

Fingerprint, iris scan, retina scan, facial recognition, voice recognition

**- Attributes**

**-- Somewhere you are**

GPS location

**-- Something you can do**

Way you sign your name

**-- Something you exhibit**

**-- Someone you know**

**• Authentication, authorization, and accounting (AAA)**

**Authentication -** when a person’s identity is established with proof and confirmed by a system

**Authorisation -** occurs when a user is given access to a certain piece of data or certain areas of a building

**Accounting -** Tracking of data, computer usage, and networking resources - **LOG** files

**• Cloud vs. on-premises requirements**

**2.5 Given a scenario, implement cybersecurity resilience.**

**• Redundancy**

**Single point of failure** - if these fail then the whole system fails.

**- Geographic dispersal**

**- Disk**

**-- Redundant array of inexpensive disks (RAID) levels**

Allows the combination of multiple physical hard disks into a **single logical** hard disk drive that is recognised by the OS. **Redundancy** and high **availability**.

Performance - faster but the failure of either drive will cause the whole logical drive to fail.

Redundancy - need twice as many drives.

**RAID 0** - data striping, 2 disks. Performance but not redundancy.

**RAID 1** - data mirroring, 2 disks. Redundancy if one drive fails.

**RAID 10/01** - nested, combines 1 and 0, at least 4 disks. Striped raid with mirroring.

**RAID 5** - data striping with parity, at least 3 disks. If one disk fails the other two can continue to operate by reconstructing data using the parity.

**RAID 6** - modified RAID 5, at least 4 disks. Has double parity stripes. Can lose two disks simultaneously.

Fault-resistant - RAID 1, 5 - can lose one disk.

Fault-tolerant - RAID 1, 5, 6 - can lose components.

Disaster-tolerant - RAID 10 - two independent zones.

**-- Multipath**

**- Network**

**-- Clustering / Load Balancers**

Two or more servers working together to perform a particular job function.

**Failover Cluster** - secondary server that can take over the function when the primary one fails with limited or no downtime. Domain Controllers - DC1/DC2. Mail Servers.

**Load-Balancing -** servers are clustered in order to share resources such as CPU, RAM, and hard disks e.g. for parallel processing of computational tasks, or for web servers that get a lot of requests e.g. any of the big ones.

**-- Network interface card (NIC) teaming**

Multiple NIC cards in case one fails. Multiple cables. Multiple internet connections.

**- Power**

Surge - unexpected increase in voltage.

Spike - short transient increase in voltage due to short circuit, lightning strike etc.

Sag - unexpected decrease in voltage.

Brownout - when voltage drops low enough that it typically causes lights to dim and can cause a computer to shut off.

Blackout - all power is lost.

**-- Uninterruptible power supply (UPS)**

Combines the functionality of a surge protector with a battery backup. Short duration - 15-60 mins.

**-- Generator**

Emergency power system used when the electricity grid goes down. Portable-gas = petrol/solar. Permanently installed generator = natgas/propane/diesel, can run the whole building. Battery-inverter = lead-acid batteries, lower powered.

**-- Dual supply**

Two power supplies in case one fails e.g. for servers.

**-- Managed power distribution units (PDUs)**

**• Replication**

**- Storage area network**

**- VM**

**• On-premises vs. cloud**

If the cloud crashes you will have a lack of availability. When you share with other tenants they can slow down or crash your server.

**• Backup types**

**- Full**

Entire drive backed up. Slow.

**- Differential**

Only conducts a backup of the contents of a drive that has changed since the last full backup. More time to backup but less time to restore.

You need to restore using the 1x last full backup and the 1x last differential backup.

**- Incremental**

Backup only contents of the drive that have changed since the last full or incremental backup. Less time to backup but more time to restore.

You need to restore with 1x last full backup and ALL incremental backups.

**- Snapshot**

A database snapshot provides a read-only, static view of a source database as it existed at snapshot creation. Entire OS including all apps and data - **virtual disk image.** Commonly used with virtual systems.

**- Tape**

**10 tape** - each tape used once per day for two weeks and then the entire set is reused.

**Grandfather-father-son** - son = daily, father = weekly, grandfather = monthly

**Towers of Hanoi** - like grf/f/son, more complex rotation.

**- Disk**

**- Copy**

**- Network-attached storage (NAS)**

Huge array of hard drives directly connected to the network to backup data. Implement RAID arrays to ensure high availability.

**- Storage area network**

Multiple NAS combined into a network. Use encryption, use proper authentication (as they are acting as file servers) individualised to each user, log NAS access.

**- Cloud**

**- Image**

**- Online vs. offline**

**- Offsite storage**

**-- Distance considerations**

**• Non-persistence**

**- Revert to known state**

**- Last known-good configuration**

**- Live boot media**

**• High availability**

**- Scalability**

**• Restoration order**

**• Diversity**

**- Technologies**

**- Vendors**

**- Crypto**

**- Controls**

**2.6 Explain the security implications of embedded and specialized systems.**

**• Embedded systems**

A computer that is designed to perform a specific, dedicated function. Very rarely updated, not designed to get updates. Very little support for identifying and correcting security issues. Keep on a separate network.

**- Field-programmable gate array (FPGA)**

IC can be programmed however you want, can run a specific application instead of using an ASIC (application-specific integrated circuit)

Anti-tamper mechanism - Can have an ‘antifuse’ mechanism applied that permanently fixes the structure of the IC when tampered with.

**- Programmable Logic Controller (PLC)**

A type of computer designed for deployment in an industrial or outdoor setting that can automate and monitor mechanical systems. Can be patched and reprogrammed.

**- Raspberry Pi**

**- Arduino**

**• Supervisory control and data acquisition (SCADA)/industrial control system (ICS)**

**OT - Operational Technology** - comms network designed to implement an industrial control system (ICS) as opposed to data networking (IT) e.g. manufacturing, factories, power plants. Basically instead of using an OS to run these, you’re using SCADA/ICS to tell it what to do.

AIC (not CIA) - availability and integrity more important than confidentiality.

**- Industrial Control Systems (ICS)**

A network that manages embedded devices e.g. power station, water, hospitals, telecoms, manufacturing, defence. Link together **PLCs** using **Fieldbus** to make changes in the physical world.

**- Fieldbus**

Digital serial data comms used in OT networks to link Programmable Logic Controllers (PLCs)

**- Human-Machine Interface (HMI)**

Input and output controls on a PLC to allow a user to configure and monitor the system

**- Data historian**

Software that catalogs data from multiple sources within an ICS (for incident response)

**- Supervisory control and data acquisition (SCADA)**

Industrial control system that manages large-scale multiple-site devices and equipment spread over a geographic region. **ICS = 1 plant, SCADA = multiple plants.**

Runs as software on ordinary computers to gather data from and manage plant devices and equipment with embedded PLCs.

**- Modbus**

Comms protocol used in OT networks **(instead of TCP/IP)** - gives control servers and SCADA hosts the ability to query and change the config of each PLC

**- Facilities**

**- Industrial**

**- Manufacturing**

**- Energy**

**- Logistics**

**• Internet of Things (IoT)**

Group of objects connected to the internet using embedded components. Linux or Android as the OS. Must be kept up to date. IoT and security do not go together - segment them into their own network.

**- Sensors**

**- Smart devices**

**- Wearables**

**- Facility automation**

**Building Automation Systems (BAS) -** components and protocols that facilitate the centralised configuration and monitoring of mechanical and electrical systems within offices and data centres e.g. external batteries, elevators, HVAC etc. - keep as a separate network.

-Vulnerabilities in PLC, credentials in app code, code injections against web user interface

-you can be DoS’d in real life e.g. your HVAC turns off

**Physical Access Control Systems (PACS)** - components and protocols that facilitate the centralised configuration and monitoring of security mechanisms within offices and data centres. Can be part of **BAS**, or a separate system. Often installed by **third-party**, can get omitted, they need to be legally responsible.

**- Weak defaults**

Mirai botnet, 100k IoT devices with default passwords.

**• Specialized**

**- Medical systems**

Use embedded systems, PLCs to run medical equipment e.g. IV drip monitor

**- Vehicles**

**- Aircraft**

Controller Area Network CAN - vehicles systems all connect to this inside the vehicle.

OBD-II - onboard diagnostics module, primary external interface to the vehicle - operates like ethernet, little security.

Some cars have cellular/WiFi - this brings cars into IoT and connects to CAN. No method authentication, **in a** **CAN bus, all messages are trusted.**

3 ways: physically attach exploit to OBD-II, exploit over onboard cellular, exploit over onboard wifi

**- Smart meters**

Smart meters for example are all part of a SCADA network (from the perspective of the utilities company).

**• Voice over IP (VoIP)**

Digital phone service provided over a data network.

Must put VoIP on its own VLAN and own subnets so they do not intermix with the other data you have between your computers. Update the firmware of the phones.

**• Heating, ventilation, air conditioning (HVAC)**

Maintain humidity, around 40%

ICS/SCADA network connection.

Power loss can shut down your HVAC.

Need shielding to prevent EMI

Can be hacked or DoS’d

**• Drones**

**• Multifunction printer (MFP)**

**• Real-time operating system (RTOS)**

Type of OS that prioritises deterministic execution of operations to ensure consistent response for **time-critical tasks** e.g. aircraft, nuclear plants etc. Cannot tolerate reboots, crashes, and must have response times to microseconds.

**• Trusted operating system (TOS)**

OS that meets the requirements set forth by the federal government and has multilevel security - Windows 7 (and newer, including server 2012/2016), Mac OSX 10.6 (and newer), TrustedBSD, Red Hat Enterprise Server - why Mac and Windows release so many patches.

**• Surveillance systems**

**Premise systems -** e.g. security cams, login doors - can often be monitored via corporate network, and therefore hackers can get in via the internet

**• System on chip (SoC)**

A processor that integrates the platform functionality of multiple PLCs programmable logical controllers onto a single chip. Power-efficient.

**• Communication considerations**

**- 5G**

**- Narrow-band**

**- Baseband radio**

**- Subscriber identity module (SIM) cards**

IC that securely stores the International Mobile Subscriber Identity (IMSI) number and its related key, which tells the cell phone towers what device is assigned to what number.

**SIM cloning** - allows two phones to utilise the same service and allows an attacker to gain access to the phone’s data. Newer **SIM version 2** cards are more difficult to clone.

**- Zigbee**

**• Vulnerabilities**

1. Establish **admin control** over OT networks - by recruiting staff with relevant expertise
2. Implement the **minimum network links** - by disabling unnecessary links, services, and protocols e.g. corporate network and plant network
3. Develop and test a **patch management program** for OT networks
4. **Perform regular audits** of logical and physical access to systems to detect possible vulnerabilities and intrusions

Vulnerability scanners can damage an OT network.

**• Constraints**

**- Power**

**- Compute**

**- Network**

**- Crypto**

**- Inability to patch**

Very rarely patched, very difficult to apply patches, not designed to be patched.

**- Authentication**

Physical access is usually enough, no passwords.

**- Implied trust**

Little security e.g. CAN network assumes everything on it is trusted.

**- Range**

**- Cost**

**2.7 Explain the importance of physical security controls.**

**• Bollards/barricades**

Prevents vehicle ramming attacks to get into your facilities.

**• Access control vestibules (mantrap)**

Area between two doorways that holds people until they are identified and authenticated

**• Badges**

**• Alarms**

**• Signage**

**• Cameras**

**- Motion recognition**

**- Object detection**

**• Closed-circuit television (CCTV)**

Wired or wireless (easier to jam).

Outdoor vs indoor cameras.

PTZ - Pan-Tilt-Zoom - guard can move it around

Infrared - heat map

Ultrasonic - sound based detection

Placement is important - exits and entrances

**• Industrial camouflage**

**• Personnel**

**- Guards**

**- Robot sentries**

**- Reception**

**- Two-person integrity/control**

**• Locks**

**- Biometrics**

‘Something you are’

Worry about **False Acceptance Rate (FAR)** - should not let people in who shouldn’t

Also **False Rejection Rate (FRR)** - should not deny authorised people

**Crossover Error Rate (CER)** or Equal Error Rate (ERR) - when the FAR and FRR are the same

Fingerprint

Facial recognition

Retina - must be very close to have beam shone into back of eye (retina)

Iris - uses camera to take a picture of coloured part of eye, 3-10 inches away

**- Electronic**

RFID badge reader (MFA with PIN number - authenticated which person entered)

**- Physical**

Basic lock with key, pin and tumbler (can be picked)

Cipher lock - the tall silver one with 14 push buttons, numbers and XYZ etc

**- Cable locks**

Plugs into case of laptop so it can’t just be picked up and stolen

**• USB data blocker**

**• Lighting**

**• Fencing**

**• Fire suppression**

**Handheld** - A, B, C, D, K class fires.

A green triangle- wood/paper/fabrics etc, water

B red square - flammable liquids/gases e.g. petrol, oil etc. CO2

C CO2 blue circle - electrical fire, CO2

D yellow star - combustible metals e.g. laptop battery

K black hexagon - cooking oil

**Sprinklers -**

wet pipe, already full of water and just needs to be triggered

dry pipe, full of air and pump water in when necessary

Pre-action - detects heat and smoke, not necessarily fire

Do not use any in a server room

**Special Hazard Protection**

HALON, CO2, FM-200 gas instead of water to not destroy server room

**• Sensors**

**- Motion detection**

**- Noise detection**

**- Proximity reader**

**- Moisture detection**

**- Cards**

**- Temperature**

**• Drones**

**• Visitor logs**

**• Faraday cages**

Shielding installed around an entire room prevents electromagnetic energy and radio frequencies from entering or leaving the room.

TEMPEST - US government standards for shielding. Also resistant to EMP.

**• Air gap**

**• Protected cable distribution**

Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats e.g. locks on all closets, special protected wiring - very expensive.

**EMI** - Electromagnetic Interference

**RFI** - Radio Frequency Interference

**Crosstalk** - wires interfering with each other

**Data Emanation** - transmit data out, mil/gov level

Fix with: STP - Shielded Twisted Pair - covered in foil (don’t use UTP, unshielded, but cheaper) or fibre optics.

**• Secure areas**

**- Air gap**

No network interfaces connected to the outside world.

**- Vault**

**- Safe**

**- Hot aisle**

**- Cold aisle**

Hot and cold aisles, hot air comes out the back of servers into the same aisle

**• Secure data destruction**

**- Burning**

**- Shredding**

**- Pulping**

**- Pulverizing**

**- Clearing**

Reasonable amount of assurance it cannot be reconstructed e.g. overwrite with 0s. Not high security.

**- Purging / Sanitizing**

Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques. Destroy the encryption key of an encrypted drive.

**- Degaussing**

Magnetic disposal - hard drives **cannot** be used after.

**- Third-party solutions**

**2.8 Summarize the basics of cryptographic concepts.**

**Data at Rest -** inactive data that is archived, such as data resident on a hard drive disk

**Data in Transit -** data crossing the network or data that resides in a computer’s memory

**Data in Use -** data that is undergoing constant change

**Cipher -** algorithm that performs encryption/decryption

Confidentiality, Integrity, Authentication, Non-Repudiation

**Plaintext vs ciphertext**

**• Digital signatures**

A hash of a message is encrypted with the sender’s private key to let the recipient know that the document was created and sent by the person claiming to have sent it. **Integrity** (hash checks it is the same message) of the message and **non-repudiation** (encrypting with private key proves sender sent it). Then encrypt the message with the recipient’s public key (**confidentiality,** only they can decrypt).

DSA (US govt), RSA (commercial), RCDSA, SHA.

**• Key length**

Strength of the encryption system lies in key strength.

**• Key stretching**

Technique used to mitigate a weaker key by increasing the time needed to crack it e.g. apply the algo 5000 times.

WPA, WPA2, PGP, bcrypt use this.

**• Salting**

Add random data into a hash to help protect against password cracking techniques e.g. rainbow tables

None - number added.

**• Hashing**

One-way cryptographic function which takes an input and produces a unique message digest. Always the same length output. **Exam: INTEGRITY. MD5 (less secure) and SHA.**

**MD5** - 128-bit hash value. Can cause hash collisions. Weak.

**SHA1 -** 160-bit hash value.

**SHA2 -** SHA-224, SHA-256, SHA-348, SHA-512.

**SHA3 -**  224-bits to 512-bits. More rounds of computations.

**RIPEMD Race Integrity Primitive Evaluation Message Digest -** open-source hash algo that creates a unique 160-bit (most common, RIPEMD-160), 256-bit, or 320-bit message digest.

**HMAC Hash-based Message Authentication Code -** uses hash algo to create a level of assurance as to the integrity and authenticity of a given message or file, HMAC-MD5, HMAC-SHA1, HMAC-SHA256 etc.

**• Password Hashing**

**LANMAN (LM Hash) -** original version of password hashing used by windows that used DES and is limited to 14 characters. Very very weak.

**NT LAN Manager Hash (NTLM Hash) -** replacement to LM Hash that uses RC4 and was released with Windows NT 3.1 in 1993. Very weak.

**NTLMv2 Hash -** replacement to NTLM Hash that uses HMAC-MD5 and is considered difficult to crack. Used when you do not have a domain with Kerberos for authentication.

**• Key exchange**

Diffie-Hellman - asymmetric algo to share a much faster symmetric key.

**• Elliptic-curve cryptography**

**• Perfect forward secrecy**

Perfect forward secrecy protects past sessions against future compromises of keys or passwords - ephemeral keys.

**• Quantum**

**- Computing**

Uses quantum mechanics to generate and manipulate quantum bits (qubits) in order to access enormous processing power.

Qubits - composed of electrons or photos that can represent numerous combinations of 1s and 0s at the same time through superposition.

**- Communications**

Relies on quantum bits (qubits) made of photos to send multiple combinations of 1s and 0s simultaneously which results in tamper resistant and extremely fast communications.

**• Post-quantum cryptography**

Asymmetric encryption algorithms have been mathematically proven to be broken by quantum computers. We need quantum-resistant cryptography that can be implemented using today’s classical computers but impervious to attacks from future quantum computers.

One method is to increase key size - good for symmetric keys.

Lattice-based cryptography and supersingular isogeny key exchange - advanced crypto.

**• Ephemeral**

Key generated for each execution of a key establishment process. Short-lived and used in key exchange for WPA3 to create perfect forward secrecy.

**• Modes of operation**

**- Authenticated**

**- Unauthenticated**

**- Counter**

**• Blockchain**

Shared immutable ledger for recording transactions, tracking assets and building trust.

Permissioned blockchain - used for business transactions and promotes new levels of trust and transparency - IBM. Supply chain, fully traceable.

**- Public ledgers**

A record keeping system that maintains participants’ identities in secure and anonymous form, their respective cryptocurrency balances, and a record book of all the genuine transactions executed between network participants.

**• Cipher suites**

**- Stream**

Keystream generator to encrypt data **bit by bit** using an XOR function to create a ciphertext. Good for securing real-time data like audio or video. Symmetric algorithms. Often used in hardware.

**One-Time Pad** - unbreakable stream cipher. Secret key is the same length as the plaintext input.

**- Block**

Breaks the input into **fixed-length blocks** of data and performs the encryption on each block. Padding can be added. Easier implementation, less susceptible to security issues, easier to implement with software.

**• Symmetric vs. asymmetric**

**Symmetric, Private Key - single key** used for encryption/decryption. Both the sender and the receiver must know the same secret using a privately held key. Confidentiality can be assured. Cannot assure non-repudiation - we don’t know who uses the key. 100-1000x faster than asymmetric, however, it is difficult to distribute the keys.

**-DES Digital Encryption Standard** - block cipher, 64-bit blocks, key-strength only 56-bits. Standard in the 1970s but not good today.

**-3DES Triple DES** - block cipher, uses three symmetric keys to encrypt, decrypt, then encrypt plaintext to cipher text in order to increase the strength of DES, 112-bit key

**-IDEA International Data Encryption Algorithm -** block cipher, 64-bit blocks, used in Pretty Good Privacy PGP.

**-AES Advanced Encryption Standard -** block cipher that uses 128-bit, 192-bit, or 256-bit blocks and a matching encryption key size.

**-Blowfish -** block cipher that uses 64-bit blocks and variable length encryption key.

**-Twofish -** block cipher that replaced blowfish and used 128-bit blocks and a 128/192/256-bit key.

**-RC4 - stream cipher (ONLY ONE)**, 40-bit to 2048-bit variable key that is used in SSL/WEP

**-RC5 -** block cipher, key size up to 2048-bit

**-RC6 -** block cipher, introduced as replacement for DES but AES was chosen instead

**Asymmetric, Public Key - two keys,** one for encryption, one for decryption.

**-Diffie-Hellman -** used to conduct key exchange and secure key distribution over a network. Used for the establishment of VPN tunnels using IPSec. Susceptible to MitM.

**-RSA -** large prime factoring. 1024-bit to 4096-bit.

**-ECC Elliptic Curve Cryptography -** algebraic structure of elliptic curves over finite fields. **Used a lot in mobile devices and low-processing power devices.** A 256-bit key is just as secure as 2048-bit RSA.

**-ECDH Elliptic Curve Diffie-Hellman**

**-ECDHE Elliptic Curve Diffie-Hellman Ephemeral**

**-ECDSA Elliptic Curve Digital Signature Algorithm**

**Hybrid - utilises asymmetric encryption to securely transfer a private key that can then be used with symmetric encryption.**

-**PGP Pretty Good Privacy -** symmetric IDEA functions use a 128-bit or higher keys and the asymmetric RSA functions use 512-bit to 2048-bit keys.

**-GPG GNU Privacy Guard -** upgraded version of PGP that uses AES instead of IDEA. Cross-platform.

**• Lightweight cryptography**

**• Steganography**

Hiding messages inside other messages. Obfuscation - not encryption.

**- Audio**

**- Video**

**- Image**

**• Homomorphic encryption**

Form of encryption that permits users to perform computations on its encrypted data without first decrypting it. Good for CLOUD - send your data to the cloud and have them work on it.

**• Common use cases**

**- Low power devices**

Elliptic Curve Cryptography.

**- Low latency**

**- High resiliency**

**- Supporting confidentiality**

PKI - encrypt with person’s public key and send to person, person can decrypt with their private key

**- Supporting integrity**

**- Supporting obfuscation**

Steganography.

**- Supporting authentication**

**- Supporting non-repudiation**

PKI - encrypt with my private key and sent to world, all can decrypt with my public key

**• Limitations**

**- Speed**

Performance impact when using whole-disk encryption software, can speed up by using hardware SED. Some prefer to use file-level encryption instead such as Microsoft EFS.

**- Size**

**- Weak keys**

**- Time**

**- Longevity**

**- Predictability**

**- Reuse**

**- Entropy**

**- Computational overheads**

**- Resource vs. security constraints**

**3.0 Implementation (25%)**

**3.1 Given a scenario, implement secure protocols.**

**• Protocols**

Inbound port - opened when listening

Outbound port - opened when connecting

0-65,535

**Well-known ports - 0 - 1023**, designated by IANA

**Registered ports - 1024 - 46,151**, vendors register these for proprietary protocols

**Dynamic/private ports - 49,152 - 65,535**, used by computer when it needs a high-number outbound port when using NAT/PAT

**- 20/21 TCP - FTP File Transfer Protocol**

Unencrypted, transfers files from host to host - transfer (20), command (21)

**- 22 TCP/UDP - SSH Secure Shell, SCP Secure Copy, SFTP Secure FTP**

Remotely control of network devices, securely copy files, securely transfer. v2 .0 great.

Requires a server (daemon) to be run on one device and a client on the other.

**- 23 TCP/UDP - Telnet**

Unencrypted, remotely administer network devices (do not use)

**- 25 TCP - SMTP Simple Mail Transfer Protocol**

Send email over the internet

**- 49 TCP/UDP - TACACS+ Terminal Access Controller Access-Control System Plus**

Handling remote authentication and related services for NAC through a centralized server - Cisco-proprietary.

**- 53 TCP/UDP - DNS Domain Name Service**

Resolve hostnames (e.g. URLs) to IPs and vice versa

**- 67/68 UDP - DHCP Dynamic Host Configuration Protocol**

Auto-assigns IP addresses to machines.

**- 69 UDP - TFTP Trivial FTP**

A simplified version of FTP to put/get a file to/from a remote host (uses UDP so connectionless and fast, with no security)

**- 80 TCP - HTTP Hypertext Transfer Protocol**

Unencrypted, transmit web page data.

**- 88 TCP/UDP - Kerberos**

Network authentication using a system of tickets with a Windows domain

**- 110 TCP - POP3 Post Office Protocol**

Unencrypted, receive email from a mail server

**- 119 TCP - NNTP Network News Transfer Protocol**

Transport Usenet articles

**- 135 TCP/UDP - RPC Remote Procedure Call**

Locate DCOM ports to request a service from a program on another computer on the network, used in Windows-based networks

**- 137/138/139 TCP/UDP - NetBIOS**

Conduct name querying, sending of data, and other functions over a NetBIOS connection

**- 143 TCP - IMAP Internet Message Access Protocol**

Unencrypted, receive email from a mail server with more features than POP3

**- 161 UDP - SNMP Simple Network Management Protocol**

Remotely monitor network devices. Incorporated into network management and monitoring systems. v1/v2 = insecure because of community strings. v3 = encryption, hashing, authentication. In-band - send over the same network, easier, cheaper, less secure. Out-of-band - secondary network to increase security, cannot be seen by users on the network.

**Managed devices** - computers and other network-attached devices monitored through the use of agents by a network management system

**Agent -** software that is loaded on a managed device to redirect information to the network management system

**Network Management Systems -** software run on one or more servers to control the monitoring of network-attached devices and computers

**- 162 TCP/UDP - SNMPTRAP**

Send Trap and InformRequests to the SNMP Manager on a network

**- 389 TCP/UDP - LDAP Lightweight Directory Access Protocol**

Maintain directories of users and other objects e.g. Active Directory

**- 443 TCP - HTTPS Hypertext Transfer Protocol Secure**

Encrypted HTTP over SSL/TLS connection

**- 445 TCP - SMB Server Message Block**

Provide shared access to files and other resources on a network

**- 465/587 TCP - SMTPS Simple Mail Transfer Protocol Secure**

Encrypted SMTP over SSL/TLS

**- 500 UDP - ISAKMP Internet Security Association and key Management Protocol**

Key exchange for VPNs.

**- 514 UDP - Syslog**

Conduct logging, especially for routers and firewalls

**- 636 TCP/UDP - LDAPS Lightweight Directory Access Protocol Secure**

Encrypted LDAP over SSL/TLS

**- 860 TCP - iSCSI (‘eye scuzzy’)**

Links data storage facilities over IP

**- 989/990 TCP - FTPS File Transfer Protocol Secure**

Encrypted FTP over SSL/TLS

**- 993 TCP - IMAPS**

Encrypted IMAP over SSL/TLS

**- 995 TCP - POP3S**

Encrypted POP3 with SSL/TLS

**- 1433 TCP - Ms-sql-s**

Microsoft SQL database queries

**- 1645/1646 UDP - RADIUS (alt ports) Remote Authentication Dial-In User Service**

(alt ports) Authentication/authorisation (1645) and accounting (1646)

**- 1701 UDP - L2TP Layer 2 Tunnel Protocol**

Unencrypted, underlying VPN protocol, need to pair with IPSec

**- 1723 TCP/UDP - PPTP Point-to-Point Tunneling Protocol**

Encrypted, underlying VPN protocol

**- 1812/1813 UDP - RADIUS Remote Authentication Dial-In User Service**

Used for 802.1X when connecting a device to a LAN, authentication/authorisation (1812) and accounting (1813)

**- 3225 TCP/UDP - FCIP Fibre Channel IP**

Encapsulate Fibre Channel frames within TCP/IP packets

**- 3260 TCP - iSCSI Target**

Listening port for iSCSI targeted devices when linking data storage facilities over IP

**- 3306 TCP - MySQL**

MySQL queries.

**- 3389 TCP/UDP - RDP Remote Desktop Protocol**

Remotely view and control other Windows systems via a GUI (NB 389 is LDAP). Does not provide authentication so need digital certificates or SSL.

**- 3868 TCP - Diameter**

Advanced AAA protocol, replacement for RADIUS

**- 5900 TCP - Virtual Network Computing (VNC)**

Platform-independent RDP - should only be used internally, so VPN into your org first.

**- 6514 TCP - Syslog over TLS**

Encrypted syslog (NB 514 is syslog)

Many of these are **unnecessary ports** and must only be opened when used.

**- Domain Name System Security Extensions (DNSSEC)**

Encrypted digital signatures when passing DNS information between servers to prevent DNS poisoning.

**- Secure/Multipurpose Internet Mail Extensions (S/MIME)**

Standard that provides cryptographic security for email. Authentication - Integrity - Non-repudiation. NB: can also encrypt malware, a lot of email gateways will load up users’ private keys to decrypt so malware cannot bypass security systems.

**- Secure Real-time Transport Protocol (SRTP)**

**- IPSec**

**- Secure Association (SA)**

Establishment of secure connections and shared security information using certificates or cryptographic keys.

**- Authentication header (AH)/Encapsulating Security Payloads (ESP)**

**Authentication header (AH)** - Protocol used in IPSec that provides integrity and authentication.

**Encapsulating Security Payloads (ESP)** - provides integrity, confidentiality, and authenticity of packets by encapsulating and encrypting them.

**- Tunnel/transport**

**Transport** - host-to-host transport mode only uses **encryption of the payload of an IP packet but not its header -** like a lorry, the back is secured with a key but the front cab (header) is not. Should only be used on a private network.

**Tunnel** - End to end network tunnel which **encrypts the entire IP packet** (payload and header) - transmissions between networks.

**• Use cases**

**- Voice and video**

**- Time synchronization**

**- Email and web**

Email Server - frequent target of attack (Windows - Microsoft Exchange), securely configured, spam filtering, AV for server and all attachments

Web Server - Open to the internet, put in the DMZ. Firewalled, monitored, logged, patched. (Windows - IIS, Mac/Linux - Apache).

**- File transfer**

File Server - encrypted, monitoring/logging, HIDS, DLP, hardening/patching

FTP Server - file server to download. Allows anonymous login. Secure for internal use. Force encrypted connection over TLS. **FTP port 20/21, FTP/S port 990, SFTP port 22 (same as SSH).**

**- Directory services**

Domain controller - server that acts as a central repository of all the user accounts and their associated passwords for the network - Microsoft - Active Directory, Linux - LDAP. Targeted for privilege escalation and lateral movement. Kerberos, Golden Ticket attack.

**- Remote access (Remote Access Service - RAS)**

Service that enables dial-up and VPN connections to occur from remote clients.

**- Domain name resolution**

**- Routing and switching**

**- Network address allocation**

**- Subscription services**

**3.2 Given a scenario, implement host or application security solutions.**

**• Endpoint protection**

Endpoint = any device we connect to the network. Need to keep machine up to date with patches

**- Endpoint Protection Platform (EPP)**

Software agent and monitoring system that performs multiple security tasks such as antivirus, HIDS/HIPS, firewall, DLP, and file encryption. What we think of as an ‘antivirus’ is actually an EPP as it does more e.g. McAfee, Bitdefender, Carbon Black, CrowdStrike, SentinelOne, Symantec etc.

**- Antivirus (AV)**

Software capable of detecting and removing malware, viruses, worms, trojans, rootkits, adware, spyware, password crackers, network mappers, DoS tools, and others.

**- Anti-malware**

Best to detect worms, trojans, and ransomware (delivered as trojan) - often also contain firewalls.

**- Anti-spyware**

**- User and Entity Behaviour Analytics (UEBA)**

System that can provide automated identification of suspicious activity by user accounts and computer hosts. Baseline of good knowledge and compare activity to that baseline. Heavily dependent on AI and ML e.g. Microsoft Advanced Threat Analytics, Splunk User Behaviour Analytics.

**- Endpoint detection and response (EDR)**

Software agent that collects system data and logs for analysis by a monitoring system to provide early detection of threats. Less on signature-detection and more on entity and behaviour analysis. Does not prevent an initial execution. Provides runtime and historical visibility into a compromise - and cant help respond when detection is confirmed.

**- Data Loss Prevention (DLP) (aka Information Leak Protection ILP or Extrusion Prevention Systems EPS)**

**(4 types total - host, network, storage, cloud)**

Monitors the data of a system while in use, in transit, or at rest to detect attempts to steal the data

Software-based client that monitors the data in use on a computer and can stop a file transfer or alert an admin of the occurrence

Detection mode or prevention mode

Could make it so you manually need to review data being sent out.

**- Next-generation firewall (NGFW)**

**- Advanced Threat Protection (ATP), Advanced Endpoint Protection (AEP), Next-generation Antivirus (NGAV)**

Marketing term for a hybrid of EPP, EDR, UEBA.

**- Host-based intrusion prevention system (HIPS)**

Can stop malicious activity from happening

**- Host-based intrusion detection system (HIDS)**

Device or software application that monitors a system or network and analyses the data passing through in order to identify an incident or attack by looking for unexpected behaviour or drastic changes. 3-types of analysis:

**Signature-based** - specific string of bytes triggers an alert

**Policy-based** - Relies on specific declaration of the security policy (e.g. no telnet allowed)

**Anomaly-based (statistic-based)** - analyses the current traffic against an established baseline and triggers an alert if outside the statistical norm e.g. out of hours downloads

True positive

True negative

False positive

False negative

HIDS can only alert and log suspicious activity

**- Host-based firewall**

Checks network traffic against rules and policies it has been assigned.

Software application that protects a **single computer** from unwanted internet traffic.

Windows Firewall - basic version in control panel, also advanced version Windows Defender Firewall with advanced security - terminal - wf.msc - good for enterprise

Mac - basic firewall in system preferences. PF (Packet Filter) in terminal, advanced firewall. IPFW (Internet Protocol Firewall - old version).

Linux - iptables from terminal.

Hardware network-based firewall often found in a router.

**• Boot integrity**

Firmware, the software written into the hardware of the machine. Need **trusted firmware**.

**Firmware exploit** gives an attacker an opportunity to run any code at the highest level of CPU privilege.

**- Boot security/Secure Boot/Unified Extensible Firmware Interface (UEFI)**

Advanced version of BIOS - has a GUI and mouse.

Loads BIOS to decide how to boot the rest of the machine e.g. load from disk, USB etc.

-Flash the BIOS - updates to the most recent firmware.

-Use a BIOS password

-Configure boot order - prevents people from booting from CD/USB.

-Disable the external ports and devices you don’t use

-Enable the **secure boot** option - loads public key from TPM to verify code of OS to make sure it has been signed by the vendor and has not been modified.

**- Measured boot**

Gathers secure metrics to validate the boot process in an attestation report e.g. how long it takes to boot, how much CPU it uses.

**- Boot attestation**

A claim that the data presented in the report is valid by digitally signing it using the TPM’s private key

**- eFUSE**

Means for a software or firmware to permanently alter the state of a transistor on a computer chip - anti-tamper mechanism (FPGA)

**- Trusted Firmware Update**

A firmware update that is digitally signed by the vendor and trusted by the system before installation

**• Database**

**- Tokenization**

**- Salting**

**- Hashing**

**• Application security**

Implement web browser policies - e.g. disable flash, require adblock, no passwords can be stored etc.

**- Secure cookies**

When a cookie has the **secure attribute**, the user agent includes the cookie in an HTTP request only if the request is transmitted over a secure channel, usually HTTPS.

**Tracking cookie** - used by spyware to track your habits by following you around the internet to see what websites you visit

**Session cookie** - the type that saves that you’re authenticated to your email, social media accounts etc. or what is in your shopping cart.

**Locally Shared Object (LSO)** - known as flash cookies they are stored in Windows user profile under the FLash folder inside of AppData folder.

**- Hypertext Transfer Protocol (HTTP) headers**

**- Allow list (whitelist) / Block/Deny list (blacklist)**

Only applications that are on the whitelist are allowed to be run by the operating system while all other applications are blocked. Vice versa for blacklist. Can be centrally managed (e.g. Active Directory)

**- Secure coding practices**

**- Code signing**

Applications should be deployed using code signing to ensure that the program is not changed inadvertently or maliciously prior to delivery to an end user.

Use digital signature with private key and hashing.

**- Input validations**

Never Trust User Input - all input from a user should undergo input validation prior to allowing it to be utilised by an application.

**Defense in Depth** - layering of security controls is more effective and secure than relying on a single control

**Minimise attack surface** - reduce code, eliminate unneeded functionality, and require authentication to run additional plugins

**Create secure defaults** - default installations should include secure configurations instead of requiring an admin or user to add in additional security

**Fail Securely -** applications should be coded to properly conduct error handling for exceptions in order to fail securely instead of crashing

**Fix security issues -** if a vulnerability is identified then it should be quickly and correctly patched to remove the vulnerability.

**- Static code analysis**

Source code is reviewed manually or with automatic tools without running the code.

**-- Manual code review**

**- Dynamic code analysis**

Analysis and testing of a program occurs while it is being executed or run

**- Fuzzing**

**Injection of randomised data** into a program in an attempt to find system failures, memory leaks, error handling issues, and improper input validation.

**• Hardening**

**- Open ports and services**

Close unnecessary open ports and terminate unnecessary running services.

**- Registry**

**- Disk encryption**

Hardware vs software. Hardware = SED (See below). Software includes FileVault on Mac, BitLocker on Windows, and other softwares like TrueCrypt and VeraCrypt. Has a performance impact as the drive needs to be decrypted to use.

**- OS**

Windows - Use NTFS (New Technology File System) over FAT32, because it is more secure and supports logging, encryption, larger partition sizes, and larger file sizes.

Mac - APFS

Linux - ext4

**- Patch management**

1. Planning, 2. Testing, 3. Implementing, and 4. Auditing of software patches.

1. Planning - verify it is compatible with your systems and plan for how you will test and deploy it. Microsoft Baseline Security Analyser,

2. Testing - need to test it before automating its deployment. To make sure it doesn’t break the wider system.

3. Implementing - Manually or automatically deploy the patch to all your clients to implement it. Microsoft System Center Configuration Management. Large organisations centrally manage updates through an update centre instead of Windows Update to give more control. Disable Windows Update by stopping wuauserv service from running.

4. Auditing - important to audit the client’s status after patch deployment. Makes sure patches have been installed properly.

There are so many patches out there we need to make sure they are not going to break things.

Patch vs hotfix - interchangeable these days, though originally a hotfix meant you didn’t need to reboot.

* Security update - Patch that is issued for a product-specific security-related vulnerability
* Critical update - addressing a critical, non-security bug
* Service Pack - grouping of other patches, tested and working together
* Windows Update - recommended update to fix a non-critical problem that users have found, as well as to provide additional features and capabilities
* Driver Update - fix a security issue or add a feature to a support piece of hardware

**-- Third-party updates**

**-- Auto-update**

Windows 10 users Windows Update to auto-update

**- Secure Processing**

A mechanism for ensuring the confidentiality, integrity and availability (CIA) of software code and data as it is executed in volatile memory.

**Processor Security Extensions** - Low-level CPU changes and instructions that enable secure processing. AMD = Secure Memory Encryption (SME) or Secure Encrypted Virtualisation (SEV). Intel = Trusted Execution Technology (TXT) or Software Guard Extensions (SGX).

**Trusted Execution** - The CPU’s security extensions invoke a TPM and secure boot attestation to ensure that a trusted operating system is running.

**Secure Enclave** - extension that allows a trusted process to create an encrypted container for sensitive data. Prevents e.g. buffer overflow attacks.

**Atomic Execution** - Certain operations should only be performed once or not at all, such as initialising a memory location. Make sure it cannot be run twice, preventing e.g. buffer overflow and race conditions.

**Bus Encryption** - Data is encrypted by an application prior to being placed on the data bus.

**• Self-encrypting drive (SED)/full-disk encryption (FDE)**

Storage device that performs whole disk encryption by using embedded hardware. Very fast, very expensive. Looks like a hard drive. Need to be trusted firmware.

**- Opal**

**• Hardware root of trust**

A cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics e.g. TPM

Secured I/O - RNG, RSA keygen, SHA1 hash-gen, encryption-decryption sig engine

Persistent Memory - Endorsement Key (EK), Storage Root Key (SRK)

Versatile Memory - Platform Configuration Registers (PCR), Attestation Identity Keys (AIK), storage keys

**• Trusted Platform Module (TPM)**

Hardware chip residing on the motherboard that contains an encryption key. Acts as a keyring for all the keys on the system used for encryption, authentication, signatures etc. If you remove the hard drive from the motherboard, you need to decrypt it first on that computer, otherwise a different TPM will not be able to decrypt it. Many systems allow a backup key in case the TPM is broken. If the motherboard does not contain a TPM, you can use an external USB device as a key or a commercial device like a YubiKey.

**• Sandboxing**

Utilises separate virtual networks to allow security professionals to test suspicious or malicious files

**3.3 Given a scenario, implement secure network designs.**

**• Load balancing**

**- Active/active**

**- Active/passive**

**- Scheduling**

**- Virtual IP**

**- Persistence**

**• Network segmentation**

**- Virtual local area network (VLAN)**

Segment network

Reduce collisions

Organise the network

Boost performance

Increase security

‘VLAN hopping’ attack

**Switch spoofing** - attacker configures their device to pretend it is a switch and uses it to negotiate a trunk link to break out of a VLAN - prevent with - disable dynamic trunking protocol (DTP)

**Double tagging -** attacker adds an additional VLAN tag to create an outer and inner tag. Prevent with - move all ports out of the VLAN group.

**- Screened subnet (previously known as demilitarized zone DMZ)**

Focused on providing controlled access to publicly available servers that are hosted within your organisational network e.g. self-hosted email and web servers.

A segment isolated from the rest of a private network by one or more firewalls that accepts connections from the Internet over designated ports.

Everything behind the DMZ is invisible to the outside network.

Good place to put IDS because it is common for attackers to compromise DMZ and pivot into the main network.

Internet-facing host - any host that accepts inbound connections from the internet.

Machines in the DMZ are not fully trusted because they are internet-facing - we use bastion hosts and jumpbox to communicate with them (see below)

**- East-west traffic**

**- Extranet**

Specialised type of DMZ that is created for your partner organisations to access over a wide area network.

**- Intranet**

Can expand internal networks across multiple areas e.g.by using VPNs.

**- Zero Trust**

**• Virtual private network (VPN)**

Allows end users to create a tunnel over an untrusted network and connect remotely and securely back to the enterprise network.

**VPN Concentrator** - specialised hardware device that allows for hundreds of simultaneous VPN connections for remote workers.

Always use when connecting to WiFi, even your own.

**- Always-on**

**- Split tunnel vs. full tunnel**

**Split tunnel** - uses internal traffic over VPN by external traffic over their own internet connection - efficient from bandwidth perspective, but security risk because now company traffic can connect to the internet via this VPN tunnel and the remote worker’s device - need to set up VPN concentrator properly as well as network segmentation.

**Full-tunnel** - all traffic encrypted but uses more bandwidth

**- Remote access/client-to-site vs. site-to-site**

**Remote access/client-to-site** - One person connecting back to the larger site.

**Site-to-site** - instead of buying a dedicated lease line from the ISP, you can create a VPN tunnel between sites over the internet. Routers are encrypted so all data sent is secure.

**- SSL/TLS**

Used by HTTPS to make a VPN when you connect.

**- HTML5**

**- Point to Point Tunnelling Protocol (PPTP)**

Protocol that encapsulates (Point to Point protocol) PPP packets and ultimately sends data as encrypted traffic. CHAP-based authentication, making it vulnerable to attacks.

**- Layer 2 tunneling protocol (L2TP)**

Connection between two or more computers of devices that are not on the same private network. Not secure on its own, no encryption - paired with IPSec for encryption.

**- IPSec**

A TCP/IP protocol that authenticates and encrypts IP packets and effectively secures comms between devices using this protocol. Provides **confidentiality** (encryption), **integrity** (hashing), and **authentication** (key exchange).

**Internet Key Exchange IKE -** method used by IPSec to create a secure tunnel by encrypting the connection between authenticated peers.

Main - 3 exchanges

Aggressive - 3 packets

Quick -

**• DNS**

**• Network access control (NAC)**

Security technique in which devices are scanned to determine its current state prior to being allowed access onto a given network. If it fails, it can be put into a digital quarantine zone where it can have its AV and OS updated. Goes up to layer 7 of OSI.

**- Agent and agentless aka persistent and non-persistent**

Persistent agent - a piece of software that is installed on the device requesting access to the network. Works well in a corporate environment, not in BYOD.

Non-persistent agentless - scans a device remotely or is installed and subsequently removed after the scan.

Hardware or software solution.

**• Out-of-band management**

**• Port security**

**- Broadcast storm prevention**

**- Bridge Protocol Data Unit (BPDU) guard**

**- Loop prevention**

**- Dynamic Host Configuration Protocol (DHCP) snooping**

**- Media access control MAC filtering**

Prevent access beyond the firewall based on their MAC addresses.

**• Network appliances**

**- Jump servers / jumpbox**

A hardened server that provides access to other hosts within the DMZ.

Admin connects to jumpbox and jumpbox connects to hosts in the DMZ.

Can use a virtual machine. Destroy when done. Then recreate.

Need to make sure it is maximally hardened and have the least amount of software on them.

**- Bastion hosts**

Hosts or servers in the DMZ which are not configured with any services that run on the local network

**- Proxy servers**

Device that acts as a middleman between a device and a remote server. On a corporate network all outside requests will be made via a proxy server, you would not directly connect from your own device. Allows the admins to look through TLS security.

**-- IP Proxy (forward proxy)**

Used to secure a network by keeping its machines anonymous during web browsing (using NAT).A forward proxy hides the identity of clients

**-- Reverse**

A reverse proxy hides the identity of servers. So outside requests connect to the proxy server that then requests data from content server and returns it.

**-- Content Filtering**

Type of proxy that blocks access to certain sites.

**-- Caching Proxy**

Attempts to serve client requests by delivering content from itself without actually contacting the remote server e.g. if everyone is reading the news it will show that same copy, saves bandwidth, increases speed. HTTP proxy, for about 24 hours. Not as effective as they used to be because of Web 2.0 e.g. social media profiles are different for each person.

Disable proxy Auto-Configuration (PAC) files for security, could be used to redirect traffic to attacker’s proxy.

**-- Web Security Gateway**

Device that scans for viruses, filters unwanted content e.g. ads, and performs data loss prevention functions.

**- Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)**

Installed on or connected to the switch, either before or after the firewall, to analyse all traffic passing through it. Best to have the firewall filter first to cut down on traffic to analyse.

**NIDS** - attempts to detect - use promiscuous mode, sees all traffic on the network, connected to the span port of switch to see all traffic. Signature-based/heuristics.

**NIPS** - attempts to remove/detain/redirect malicious traffic. Should be installed in-line of the network flow. Should it fail-open (less secure) or fail-shut (DoS yourself)? Most orgs choose fail-open and use other defensive measures e.g. firewalls. Can also work as a protocol analyser (like WireShark) - packet sniffer. Can help it work out what normal is - can reduce performance.

**-- Signature-based**

Analysed for **predetermined** attack patterns - least false positives.

**-- Heuristic/behavior**

Activity is evaluated based on the **previous behaviour** in comparison to current activity - there are a lot of false positives as there are so many ways for apps to interact.

**-- Anomaly**

**Baseline** is established and any network traffic outside the baseline is evaluated.

**-- Inline vs. passive**

**- HSM**

**- Sensors**

**- Collectors**

**- Aggregators**

**- Firewalls**

Screen traffic between two portions of a network.

**-- Web application firewall (WAF) / Application-layer gateway**

Conducts an in-depth inspection based upon the application being used (layer 7 firewall) - whereas most firewalls operate at layers 3 (IP addresses) and 4 (ports). Can protect against SQL injection, XSS etc.

**-- Unified threat management (UTM) aka Next generation firewall (NGFW)**

Relying on a single firewall is not enough. Combination of network security devices that are added to a network to provide more defense in depth than with a single device. Might include a firewall, NIDS/NIPS, content filter, anti-malware, DLP, and VPN. Nice GUI instead of CLI. Can replace the firewall and be placed as an outer perimeter device.

**-- Circuit-level gateway**

Operates at the session layer (4) and only inspects the traffic during the establishment of the initial session over TCP/UDP.

**-- Network address translation (NAT) gateway**

Process of changing an IP address while it transits across a router. Private to public IP address mapping. Can also hide our Network IPs.

**Port Address Translation (PAT)** - router keeps track of requests from internal hosts by assigning them random high number ports for each request. Hides private IP from internet just one single public IP.

**Private IPs: 10.x.x.x, 172.16.x.x - 172.31.x.x, 192.168.x.x -** cannot be sent over the internet, your router will use NAT/PAT to translate it.

**NAT Filtering -** filters traffic based upon the ports being utilised and the type of connection TCP/UDP.

**-- Content/URL filter**

**-- Packet filtering - stateful vs stateless**

Inspects each packet passing through the firewall and accepts or rejects it based on the rules.

Stateless - accept/reject based on IP/port.

Stateful - tracks the requests leaving through the firewall, temporarily opens up port numbers - eliminates IP spoofing by reading headers.

**-- Open-source vs. proprietary**

**-- Hardware vs. software vs. embedded**

Software - run as software on an endpoint.

Hardware - a standalone piece of equipment you plug into your network.

Embedded - inside something like a router.

**-- Appliance vs. host-based vs. virtual**

**• Access control list (ACL)**

An ordered set of rules that a router uses to decide whether to permit or deny traffic based upon given characteristics e.g. source/destination IP/port. Goes to layer 3 of OSI.

**IP Spoofing** is used to trick a router’s ACL into thinking you are a different IP.

**Rule - protocol - source - destination - port**

**Explicit allow** e.g. allow TCP 10.0.0.2 any port 80 (allows TCP connections from 10.0.0.2 to any address via port 80 (HTTP))

**Explicit deny** - e.g. deny TCP any any port 23 (denies all access to all address using TCP over port 23 (telnet))

**Implicit deny** - ACL processes rules top to bottom, so at bottom put this blocks everything else, most firewalls do this today by default e.g. deny TCP any any port any

**• Route security**

**• Quality of service (QoS)**

Availability.

**• Implications of IPv6**

**• Port spanning/port mirroring**

One or more switch ports are configured to forward all of their packets to another port on the switch - SPAN port

**- Port taps**

Physical device that allows you to intercept the traffic between two points on the network.

**• Monitoring services**

**• File integrity monitors**

An internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline. Checks the hashes to make sure there have been no unexpected changes.

**3.4 Given a scenario, install and configure wireless security settings.**

**• Cryptographic protocols**

**- Wired Equivalent Privacy (WEP)**

Do not use it! Broken, due to its 24-bit initialisation vector IV.

**- WiFi Protected Access(WPA)**

Flawed, TKIP, RC4

**- WiFi Protected Access 2 (WPA2)**

High level of wifi security - uses CCMP, 128 bit AES

**- WiFi Protected Access 3 (WPA3)**

News and best wifi security - 256 bit AES (enterprise mode) - SAE, always using new keys

**- Counter-mode/CBC-MAC Protocol (CCMP)**

**• Authentication protocols**

**- IEEE 802.1X**

See diff section

**- Extensible Authentication Protocol (EAP)**

**-- EAP-MD5**

**-- EAP-TLS**

**-- EAP-TTLS**

**-- EAP-FAST**

**-- Protected Extensible Authentication Protocol (PEAP)**

**-- Lightweight Extensible Authentication Protocol (LEAP)**

See diff section for all EAP.

**- Remote Authentication Dial-in User Service (RADIUS) Federation**

See diff section.

**• Methods**

**- Pre-shared key (PSK) vs. Enterprise vs. Open**

**- Simultaneous Authentication of Equals (SAE)**

WPA3 removes pre-shared key, prevents MitM attacks. Replaced with SAE, secure password-based authentication - forward secrecy, won’t be compromised in the future.

1 WAP and client use public key system to generate pair of long-term keys

2 WAP and client exchange one-time use session key using e.g. Diffie-Hellman

3 WAP sends the client messages and encrypts them using key from step 2

4 Client decrypts messages received using same one-time session key

5 Process repeats steps 2-4 to ensure forward secrecy

**- WiFi Protected Setup (WPS)**

Flawed, can be hacked, where you press a button on your router. Always disable.

**- Captive portals**

**• Installation considerations**

**On the exam, disable SSID broadcast.**

**- Site surveys**

Analyse to choose best WAP placement.

**- Heat maps**

2.4Ghz further distance than 5GHz

**- WiFi analyzers**

**- Channel overlaps**

Wifi

**- Wireless access point (WAP) placement**

Omnidirectional, goes in all directions less secure vs. bi/unidirectional.

**- Controller and access point security**

**3.5 Given a scenario, implement secure mobile solutions.**

**• Connection methods and receivers**

**- Cellular**

**- WiFi**

**- Bluetooth**

Creates a shared **link key** to encrypt the connection.

**- NFC**

**- Infrared**

**- USB**

**- Point-to-point**

**- Point-to-multipoint**

**- Global Positioning System (GPS)**

Can be jammed as the power from the satellite is weak.

**- RFID**

**• Mobile device management (MDM)**

Centralised software solution that allows system administrators to create and enforce policies across its mobile devices.

Apple is more secure as they update their software faster than third-party companies adding patches to their version of Android.

But can we load this onto people’s BYOD?

**- Application management**

**- Content management**

**- Remote wipe, remote lock**

E.g. find my iPhone, in case of theft/loss.

**- Geofencing**

Puts a virtual fence around a location. Allows monitoring for when the device has entered/left the area. Can alert on theft, or only allow access to certain apps in certain places.

**- Geolocation**

E.g. find my iPhone, in case of theft/loss.

**- Screen locks**

**- Push notifications**

**- Passwords and PINs**

**- Biometrics**

Face ID / Touch ID, more secure.

**- Context-aware authentication**

Process to check the user’s or system’s attributes prior to allowing it to connect - restrict authentication based on the time of day or location

**- Containerization**

**- Storage segmentation**

Operating a clear separation between personal and company data on a single device. Multiple ways of doing it e.g. technically, an app that is a virtual environment to all your work. Or administratively, perhaps two mail apps where you are not allowed to load the profile into the other one.

**- Full device encryption**

Protects data in the case of device theft/loss.

**• Mobile devices**

**- MicroSD hardware security module (HSM)**

**- MDM/Unified Endpoint Management (UEM)**

**- Mobile application management (MAM)**

**- SEAndroid**

**• Enforcement and monitoring of:**

**- Third-party application stores**

Should only download apps from official Apple Story or Play Store, as these are checked by Apple/Google and digitally signed. Sometimes malware can get past though.

**- Rooting/jailbreaking**

Bypasses natural system protections that come from having your device managed by Apple/Android manufacturer. Allows any app to be installed.

**- Sideloading**

**- Custom firmware**

Specific to Android - modification of the standard OS, may not be updated often with patches.

**- Carrier unlocking**

**- Firmware over-the-air (OTA) updates**

**- Camera use**

**- SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS)**

**- External media**

**- USB On-The-Go (USB OTG)**

**- Recording microphone**

**- GPS tagging**

**- WiFi direct/ad hoc**

**- Tethering**

**- Hotspot**

**- Payment methods**

**• Deployment models**

**- Bring your own device (BYOD)**

Bring your personal devices and connect it to the corporate network. Brings a lot of security issues. People can bring and introduce malware. Benefits are that they don’t need to buy and manage devices like laptops and phones. Issues, who owns the data on the device? Sometimes called ‘Bring Your Own Disaster’ - you need to have storage segmentation and strong security controls.

**- Choose your own device (CYOD)**

Choice of a few different devices, and the company will run MDM and DLP etc. (Recorded Future).

**- Corporate-owned personally enabled (COPE)**

Company provides the device but can still install your own apps.

**- Corporate-owned**

Corporation provides, owns, and manages devices.

**- Virtual desktop infrastructure (VDI)**

Cloud - allows a cloud provider to offer a full desktop operating system to an end user from a centralised server. Security improvements - make a new VDI every time you log on and destroy it afterwards, destroying the attacker’s persistence.

**3.6 Given a scenario, apply cybersecurity solutions to the cloud.**

**• Cloud security controls**

Collocated data - if the server is compromised (e.g. via a different tenant on the machine) then your data could be compromised too.

**- High availability across zones**

**- Resource policies**

**- Secrets management**

**- Integration and auditing**

**- Storage**

**-- Permissions**

**-- Encryption**

**-- Replication**

**-- High availability**

**- Network**

**-- Virtual networks**

**-- Public and private subnets**

Act of creating subnetworks logically through the manipulation of IP addresses.

Have different policies and monitoring for each subnet, logically break up into business roles e.g. printer subnet, guest subnet, production data subnet

Compartmentalised - increased security

Efficient Use of IP addresses

Reduced broadcast traffic

Reduced collisions

**-- Segmentation**

**Secure Enclave** - split the data into different secure enclaves, each with their own security policies, access control etc. Azure does this.

**Secure Volume** - data at rest is encrypted, and mounted and unencrypted when required.

**-- API inspection and integration**

**- Compute**

**-- Security groups**

**-- Dynamic resource allocation**

**-- Instance awareness**

**-- Virtual private cloud (VPC) endpoint**

A private network segment made available to a single cloud consumer without a public cloud - IaaS. Consumer is responsible for configuring the entire system, everything, it is like you own the servers. Typically used to provision internet-accessible applications that need to be accessed from geographically remote sites.

**-- Container security**

**• Solutions**

**- CASB - Cloud Access Security Broker**

Enterprise management software designed to mediate access to cloud services by users across all types of devices. Make sure people are connecting to the right device with the right security. Can enforce SSO, can help scan for malware and rogue devices, can help monitor/audit user activity, can help mitigate data exfiltration (DLP).

Provide visibility into how clients and other network nodes use cloud services.

**Forward proxy** - positioned at edge of client network, will forward to cloud if traffic complies with security policy. Users may be able to bypass this proxy.

**Reverse proxy** - positioned at edge of cloud server, will forward to cloud if traffic complies with security policy. Only works if the cloud application supports a proxy.

**API** - uses the broker’s connections between the cloud service and the cloud consumer. Depending on the API supporting policy functions that the organisation needs.

**- Application security**

**- Next-generation secure web gateway (SWG)**

**- Firewall considerations in a cloud environment**

**-- Cost**

**-- Need for segmentation**

**-- Open Systems Interconnection (OSI) layers**

Please - **1** **Physical**, hub, bit - network cables, radio waves

Do - **2 Data Link**, switch, frame, MAC address - how a connection is established, maintained, transferred over physical layer

Not - **3** **Network**, router, packet, IP address - route information between hosts and networks

Throw - **4 Transport** - TCP/UDP segment (TCP), datagram (UDP) - manages and ensures transmission of packets from host to destination. TCP 3-way handshake, UDP no.

Sausage - **5** **Session** - API, socket - manages the establishment, termination, and synchronisation of a session over a network.

Pizza - **6 Presentation** - SSL, JPEG etc. - translates information (binary) into a format that the sender and receiver both understand.

Away - **7** **Application** - HTTP, SMTP, FTP etc. - layer from which the message is created and sent from. Not app like a program.

**• Cloud native controls vs. third-party solutions**

**3.7 Given a scenario, implement identity and account management controls.**

**• Identity**

**- Identity provider (IdP)**

**- Attributes**

**- Certificates**

**- Tokens**

**- SSH keys**

**- Smart cards**

**• Account types**

**User rights** - permissions assigned to a given user, many different areas e.g. permissions to view files/folders, login hours, printers they can use etc.

**Groups -** collection of users based on common attributes (e.g. work roles).

**Permissions in Windows -** Full Control, Modify, Read & Execute, List Folder Contents, Read, Write

**Linux -** read/write/execute - Owners/Groups/All (U/G/A) (see chmod)

**Privilege Creep** - as people change roles etc. they keep accumulating privileges, too many

**User Access Recertification -** process where each user’s rights and permissions are revalidated to ensure they are correct - hired/fired/promoted.

**Propagation -** occurs when permissions are passed down to a child subfolder from the parent through inheritance. Can disable inheritance in child folders in Windows folder settings.

**Copying -** if you copy a folder then permissions are inherited from the parent folder it is copied **INTO, its NEW parent.**

**Moving -** if you move, then permissions are **retained from its original parent.**

**- User account**

Never use the admin account as a regular user account, should only login to admin when necessary.

**User Account Control (UAC)** - security component in Windows that keeps every user in standard user mode instead of acting like an admin user. Eliminates unnecessary admin-level requests for Windows resources. Reduces risk of malware.

**- Shared and generic accounts/credentials**

**- Guest accounts**

Disable in Windows

**- Service accounts**

**• Account policies**

**- Password complexity**

upper/lower case, numbers, symbols, at least 8 char but 14+ better

Require the user to change the default password.

Required that password is changed frequently every 90 days.

**- Password history**

How many passwords the machine remembers before you can reuse it.

**- Password reuse**

Should not reuse the same password across different logins.

**- Network location**

**- Geofencing**

**- Geotagging**

Puts location/GPS coordinates into photo as metadata, allows anyone to view the location where that photo was taken, could be removed for more security.

**- Geolocation**

**- Time-based logins**

**- Access policies**

**- Account permissions**

**- Account audits**

**- Impossible travel time/risky login**

**- Lockout**

**- Disablement**

**3.8 Given a scenario, implement authentication and authorization solutions.**

**• Authentication management**

**- Password keys**

**- Password vaults**

LastPass etc.

**- TPM**

Trusted Platform Module, see earlier section

**- HSM (Hardware Security Module)**

Physical devices that act as a secure cryptoprocessor during the encryption process. Usually in the form of a plug-in card (to motherboard) or external device that attaches directly to computer or network server. Has features to prevent and identify tampering attempts.

**- Knowledge-based authentication**

**• Authentication/authorization**

**- Lightweight Directory Access Protocol (LDAP)**

**Application layer (7) protocol for accessing and modifying directory services data.** Database used to centralise information about clients and objects on the network. Active Directory is Microsoft’s version.

**- Password Authentication Protocol (PAP)**

Used to **provide authentication** but is not considered secure since it transmits the login credentials **unencrypted**

**- Challenge-Handshake Authentication Protocol (CHAP)**

Used to **provide authentication** by using the user’s password to encrypt a challenge string of random numbers - server sends random string, client hashes string+password, server does the same and if they match then authenticate - prevents sending password in cleartext.

MS-CHAP - Microsoft’s version.

EAP is used these days instead of CHAP. PAP/CHAP were used mainly for dial-up.

**- 802.1x**

IEEE **standardised framework** that defines Port-based Network Access Control (PNAC) and is a **data link layer (2)** authentication technology used to connect devices to a wired or wireless LAN. Defines the EAP protocol.

Can prevent rogue devices. Used in port-based NAC Network Access Control.

**Supplicant**, device requesting access

**Authenticator**, device through which the supplicant is using to access the network e.g. switch, WAP, VPN

**Authentication server**, centralised device that performs the authentication e.g. RADIUS or TACACS+ server.

**- Extensible Authentication Protocol (EAP)**

**Framework of protocols** that allow for numerous methods of authentication including passwords, digital certificates, and public key infrastructure (PKI)

**-- EAP-MD5**

Uses simple passwords for its challenge-authentication - need to use long/strong passwords - one-way due to hashing, does not provide mutual authentication

**-- EAP-TLS**

Uses digital certificates on both client/server for mutual authentication, PKI - immune to password-based attacks as neither side uses a password

**-- EAP-TTLS**

Uses a server-side digital certificate and a client-side password for mutual authentication

**-- EAP-FAST**

Provides Flexible Authentication via Secure Tunnelling (FAST), by using a protected access credential instead of a certificate for mutual authentication

**-- Protected Extensible Authentication Protocol (PEAP)**

Supports mutual authentication by using server certificates and Microsoft’s Active Directory to authenticate clients’ passwords

**-- Lightweight Extensible Authentication Protocol (LEAP)**

Proprietary to Cisco-based networks

**- Remote Authentication Dial-in User Service (RADIUS)**

AAA - Authentication/Authorisation/Accounting - Provides **centralised administration** of dial-up, VPN, and wireless authentication services for 802.1x and the Extensible Authentication Protocol (EAP). Operates at Layer 7 (Application layer). Usually configured on a separate server.

**- Terminal Access Controller Access Control System Plus (TACACS+)**

Cisco proprietary version of RADIUS, not cross-platform.

**- Single sign-on (SSO)**

A default user profile for each user is created and linked with all of the resources needed e.g. Google account, Microsoft account (also federated) (single point of failure however, all accounts breached simultaneously)

**- Security Assertion Markup Language (SAML)**

Attestation model built upon XML used to share federated identity management information between systems - standardisation of SSO

**- OAuth**

**- OpenID**

**An open standard and decentralised protocol** that is used to authenticate users in a federated identity management system - login to Identity Provider (IdP) and use their account at Relying Parties (RP) - easier to implement than SAML

**- Kerberos**

**Authentication protocol** used by windows to provide for two-way mutual authentication using a system of tickets.

Client connects to the domain controller which acts as the **Key Distribution Centre (KDC)**, which authenticates and grants tickets. If authenticates properly, KDC will issue a **Ticket Granting Ticket (TGT)**, TGT then offered to domain controller every time client needs to access a resource, KDC then provides client with session key or service ticket - this is then offered to the resource which will trust all tickets granted by domain controller. Domain controller is a single point of failure - many orgs will have a primary and secondary domain controller for redundancy.

**• Access control schemes**

Methods used to secure data by verifying a user has **permissions** to read, write, delete, or otherwise modify it.

**- Discretionary access control (DAC)**

Access control policy is determined by the owner - commonly-used e.g. they decide who else can read/write it. 1. Every object must have an owner. 2. Each owner has to determine permissions for each object - lots of effort and power.

**- Mandatory Access Control (MAC)**

Access control policy is determined by the computer system. Relies on security **data labels** being assigned to every user (**subject**) and every file/folder/device/network connection (**object**). **Mainly used in high security systems due to its complex configuration.**

Data labels create **trust levels** for all subjects and objects. But they also require a **need-to-know.**

E.g. **military clearance** **levels** - unclassified, confidential, secret, top secret.

**-- MAC type 1 - Rule-based access control**

Label-based access control that defines whether access should be granted or denied to objects by comparing the object label and the subject label.

**-- MAC type 2 - Lattice-based access control**

Utilises complex maths to create sets of objects and subjects to define how they interact.

**- Role-based access control (RBAC)**

Access model that is controlled by the computer system (like MAC) but utilises a set of permissions instead of a single data label to define the permission level. Create roles for each job function and then assign roles to individuals e.g. Admin role, Editor role, Viewer role, Sales team member etc.

**- Attribute-based access control (ABAC)**

Access control model that is **dynamic** and context-aware using IF-THEN statements and tags e.g. if X is in team Y then give access to folder Z.

**- Implicit Deny**

By default, access control policy should deny access unless explicitly stated. Higher-security environment.

**- Conditional access**

**- Privileged access management**

**- Filesystem permissions**

**3.9 Given a scenario, implement public key infrastructure.**

**• Public key infrastructure (PKI)**

The entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption. **PKI is the entire system** that **uses** public key cryptography.

**- Key management**

Refers to how an organisation will generate, exchange, store, and use encryption keys.

**- Registration authority (RA)**

Used to verify information about a user prior to requesting that a certificate authority issue the certificate. Forwards info to CA.

**- Certificate authority (CA)**

Certificate - Digitally-signed electronic documents that bind a public key with a user’s identity. X.509 standard, contains owner’s info and CA’s info. Verisign, Digisign, Microsoft - **root CA**.

Trusted third-party that issues certificates. Purchased for one server at a time.

**- Intermediate CA**

CA that issues certificates that have been signed by a root authority.

**- Certificate revocation list (CRL)**

Online list of digital certificates that the certificate authority has revoked.

**- Online Certificate Status Protocol (OCSP)**

Protocol that allows you to determine the revocation status of a digital certificate using its serial number.

**- Certificate attributes**

**- Certificate signing request (CSR)**

A CSR (certificate signing request) is what is submitted to the CA (certificate authority) to request a digital certificate.

**- Common Name (CN)**

Common Name = Domain Name + Host Name e.g. google.com,

**- Expiration**

Max lifespan is 13 months.

**- Web of Trust**

Decentralised trust model that addresses issues associated with the public authentication of public keys within a CA-based PKi system. Peer-to-peer model.

**• Types of certificates**

‘Invalid or expired’ certificates can be caused by the clock being wrong on the user’s machine.

**- Wildcard**

All subdomains can use the same certificate. Easier to manage. If one server is compromised then all will lose the certificate though.

**- Subject alternative name (SAN)**

Allows a certificate owner to specify additional domains and IP addresses to be supported.

**- Code signing**

**- Self-signed**

Not issued by a CA. Free though.

**- Machine/computer**

**- Email**

**- User**

**- Root**

**- Domain validation**

**- Extended validation**

**• Certificate formats**

**- Basic encoding rules (BER)**

Original rule set governing the encoding of data structures for certificates where several different encoding types can be utilised. Multiple encoding types.

**- Canonical encoding rules (CER)**

Restricted version of BER that only allows the use of one encoding type.

**- Distinguished encoding rules (DER)**

Restricted version of BER that allows one encoding type and has more restrictive rules for length, character strings, storage etc

**- Privacy enhanced mail (PEM)**

Uses DER encoding, file types are: **.pem .cer .crt .key**

**- Personal information exchange (PFX)**

File type **.pfx -** used by Microsoft for release signing

**- Public Key Cryptographic System #12 (PKCS#12)**

File type **.p12**

**- Public Key Cryptographic System #7 (PKCS#7)**

File type **.p7b**

**• Concepts**

**- Online vs. offline CA**

**- 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/TLS handshake. Eliminates additional connection. Alternative to OCSP.

**- 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 - transitive trust**

Family tree - pass down the trust as each certificate issues the next.

**- Key escrow**

When a secure copy of a user’s private key is held in case the user accidentally loses their key. Separation of duties - at least two admins should be present to take a key out of escrow.

**- Key recovery agent**

Specialised type of software that allows the restoration of a lost or corrupted key

**- Certificate chaining**

**- Single-sided**

Only require the server to be validated.

**- Dual-sided**

Both server and the user need a certificate to be validated - uses more processing power so mainly used in high-security environments.

# 4.0 Operations and Incident Response (16%)

**4.1 Given a scenario, use the appropriate tool to assess organizational security.**

**• Network reconnaissance and discovery**

Discovery and documentation of physical and logical connectivity that exists in the network.

#### - tracert/traceroute

**Traces the route.** A network diagnostic command for displaying possible routes and measuring transit delays of packets across an IP network.

**- nslookup/dig**

**Name server lookup, DNS info.** Utility used to determine the IP address associated with a domain name, obtain the mail server settings for a domain, and other DNS info.

**- ipconfig/ifconfig**

Displays all the **network configurations** **of the currently connected network devices** and can modify the DHCP and DNS settings.

**- nmap**

Open-source **network/port scanner** that is used to discover hosts and services on a computer network by sending packets and analysing their responses. Port scanner, network mapping, vulnerability scanner, finds open ports, finds software running.

**- ping/pathping**

Used to **determine if a host is reachable** on an IP network.

**- hping**

Open source packet generator and analyser for the TCp/IP protocol that is used for security auditing and testing of firewalls and networks.

**- netstat**

Displays network connections for TCP, routing tables, networking protocol statistics, used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement. Can find backdoors etc. **Shows what IP addresses/websites you are connected to.**

**- netcat**

Utility for reading from and writing to network connections using TCP or UDP which is a dependable back-end that can be used directly or easily by other programs and scripts. Network tool that can perform port scanning/listening,

**Banner Grabbing** - technique used to gain info about servers and inventory the system or services

**- IP scanners**

**- arp**

Utility for viewing and modifying the local **Address Resolution Protocol (ARP)** **cache** on a given host or server, other machines on your network and their IP/MAC addresses

**- route**

Utility that is used to view and manipulate the IP **routing table** on a host or server (IP routing on your local machine)

**- curl**

Tool to transfer data from or to a server using one of multiple supported protocols e.g. HTTP, FTP, IMAP, LDAP, SMTP etc. etc.

**- theHarvester**

Python script used **as a recon tool to gather OSINT** like gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and Shodan.

**- scanless**

Used to create an exploitation website that can perform open port scans in a more stealth like manner. **Scanning comes from your web server, not you.**

**- dnsenum**

**‘DNS enum’** - Utility that is used for DNS enumeration to locate all DNS servers and DNS entries for a given organisation.

**- ZenMap, SolarWinds**

**Network mapping**

**- Nessus - Qualysguard - AlienVault - sn1per**

**Vulnerability scanners -** Automated scanner that can be used during a pentest to enumerate and scan for vulnerabilities across a network.

**- Cuckoo**

**Malware sandbox** for automating analysis of suspicious files.

**• File manipulation**

**- head**

First 10 lines

**- tail**

Last 10 lines

**- cat (concatenate, entire file)**

Output entire file

**- grep**

Search for string or regex.

**- chmod**

Changes permissions of files/folders in Linux.

R Read = 4

W Write = 2

X Execute = 1

R + W = 6

R + X = 5

W + X = 3

R + W + X = 7

None = 0

E.g. chmod 760 filename

U/Owner = 7 = R + W + X

G/Groups = 6 = R + W

A/All = 0 = None

777 = everyone can do everything

**- logger**

Utility that provides an easy way to add messages to the /var/log/syslog file from the command line.

**- openfiles (Windows)**

Shows all opened files and by what process

**• Shell and script environments**

**- SSH**

Encrypted data transfer between two computers. Shell - CLI.

**- PowerShell**

Microsoft Windows - task automation and config management tool **.ps1**

**- Python**

**- OpenSSL**

Software library for applications that secure comms over computer networks against eavesdropping. SSH uses OpenSSL.

**• Packet capture and replay**

**Network sniffer, packet sniffer** - process of finding and investigating other computers on the network by analysing the network traffic or capturing the packets being sent

**- Tcpreplay**

Replay previously captured network traffic.

**- Tcpdump**

Utility that allows you to capture and analyse network traffic going through your system.

**- Wireshark**

**Protocol analyser** - capture , reassemble, and analyse packets from the network - advanced packet sniffer.

**Promiscuous mode** - network adapter is able to capture all of the packets on the network regardless of the destination MAC address of the frames carrying them.

**Non-promiscuous mode** - can only capture packets that are directly addressed to itself.

**• Forensics**

**- dd**

CLI tool used to copy disk images using a bit by bit copying process. So you can do forensics on a copy of the disk.

**- Memdump**

CLI utility used to dump system memory to the standard output stream by skipping over holes in memory maps - **dump RAM etc.** can output to image.

**- WinHex**

Disk and **hex editor.**

**- FTK imager**

GUI, data preview and imaging tool. Let you work out if you need to do further analysis. Capture and hash system images

**- Autopsy**

GUI and digital forensics platform.

**- EnCase**

**• Exploitation frameworks**

**- MetaSploit Framework (MSF)**

Computer security tool that offers information about software vulnerabilities, IDS signature development, and improves penetration testing. **For Exploiting.**

**- Browser Exploitation Framework (BeEF)**

Tool that can hook one or more browsers and can use them as a beachhead for launching various direct commands and further **attacks against the system** from within the browser context.

**• Password crackers**

**- Cain & Abel, John the Ripper**

**Password recovery tool with a lot of features** that can be used to sniff the network, crack encrypted passwords using a dictionary, brute-force, or cryptanalysis attacks, record VoIP convos, decode scrambled passwords, reveal password boxes, and analyse routing protocols.

**• Data sanitization**

**4.2 Summarize the importance of policies, processes, and procedures for incident response.**

**• Incident response plans**

Set of procedures that an investigator follows when examining a computer security incident.

**• Incident response process**

Program consisting of the monitoring and detection of security events on a computer network and the execution of proper responses to those security events.

**Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned**

**PICERL**

**- Preparation**

Well-planned procedures, good CISO.

Need secure comms for communications. E.g. not VoIP.

**Out-of-band comms** - signals sent between two parties via a method different to their primary method e.g. encrypted messaging.

Up-to-date contact list **-** phone/emails etc. people you need.

At what point do you call people in

What level of incident e.g. email, phone call, 3am in-person.

Do we need to notify management?

Prevent unauthorised release of information.

Who are the affected stakeholders - senior leaders, regulatory bodies, legal, law enforcement, HR, PR

Senior leaders - need to understand the business needs before you make technical decisions.

Regulatory bodies -

Legal - mitigating risks from civil lawsuits.

Law enforcement - senior execs with guidance from legal must choose to do this.

HR - no breaches of employment law or employee contracts

PR - used to manage negative publicity

**- Identification**

Should an event be categorised as an incident. Identify symptoms of a malware infection, Indicators of Compromise

**- Containment**

Quarantine/isolate the infected systems - turn off network card or remove network cable

Disable system restore (if using windows machine) - do not want windows to take snapshots of the malware, must delete old snapshots.

**- Eradication**

Remediate the infected system - use anti-virus/anti-malware software and techniques to remove, anti-virus scanner, booting into safe mode, booting from external device, remove hard drive and hook up as external drive to a clean machine

**- Recovery**

Data restoration, system repair, re-enable offline servers.

**- Lessons learned**

Schedule automatic updates and scans. Enable system restore and create a new restore point. Provided end user security awareness training

**• Computer Security Incident Response Team - CSIRT**

Should be the single point of contact for security incidents, and may be part of the SOC or an independent team. 24/7 on call, or outsourced to MSSP.

**Incident Response Manager** - oversee and prioritise actions. Convey response to C-suite in business language, possibly public-facing to media or law enforcement.

**Security Analysts -** triage and forensic:

**Triage Analyst -** assigned to work on network during the response - filter out false positives by configuring IDS/IPS, monitoring for any new intrusions

**Forensic Analyst -** detective work - what has occurred, recovering artefacts and evidence to build a timeline, to work out what happened

**Threat Researcher -** threat intel, overall context during incident response, up to date on current threats and previous incidents - futurist and historian

**Cross functional support -** management, exec team, HR, lawyer, IT admins.

Providing information to stakeholders e.g. downtime, systems/data affected etc.

**• Exercises**

**- Tabletop**

**- Walkthroughs**

**- Simulations**

**• Attack frameworks**

3 models can be combined with each other

**- MITRE ATT&CK**

**ATT&CK -** Lists and explains Adversary Tactics, Techniques and Common Knowledge (or procedures) aka Tactics, Techniques and Procedures - TTPs

Not linear like the kill chain, it uses a matrix model.

Each individual attacker has their most used TTPs mapped out e.g. APTs.

**pre-ATT&CK** - aligns to the reconnaissance and weaponization phases of the kill chain, as main ATT&CK very focused on exploitation phases

**- The Diamond Model of Intrusion Analysis**

**Adversary vs Victim** on two opposites

**Infrastructure vs Capability** on other two opposites

**Meta-features** - timestamp, phases, result, direction, methodology, resources

Allows analyst to exploit the fundamental relationship between features

Tuple - E = something, algorithm that can be used inside a SIEM

**- Lockheed Martin Cyber Kill Chain**

Describes the **7 stages** by which a threat actor progresses during an attack and how to disrupt them depending on what stage they are at.

**1 - Reconnaissance** - attacker determines what methods to use to complete the phases of the attack. They try to be sneaky, such as passive scanning, to analyse the network and its vulnerabilities.

**2 Weaponization -** attacker couples payload code that will enable access with exploit code that will use a vulnerability to execute on the target system. Coding/creating the malware you want to run, but you haven’t sent it yet.

**3 Delivery -** attacker identifies a vector to transmit the weaponized code to the target environment e.g. email, usb stick.

**4 Exploitation -** weaponized code is executed on the target system by this mechanism e.g. clicking the link in the email is exploitation.

**5 Installation -** enables the weaponized code to run a remote access tool and achieve persistence on the target system.

**6 Command and Control C2 -** weaponized code establishes an outbound channel to a remote server that can then be used to control the remote access tool and possibly download additional tools to progress the attack

**7 Actions on Objectives -** attacker typically uses the access he has achieved to convertyyl collect information from target systems and transfer it to a remote system (data exfiltration) or achieve other goals and motives

**Kill chain analysis -** can be used to identify a defensive courts of ation matrix to counter the progress of an attack at each stage

**• Stakeholder management**

**• Retention policies**

**• Disaster recovery plan**

**• Business continuity plan**

**• Continuity of operations planning (COOP)**

**• Communication plan**

**• Incident response team**

Development of an organised and in-depth plan for problems that could affect the access of data or the organisation’s building e.g. in case of serious incidents - theft, riots, fire, floods, blizzards, earthquakes, hurricanes, natural disasters etc. Needs to be written down.

Contact Info - who to call.

Impact Determination - how bad is it.

Recovery Plan - order and priority.

Business Continuity Plan - how to keep business running.

Copies of Agreements - hard copy/digital, can access from anywhere.

Disaster Recovery Exercises - simulated drills etc.

**4.3 Given an incident, utilize appropriate data sources to support an investigation.**

**• Vulnerability scan output**

**• SIEM dashboards**

**- Sensor**

Endpoint being monitored.

**- Sensitivity**

How much or how little logging - not TOO much

**- Trends**

See trends in the network

**- Alerts**

Set up alerts based on trends or discrete events.

**- Correlation**

Can correlate data across different sources.

**• Log files**

Events that occur, or communications

Config, save, back up, secure, encrypt

Eventually they need overwriting and deleting as too much data eventually.

Saved to a different partition or external server.

Overwrite events - overwrite oldest events if max log file size is reached.

Archived and backed up to different servers - could be compromised otherwise.

WORM - write once read many e.g. a DVD-R. Cannot be altered.

**- Network**

Routers, switches, WAPs

**- System**

Logs the events such as a system shutdown and driver failures

**- Application**

Logs events for the OS and third-party apps

**- Security**

Logs events such as successful and unsuccessful logins to the system

**- Web**

Proxy server logs, what websites looked at, what files are being downloaded

**- DNS**

What requests have been made

**- Authentication**

Logs times users tried to authenticate with a resource that required it, include logins

**- Dump files**

Dumps contents of system memory during crashes.

**- VoIP and call managers**

Skype, zoom, phone calls etc.

**- Session Initiation Protocol (SIP) traffic**

**• syslog/rsyslog/syslog-ng**

**Unix/Linux**. Protocol. Client-server model, de facto standard for transmitting from distributed devices to centralised logging server. Standardised format used for computer message logging that allows for the separation of 1. the software that generates messages, 2. the system that stores them, and 3. the software that reports and analyses them

‘Syslog’ can refer to 1. Protocol, 2. Server, 3. Log entries.

PRI code, header, message portion

**PRI code** - PRIORITY - calculated from facility and severity level of the data

**Header** - contains the timestamp of the event and the hostname

**Message** - contains source process of the event and the related content

Issues - because it uses UDP, there can be delivery issues in congested networks. No encryption or authentication.

Upgrade uses 6514 over TCP for better delivery, also uses TLS for encryption, and MD5/SHA1 hashing authentication and integrity. rsyslog/syslog-ng is upgraded version.

**syslog server -** Centralised monitoring server

**• journalctl**

Logs on Linux. Linux CLI utility used for querying and displaying logs from journald, the systemd logging service on Linux.

**• NXLog**

Multi-platform log management tool that helps to easily identify security risks, policy breaches or analyse operational problems in server logs, operation system logs, and application logs. **Cross platform, open source version of rsyslog.**

**• Bandwidth monitors**

**• Metadata**

Data about data e.g. call was X minutes on Y date to Z person.

**- Email**

Metadata - header info e.g. sending server

**- Mobile**

Who is being called

**- Web**

Which websites are you visiting

**- File**

Who created it, how many times it has been opened etc.

**• Netflow/sFlow**

**- Netflow**

Network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface, including its point of origin, destination, volume and paths on the network. Summarisation - not a packet analyser.

**- sFlow**

‘Sampled flow’ - open-source version of Netflow. Provides a means of exporting truncated packets, together with interface counters for the purpose of network monitoring. E.g. 1% of packets.

**- Internet Protocol Flow Information Export IPFIX**

**Universal standard for e.g. keeping track of usage like for phone data** of export for IP flow information from routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing by defining how IP flow information is to be formatted and transferred from an exporter to a collector.

**• Protocol analyzer output**

**4.4 Given an incident, apply mitigation techniques or controls to secure an environment.**

**• Reconfigure endpoint security solutions**

**- Application approved list**

**- Application blocklist/deny list**

**- Quarantine**

**• Configuration changes**

**- Firewall rules**

**- MDM**

**- DLP**

**Host DLP**

**Network DLP** - software or hardware-based solution that is installed on the perimeter of the network to detect data in transit. Checks all data going out of the network.

**Storage DLP** - Software installed on servers in the data centre to inspect the data at rest - checking it is not being access out of hours or trying to steal

**Cloud DLP** - protects data being store in cloud services, comes with the cloud provider

**- Content filter/URL filter**

Blocks gambling etc. sites

**- Update or revoke certificates**

**• Isolation**

**• Containment**

**• Segmentation**

**• SOAR**

**- Playbooks**

Checklist of actions to perform to detect and respond to a specific type of incident.

**- Runbooks**

**Automated version of a playbook** that leaves clearly defined interaction points for human analysis.

## 4.5 Explain the key aspects of digital forensics.

**Written procedures** are very important. Ensure that personnel handle forensics properly, effectively, and in compliance with required regulations - always done the same way.

1. **Identification -** ensure the scene is safe, secure the scene to prevent evidence contamination, and identify the scope of evidence to be collected. ‘Crime scene’.
2. **Collection -** ensure authorisation to collect evidence is obtained, and then document and prove the integrity of evidence as it is collected.
3. **Analysis -** create a copy of evidence for analysis and use repeatable methods and tools during analysis. CHECKLIST.
4. **Reporting -** create a report of the methods and tools used in the investigation and present detailed findings and conclusions based on the analysis. May need to be called as a witness in court - lawyers will try and pick holes in your arguments.

**Ethics**

1. Analysismust be performed **without bias**
2. Analysismethods must be **repeatable by third-parties**
3. Evidence **must not be changed** or manipulated

Any deviation from these ethics can get your evidence thrown out.

How was access to the system obtained?

What tools have been installed?

What changes to the files were made?

What data has been retrieved?

Was data exfiltrated?

**• Documentation/evidence**

**- Legal hold**

Process designed to preserve all relevant information when lawsuits are reasonably expected to occur. Need liaison with legal knowledge as point of contact with law enforcement.

**- Video**

Record the scene.

**- Admissibility**

**- Chain of custody**

Chain of custody indicates the collection, sequence of control, transfer and analysis. It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer. It demonstrates trust to the courts and to the client that the evidence has not been tampered with.

**- Timelines of sequence of events**

Tool that shows the sequence of file system events within a source image in a graphical format.

**-- Time stamps**

**-- Time offset**

**- Tags**

**- Reports**

**- Event logs**

**- Interviews**

**• Acquisition**

Evidence can be lost when you shut down a computer. Analyse Windows Registry via a memory dump.

**- Order of volatility**

L3 Cache -> temporary: RAM/routing tables/ARP cache/process table -> Swap Files -> HDD/SSD/USB -> Remote logging -> Physical configuration/network topology -> Backups

**- Cache**

**- Random-access memory (RAM)**

**- Swap/pagefile**

**- Disk**

**- OS**

**- Snapshot**

**- Artifacts**

**- Network**

**- Device**

**- Firmware**

**• On-premises vs. cloud**

**- Right-to-audit clauses**

**- Regulatory/jurisdiction**

**- Data breach notification laws**

**• Integrity**

**- Hashing**

**- Checksums**

**- Provenance**

**• Preservation**

**• E-discovery**

### • Data recovery

**• Non-repudiation**

(repudiation = denial of truth) When you have **proof** that someone has taken an action - the user cannot say they did not take the action - logs used here

**• Strategic intelligence/counterintelligence**

**5.0 Governance, Risk, and Compliance (14%)**

**5.1 Compare and contrast various types of controls.**

**• Security Controls**

**Set 1**

**- Physical**

Security measures that are designed to deter or prevent unauthorised access to sensitive information or the systems that contain it.

-Alarm systems, locks, cameras, ID cards, security guards

**- Administrative**

Change the behaviour of people instead of removing the actual risk involved. Contingency plans, disaster recovery plans.

**Procedural** - an organisation chooses to follow these

**Legal/regulatory** - organisation forced to follow by the government - HIPAA healthcare, SOX (Sarbanes-Oxley) finance

**- Technical**

Safeguards and countermeasures used to avoid, detect, counteract, or minimise security risks to our systems

**Set 2 - NIST**

**- (NIST) Managerial**

Focused on decision-making and the management of risk. Policies, procedures, security awareness training (MOST EFFECTIVE CONTROL), vulnerability management program

**- (NIST) Operational**

Focused on the things done by people. Control actions of individuals - user training. Implements the policies of managerial controls.

**- (NIST) Technical**

Logical controls that are put into a system to help secure it.

-AAA, encryption, access control lists (ACLs), intrusion detection systems (IDS), network authentication, MFA.

**Set 3**

**- Preventive/Deterrent**

Security controls that are installed **before** an event happens and are designed to prevent something from occurring e.g. an uninterruptible power supply

Deterrent controls reduce the likelihood of a deliberate attack and is usually in the form of a tangible object or person e.g. cable locks, security guards

**- Detective**

Used **during** the event to find out whether something bad might be happening e.g. CCTV, IDS, logs

**- Corrective**

Used **after** the event occurs - tape backups, incident response, disaster recovery

**Set 4**

**- Compensating**

Used when you cannot meet the requirement for a normal control. NB, this is close to, but not exactly, the original control required by policy. Whatever is left over is residual risk that is accepted risk by the organisation.

**5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.**

**• Regulations, standards, and legislation**

**Standards** - are used to implement a policy in an organisation

**Guidelines** - more flexible suggestions, can make exceptions

**Procedures** -detailed step-by-step instructions that are created to ensure personnel can perform a given action

**Exam:**

**Policies = generic**

**Procedures = specific**

**- General Data Protection Regulation (GDPR)**

Personal data cannot be collected, processed, or retained without the individual’s informed consent. Allows a user to withdraw consent - and can inspect/erase data - ‘right to be forgotten’.

**- National, territory, or state laws**

**- Payment Card Industry Data Security Standard (PCI DSS)**

Any org that deals w credit cards, its a standard, not a law. Need an external audit.

**• Key frameworks**

**- Center for Internet Security (CIS)**

Consensus-developed secure configuration guidelines for hardening (**benchmarks**) and prescriptive, prioritised, and simplified sets of cybersecurity best practices (**configuration guides**). What should we be using when we’re checking our systems are up to standard.

**- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/Cybersecurity Framework (CSF)**

**NIST Risk Management Framework RMF** - Developed for the federal government. A process that integrates security and risk management activities into the system development life cycle through an approach to security control selection and specification that considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards or regulation.

**NIST Cybersecurity Framework CSF -** set of industry standards and best practices to help organisations manage cybersecurity risks - **IPDRR - Identify, Protect, Detect, Respond, Recover**

**- International Organization for Standardization (ISO) 27001/27002/27701/31000**

**ISO 27001 - basic procedure, international standard** that details requirements for **establishing, implementing,** maintaining, and continually improving an information security management system (ISMS).

**ISO 27002 - international standard** that provides best practice recommendations on **information security controls** for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMS).

**ISO 27701 - international standard** that **acts as a privacy extension** to the existing information security management system (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a privacy information management system (**PIMS**)

**ISO 31000 -** **international standard, global version of RMF** for enterprise risk management that provides a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies, and paradigms that differed between industries, subject matters, and regions.

**- SSAE SOC 2 Type I/II - System and Organisation Controls (SOC)**

A **suite of reports** **produced during an audit** which is used by service orgs to issue validated reports of internal controls over those info systems to the users of those services.

**SOC 2 - Trust Services Criteria**

**Type II - addresses the operational effectiveness** **of the specified controls** over a period of time (9-12 months).

**- Cloud Security Alliance - Cloud control matrix**

Designed to provide fundamental security principles to guide cloud vendors and to **assist prospective cloud customers** in assessing the overall security risk of a cloud provider.

**- Cloud Security Alliance - Reference architecture**

**‘This is what we are going to build towards’** - A methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions that fulfil their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities and to plan a roadmap to meet the security needs of their business.

**- Control Objectives for Information and Related Technology (COBIT)**

Divides IT into 4 domains: Plan & Organize; Acquire and Implement; Deliver & Support; Monitor & Evaluate.

**- Sherwood Applied Business Security Architecture (SABSA)**

Risk-driven architecture.

**- NIST SP 800-53**

Security control framework developed by US Department of Commerce - Technical, Operational, Management.

**- ITIL4**

**• Benchmarks /secure configuration guides**

**- Platform/vendor-specific guides**

**-- Web server**

**-- OS**

**-- Application server**

**-- Network infrastructure devices**

**5.3 Explain the importance of policies to organizational security.**

**• Personnel**

**- Acceptable use policy**

Restricts how a computer, network, or other system may be used.

**- Job rotation**

Users are cycled through various jobs to learn the overall operations better, reduce their boredom, enhance their skill level, and most importantly, increase security - identifies theft/fraud etc.

**- Mandatory vacation**

Identifies theft/fraud.

**- Separation of duties**

Requires more than one person to conduct a sensitive task or operation. Can be implemented by a single user with a user and admin account - malware can only run at the lower level.

**Dual control** - two people need to be present.

**Split knowledge** - knowledge is split between multiple people.

**- Least privilege**

Users and processes should be run using the lowest level of access necessary to perform the given function.

**- Clean desk space**

All employees must put away everything from their desk at the end of the day into locked drawers and cabinets.

**- Background checks**

Check the person is who they say they are and does not have a history of bankruptcy, crime etc.

**- Non-disclosure agreement (NDA)**

Non-compete.

**- Social media analysis**

Look at their social media accounts to check for any unwanted behaviour.

**- Onboarding**

**- Offboarding**

What do you do when you hire/fire someone, from an IT security perspective.

**- User training**

**Security Awareness Training** - used to reinforce to users the importance of their help in securing the org’s resources. At least annually. Best return on investment.

**Security Training** - used to teach personnel the skills they need to perform their job in a more secure manner.

**Security Education -** generalised training e.g. courses like Security+

**-- Gamification**

**-- Capture the flag**

**-- Phishing campaigns**

**-- Phishing simulations**

**-- Computer-based training (CBT)**

**-- Role-based training**

**• Diversity of training techniques**

**• Third-party risk management**

Need to do due diligence on third-party suppliers

Check for properly resourced cybersecurity programs, security assurance and risk management processes, product support life cycle will keep patching you for the foreseeable future, security controls exist to protect confidential data and the company can provide incident response and forensics assistance, general and historical company information.

**- Vendors**

**- Supply chain**

Trusted Foundry program of the US DoD to make sure all ICs do not deviate from their stated function.

Hardware source authenticity - ensure all hardware is procured tamper-free from trustworthy suppliers e.g. buying second-hand/aftermarket vs directly from the supplier.

**- Business partners**

**- Service level agreement (SLA)**

Agreement concerned with the ability to support and respond to problems within a given timeframe and continuing to provide the agreed upon level of service to the user - **‘99.999% Uptime’**.

**- Memorandum of understanding (MOU)**

**Non-binding** agreement between two or more organisations to detail an intending common line of action. ‘Letter of intent’. Can be internal between business units, or between multiple organisations.

**- Interconnection Security Agreement (ISA)**

Agreement for the owners and operators of the IT systems to document what technical requirements each org must meet esp for security.

**- Measurement systems analysis (MSA)**

**- Business partnership agreement (BPA)**

Conducted between two business partners that establishes the conditions of their relationship. Can also include security requirements.

**- End of life (EOL)**

**- End of service life (EOSL)**

**- Non-Disclosure Agreement (NDA)**

Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship. Legally **binding**.

**• Data**

**- Classification**

**- Governance**

**- Retention**

Data should not be kept forever. Need to know how long. Legislation against it e.g. GDPR.

**• Credential policies**

**- Personnel**

**- Third-party**

**- Devices**

**- Service accounts**

**- Administrator/root accounts**

**Due Diligence -** ensuring that IT infrastructure risks are known and managed properly.

**Due Care -** mitigation actions that an organisation takes to defend against the risk that have been uncovered during due diligence.

**Due Process -** legal term that refers to how an org must respect and safeguard personnel’s rights - protects persons from governments and companies from lawsuits.

**• Organizational policies**

Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms.

**System-specific** - address the security needs of a specific technology, app, network, or system.

**Issue-Specific** - built to address a specific security issue, such as email privacy, employee termination etc.

**Regulatory -** mandatory standards and laws

**Advisory -** says what is and isn’t allowed

**Informative -** focus on a certain topic, educational in nature e.g. how to use social media outside of business hours.

**- Change management**

Defines the structured way of changing the state of a computer system, network, or IT procedure.

**- Change control**

**- Asset management**

**5.4 Summarize risk management processes and concepts.**

**• Risk types**

**Risk exists at the intersection between threats and vulnerabilities**

Threat with no vulnerability = no risk

Vulnerability with no threat = no risk

**Security Posture** - risk level to which a system or other technology element is exposed

**- External**

Risk from a source that is out of your control e.g. fire, flood, blackouts, hackers.

Threat = external, outside your control

**- Internal**

Risks that are formed within the org, arise during normal ops, and are often foreseeable e.g. server crashes.

Vulnerability = internal, inside your control

**- Legacy systems**

An old method, tech, system, or program which includes an outdated computer system still in use e.g. Windows XP. Prevent issues: do not connect them to the internet.

**- Multiparty**

Risk that refers to the connection of multiple systems or orgs where each brings their own inherent risks.

**- IP theft**

Risk associated with business assets being stolen from an org in which economic damage, the loss of a competitive edge, or a slowdown in business growth occurs. Data Loss Prevention DLP system can prevent this.

**- Software compliance/licensing**

Risk associated with a company not being aware of what software or components are installed within its network. If anyone installs random stuff on the network then we are taking on that risk. Licensing - people just click yes on everything, but are we allowed, will the program get turned off, will we get sued.

**• Risk management strategies**

Used to minimise the likelihood of a negative outcome from occurring

**- Avoidance**

Stopping the activity that has risk or choosing a less risky alternative.

**- Transference**

Pass the risk to a third-party.

**-- Cybersecurity insurance**

**- Mitigation**

Minimise the risk to an acceptable level.

**- Acceptance**

Accept the current level of risk and the costs associated with it if the risk were realised.

**- Residual Risk**

Risk that remains after trying to avoid, transfer, or mitigate the risk. There will always be some - this has to be at an acceptable level for your organisation.

**• Risk analysis**

Risk = the probability that a threat will be realised.

**- Risk register**

**- Risk matrix/heat map**

**- Risk control assessment**

**- Risk control self-assessment**

**- Risk awareness**

**- Inherent risk**

**- Residual risk**

**- Control risk**

**- Risk appetite**

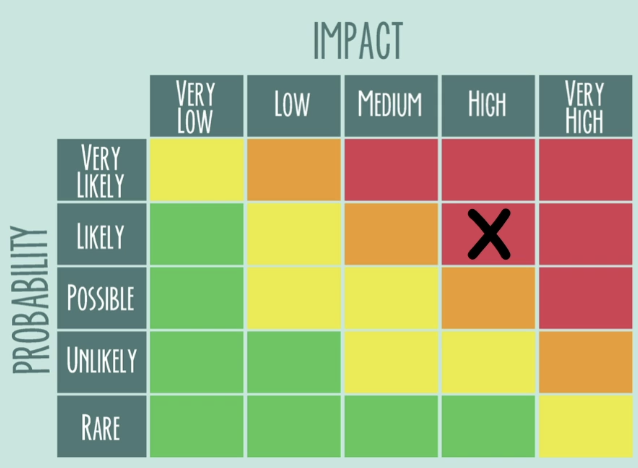
**- Regulations that affect risk posture**

**- Risk assessment types**

Identifies how much risk exists in a given network or system.

1. Identify assets
2. Identify vulnerabilities
3. Identify threats
4. Identify the impact

**-- Qualitative**

Uses intuition, experience, and other methods to assign a relative value to risk.

Experience is critical in qualitative analysis. **No numerical analysis involved.**

**-- Quantitative**

Numerical and monetary values to calculate risk. Removes estimation and guesswork - becomes a large maths problem.

**- Likelihood of occurrence**

**- Impact (Magnitude of Impact)**

An estimation of the amount of damage that a negative risk might achieve.

**- Asset value**

**- Single-loss expectancy (SLE)**

Cost associated with the realisation of each individualised threat that occurs.

Single Loss Expectancy = Asset Value x Exposure Factor

**SLE = AV x EF**

**- Annualized rate of occurrence (ARO)**

Number of times per year that a threat is realised

**- Annualized loss expectancy (ALE)**

Expected cost of a realised threat over a given year. Used in decision-making, you can compare numbers instead of tons of expertise. Easier to justify to upper management if you relied on numbers. In reality we rely on both quantitative and qualitative, subjectivity.

Annualised Loss Expectancy = Single-loss Expectancy x Annualized Rate of Occurrence

**ALE = SLE x ARO**

**• Disasters**

**- Environmental**

Fire, flood, hurricane, earthquake, blizzard etc.

**- Person-made**

Theft, violence, rioting, hackers etc.

**- Internal vs. external**

Insider threat, controllable vs everything else external, uncontrollable

**• Business impact analysis**

Systematic activity that identifies organisational risks and determines their effect on ongoing, mission critical operations. Governed by metrics that express system availability.

**- Maximum Tolerable Downtime (MTD)**

**Longest period of time a business can be inoperable** without causing irrevocable business failure. Each business process can have its own MTD e.g. minutes-hours for critical, 24 hours for urgent, 7 days for others. Upper limit on the recovery time to resume operations.

**- Recovery time objective (RTO)**

**Length of time** it takes after an event to resume normal business operations e.g 1 day.

**- Work Recovery Time (WRT)**

**Length of time in addition to the RTO** of individual systems to perform re-integration and testing of a restored or upgraded system following an event.

**- Recovery point objective (RPO)**

Longest period of time that an organisation can tolerate lost data being unrecoverable.

**Length of time you can be without your data** e.g. 6 hours

**- Mean time to failure (MTTF)**

Average time it takes for a system to fail **since it was last resumed - ‘uptime’**.

**- Mean time to repair (MTTR)**

Average time to go from system failure to resuming operations. **Tells you how much downtime there will be.**

**- Mean time between failures (MTBF)**

Average time between failures. MTTR + MTTF.

**- Functional recovery plans**

**- Single point of failure**

**- Disaster recovery plan (DRP)**

**- Mission essential functions**

**- Identification of critical systems**

**- Site risk assessment**

**5.5 Explain privacy and sensitive data concepts in relation to security.**

**• Organizational consequences of privacy and data breaches**

**- Reputation damage**

**- Identity theft**

**- Fines**

**- IP theft**

**• Notifications of breaches**

**- Escalation**

**- Public notifications and disclosures**

**GDPR -** must do within 72 hours.

**SB 1386 (California Only) -** any business that stores personal data must disclose a breach.

**• Data types**

**- Classifications**

Category based on the value to the organisation and the sensitivity of the information if it were to be disclosed. Do not over-classify.

Commercial: Public, Sensitive, Private, Confidential

Government: Unclassified, Sensitive but Unclassified, Confidential, Secret, Top Secret

Confidential - seriously **affect** us

Secret - seriously **damage** us

Top Secret - **gravely** **damage** us

**-- Public**

No impact to the company, often posted as open-source.

**-- Sensitive**

Minimal impact if released. Any information that can result in a loss of security, or loss of advantage to a company, if accessed by unauthorised persons.

**-- Private**

Should only be used within the organisation e.g. HR data

**-- Confidential**

Trade secrets, IP, source code etc. seriously affected if disclosed.

**-- Critical**

**-- Proprietary**

**-- Personally identifiable information (PII)**

Piece of data can be used by itself or in combination with some other piece of data to personally identify an individual.

**-- Personal Health information (PHI)**

**-- Payment Card Industry (PCI)**

Credit card info.

**-- Health information**

**Health Insurance Portability and Accountability Act (HIPAA) -** affects healthcare providers, facilities, insurance companies etc.

**-- Financial information**

**Sarbanes-Oxley (SOX) -** publicly-traded US corps, specific accounting and financial reporting. C-suite can go to jail.

**Gramm-Leach-Bliley Act (GLBA)** -affects banks, mortgages, loans, insurance, investment, credit cards. Security of PII, cannot share with third-parties.

**-- Government data**

**Privacy Act of 1974** - affects US govt computer systems that collects, stores, uses, or disseminates PII

**Federal Information Security Management Act (FISMA) -** requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data.

**Help America Vote Act (HAVA) -** PII during voting and elections.

**-- Customer data**

**Children’s Online Privacy Protection Act COPPA -** Concerns data taken from children under 13 years old.

**• Privacy enhancing technologies**

**- De-identification**

Methods that remove identifying information from data before it is distributed.

**- Re-identification**

With a small number of people, you could reverse it, which is bad.

**- Data minimization**

**- Aggregation/banding**

Data is generalised to protect the individuals involved e.g. 90% of people did X.

**- Data masking**

Generic/placeholder labels are substituted for real data while preserving the data structure.

**- Tokenization**

Unique token is substituted for real data. Is it reversible, usually it is.

**- Anonymization**

**- Pseudo-anonymization**

**• Roles and responsibilities**

Process of identifying the person responsible for the confidentiality, integrity, availability, and privacy of information assets.

**- Data owners**

A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset. Labels assets and ensures they are protected with appropriate controls.

**- Data controller**

**- Data processor**

**- Privacy officer**

Responsible for the oversight of any PII/SPI/PHI assets managed by the company

**- Data steward**

Focused on quality of data and associated metadata.

**- Data custodian**

Responsible for handling the management of the system on which the data assets are stored e.g. **sysadim**

**- Data protection officer (DPO)**

**• Information life cycle**

**• Impact assessment**

**• Terms of agreement**

**• Privacy notice**

Govern the labeling and handling of data.

**5 Top Exam Tips:**

1. Use a cheat sheet. Digital whiteboard to do a braindump.
2. Leave the simulations until the end.
3. Guess all unknown answers, no penalty.
4. Pick a good time (morning).
5. Be confident. You will pass.

**Acronyms**

| 3DES | Triple Data Encryption Standard |
| --- | --- |
| AAA | Authentication, Authorization, and Accounting |
| ABAC | Attribute-based Access Control |
| ACL | Access Control List |
| AD | Active Directory |
| AEP | Advanced Endpoint Protection |
| AES | Advanced Encryption Standard |
| AES256 | Advanced Encryption Standards 256bit |
| AH | Authentication Header |
| AI | Artificial Intelligence |
| AIK | Attestation Identity Keys |
| AIS | Automated Indicator Sharing |
| ALE | Annualized Loss Expectancy |
| AP | Access Point |
| APFS | Apple File System |
| API | Application Programming Interface |
| APT | Advanced Persistent Threat |
| ARO | Annualized Rate of Occurrence |
| ARP | Address Resolution Protocol |
| ASLR | Address Space Layout Randomization |
| ASP | Active Server Pages |
| ATP | Advanced Threat Protection |
| ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge |
| AUP | Acceptable Use Policy |
| AV | Antivirus |
| BASH | Bourne Again Shell |
| BCP | Business Continuity Planning |
| BGP | Border Gateway Protocol |
| BIA | Business Impact Analysis |
| BIOS | Basic Input/Output System |
| BPA | Business Partnership Agreement |
| BPDU | Bridge Protocol Data Unit |
| BSSID | Basic Service Set Identifier |
| BYOD | Bring Your Own Device |
| CA | Certificate Authority |
| CAPTCHA | Completely Automated Public Turing Test to Tell Computers and Humans Apart |
| CAR | Corrective Action Report |
| CASB | Cloud Access Security Broker |
| CBC | Cipher Block Chaining |
| CBT | Computer-based Training |
| CCMP | Counter-Mode/CBC-MAC Protocol |
| CCTV | Closed-Circuit Television |
| CERT | Computer Emergency Response Team |
| CFB | Cipher Feedback |
| CHAP | Challenge-Handshake Authentication Protocol |
| CIO | Chief Information Officer |
| CIRT | Computer Incident Response Team |
| CIS | Center for Internet Security |
| CMS | Content Management System |
| CN | Common Name |
| COOP | Continuity of Operations Planning |
| COPE | Corporate-owned Personally Enabled |
| CP | Contingency Planning |
| CRC | Cyclic Redundancy Check |
| CRL | Certificate Revocation List |
| CSA | Cloud Security Alliance |
| CSIRT | Computer Security Incident Response Team |
| CSO | Chief Security Officer |
| CSP | Cloud Service Provider |
| CSR | Certificate Signing Request |
| CSRF | Cross-Site Request Forgery |
| CSU | Channel Service Unit |
| CTM | Counter-Mode |
| CTO | Chief Technology Officer |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| CYOD | Choose Your Own Device |
| DAC | Discretionary Access Control |
| DBA | Database Administrator |
| DDoS | Distributed Denial-of-Service |
| DEP | Data Execution Prevention |
| DER | Distinguished Encoding Rules |
| DES | Data Encryption Standard |
| DHCP | Dynamic Host Configuration Protocol |
| DHE | Diffie-Hellman Ephemeral |
| DKIM | Domain Keys Identified Mail |
| DLL | Dynamic-link Library |
| DLP | Data Loss Prevention |
| DMARC | Domain Message Authentication Reporting and Conformance |
| DNAT | Destination Network Address Transaction |
| DNS | Domain Name System |
| DNSSEC | Domain Name System Security Extensions |
| DoS | Denial-of-Service |
| DPO | Data Protection Officer |
| DRP | Disaster Recovery Plan |
| DSA | Digital Signature Algorithm |
| DSL | Digital Subscriber Line |
| EAP | Extensible Authentication Protocol |
| ECB | Electronic Code Book |
| ECC | Elliptic-curve Cryptography |
| ECDHE | Elliptic-curve Diffie-Hellman Ephemeral |
| ECDSA | Elliptic-curve Digital Signature Algorithm |
| EDR | Endpoint Detection and Response |
| EFS | Encrypted File System |
| EIP | Extended Instruction Pointer |
| EK | Endorsement Key |
| EOL | End of Life |
| EOS | End of Service |
| EPP | Endpoint Protection Platform |
| ERP | Enterprise Resource Planning |
| ESN | Electronic Serial Number |
| ESP | Encapsulating Security Payload |
| ESSID | Extended Service Set Identifier |
| FaaS | Function as a Service |
| FACL | File System Access Control List |
| FAT32 | File Allocation Table 32 |
| FDE | Full Disk Encryption |
| FIdM | Federated Identity Management |
| FIM | File Integrity Monitoring |
| FPGA | Field Programmable Gate Array |
| FRR | False Rejection Rate |
| FTP | File Transfer Protocol |
| FTPS | Secured File Transfer Protocol |
| GCM | Galois/Counter Mode |
| GDPR | General Data Protection Regulation |
| GPG | GNU Privacy Guard |
| GPO | Group Policy Object |
| GPS | Global Positioning System |
| GPU | Graphics Processing Unit |
| GRE | Generic Routing Encapsulation |
| HA | High Availability |
| HDCP | High-bandwidth Digital Content Protection |
| HDD | Hard Disk Drive |
| HIDS | Host-based Intrusion Detection System |
| HIPS | Host-based Intrusion Prevention System |
| HMAC | Hash-based Message Authentication Code |
| HOTP | HMAC-based One-time Password |
| HSM | Hardware Security Module |
| HSMaaS | Hardware Security Module as a Service |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| HVAC | Heating, Ventilation, Air Conditioning |
| IaaS | Infrastructure as a Service |
| IAM | Identity and Access Management |
| ICMP | Internet Control Message Protocol |
| IC | Integrated Circuit |
| ICS | Industrial Control Systems |
| IDEA | International Data Encryption Algorithm |
| IDF | Intermediate Distribution Frame |
| IdP | Identity Provider |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IKE | Internet Key Exchange |
| IM | Instant Messaging |
| IMAP4 | Internet Message Access Protocol v4 |
| IoC | Indicators of Compromise |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security |
| IR | Incident Response |
| IRC | Internet Relay Chat |
| IRP | Incident Response Plan |
| ISA | Interconnection Security Agreement |
| ISFW | Internal Segmentation Firewall |
| ISO | International Organization for Standardization |
| ISP | Internet Service Provider |
| ISSO | Information Systems Security Officer |
| ITCP | IT Contingency Plan |
| IV | Initialization Vector |
| KDC | Key Distribution Center |
| KEK | Key Encryption Key |
| L2TP | Layer 2 Tunneling Protocol |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LEAP | Lightweight Extensible Authentication Protocol |
| MaaS | Monitoring as a Service |
| MAC | Media Access Control |
| MAM | Mobile Application Management |
| MAN | Metropolitan Area Network |
| MBR | Master Boot Record |
| MBSA | Microsoft Baseline Security Analyser |
| MD5 | Message Digest 5 |
| MDF | Main Distribution Frame |
| MDM | Mobile Device Management |
| MFA | Multifactor Authentication |
| MFD | Multifunction Device |
| MFP | Multifunction Printer |
| ML | Machine Learning |
| MMS | Multimedia Message Service |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MPLS | Multiprotocol Label Switching |
| MSA | Measurement Systems Analysis |
| MS-CHAP | Microsoft Challenge-Handshake Authentication Protocol |
| MSP | Managed Service Provider |
| MSSP | Managed Security Service Provider |
| MTBF | Mean Time Between Failures |
| MTTF | Mean Time to Failure |
| MTTR | Mean Time to Repair |
| MTU | Maximum Transmission Unit |
| NAC | Network Access Control |
| NAS | Network-attached Storage |
| NAT | Network Address Translation |
| NDA | Non-disclosure Agreement |
| NFC | Near-field Communication |
| NFV | Network Function Virtualization |
| NGAV | Next-generation Antivirus |
| NGFW | Next-generation Firewall |
| NG-SWG | Next-generation Secure Web Gateway |
| NIC | Network Interface Card |
| NIDS | Network-based Intrusion Detection System |
| NIPS | Network-based Intrusion Prevention System |
| NIST | National Institute of Standards & Technology |
| NOC | Network Operations Center |
| NTFS | New Technology File System |
| NTLM | New Technology LAN Manager |
| NTP | Network Time Protocol |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| OSINT | Open-source Intelligence |
| OSPF | Open Shortest Path First |
| OT | Operational Technology |
| OTA | Over-The-Air |
| OTG | On-The-Go |
| OVAL | Open Vulnerability and Assessment Language |
| OWASP | Open Web Application Security Project |
| P12 | PKCS #12 |
| P2P | Peer-to-Peer |
| PaaS | Platform as a Service |
| PAC | Proxy Auto Configuration |
| PAM | Privileged Access Management |
| PAM | Pluggable Authentication Modules |
| PAP | Password Authentication Protocol |
| PAT | Port Address Translation |
| PBKDF2 | Password-based Key Derivation Function 2 |
| PBX | Private Branch Exchange |
| PCAP | Packet Capture |
| PCI | DSS Payment Card Industry Data Security Standard |
| PCR | Platform Configuration Registers |
| PDU | Power Distribution Unit |
| PE | Portable Executable |
| PEAP | Protected Extensible Authentication Protocol |
| PED | Portable Electronic Device |
| PEM | Privacy Enhanced Mail |
| PFS | Perfect Forward Secrecy |
| PGP | Pretty Good Privacy |
| PHI | Personal Health Information |
| PII | Personally Identifiable Information |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKCS | Public Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| PoC | Proof of Concept |
| POP | Post Office Protocol |
| POTS | Plain Old Telephone Service |
| PPP | Point-to-Point Protocol |
| PPTP | Point-to-Point Tunneling Protocol |
| PSK | Preshared Key |
| PTZ | Pan-Tilt-Zoom |
| PUF | Physically Unclonable Function |
| PUP | Potentially Unwanted Program |
| QA | Quality Assurance |
| QoS | Quality of Service |
| PUP | Potentially Unwanted Program |
| RA | Registration Authority |
| RAD | Rapid Application Development |
| RADIUS | Remote Authentication Dial-in User Service |
| RAID | Redundant Array of Inexpensive Disks |
| RAM | Random Access Memory |
| RAS | Remote Access Server |
| RAT | Remote Access Trojan |
| RC4 | Rivest Cipher version 4 |
| RCS | Rich Communication Services |
| RFC | Request for Comments |
| RFID | Radio Frequency Identification |
| RIPEMD | RACE Integrity Primitives Evaluation Message Digest |
| ROI | Return on Investment |
| RPO | Recovery Point Objective |
| RSA | Rivest, Shamir, & Adleman |
| RTBH | Remotely Triggered Black Hole |
| RTO | Recovery Time Objective |
| RTOS | Real-time Operating System |
| RTP | Real-time Transport Protocol |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SaaS | Software as a Service |
| SAE | Simultaneous Authentication of Equals |
| SAML | Security Assertions Markup Language |
| SCADA | Supervisory Control and Data Acquisition |
| SCAP | Security Content Automation Protocol |
| SCCM | System Center Configuration Management (Microsoft) |
| SCEP | Simple Certificate Enrollment Protocol |
| SDK | Software Development Kit |
| SDLC | Software Development Life Cycle |
| SDLM | Software Development Life-cycle Methodology |
| SDN | Software-defined Networking |
| SDP | Service Delivery Platform |
| SDV | Software-defined Visibility |
| SECaaS | Security as a Service |
| SED | Self-Encrypting Drives |
| SEH | Structured Exception Handling |
| SFTP | SSH File Transfer Protocol |
| SHA | Secure Hashing Algorithm |
| SIEM | Security Information and Event Management |
| SIM | Subscriber Identity Module |
| SIP | Session Initiation Protocol |
| SLA | Service-level Agreement |
| SLE | Single Loss Expectancy |
| SMB | Server Message Block |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SMS | Short Message Service |
| SMTP | Simple Mail Transfer Protocol |
| SMTPS | Simple Mail Transfer Protocol Secure |
| SNMP | Simple Network Management Protocol |
| SOAP | Simple Object Access Protocol |
| SOAR | Security Orchestration, Automation, Response |
| SoC | System on Chip |
| SOC | Security Operations Center |
| SPF | Sender Policy Framework |
| SPIM | Spam over Instant Messaging |
| SQL | Structured Query Language |
| SQLi | SQL Injection |
| SRK | Storage Root Key |
| SRTP | Secure Real-time Transport Protocol |
| SSD | Solid State Drive |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| SSO | Single Sign-on |
| STIX | Structured Threat Information eXpression |
| STP | Shielded Twisted Pair |
| SWG | Secure Web Gateway |
| TACACS+ | Terminal Access Controller Access Control System |
| TAXII | Trusted Automated eXchange of Intelligence Information |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TGT | Ticket Granting Ticket |
| TKIP | Temporal Key Integrity Protocol |
| TLS | Transport Layer Security |
| TOS | Trusted Operating System |
| TOTP | Time-based One Time Password |
| TPM | Trusted Platform Module |
| TSIG | Transaction Signature |
| TTP | Tactics, Techniques, and Procedures |
| UAT | User Acceptance Testing |
| UDP | User Datagram Protocol |
| UEBA | User and Entity Behavior Analytics |
| UEFI | Unified Extensible Firmware Interface |
| UEM | Unified Endpoint Management |
| UPS | Uninterruptible Power Supply |
| URI | Uniform Resource Identifier |
| URL | Universal Resource Locator |
| USB | Universal Serial Bus |
| USB | OTG On-The-Go |
| UTM | Unified Threat Management |
| UTP | Unshielded Twisted Pair |
| VBA | Visual Basic for Applications |
| VDE | Virtual Desktop Environment |
| VDI | Virtual Desktop Infrastructure |
| VLAN | Virtual Local Area Network |
| VLSM | Variable-length Subnet Masking |
| VM | Virtual Machine |
| VoIP | Voice over IP |
| VPC | Virtual Private Cloud |
| VPN | Virtual Private Network |
| VTC | Video Teleconferencing |
| WAF | Web Application Firewall |
| WAP | Wireless Access Point |
| WEP | Wired Equivalent Privacy |
| WIDS | Wireless Intrusion Detection System |
| WIPS | Wireless Intrusion Prevention System |
| WORM | Write Once Read Many |
| WPA | WiFi Protected Access |
| WPS | WiFi Protected Setup |
| XaaS | Anything as a Service |
| XXE | XML External Entity |
| XML | Extensible Markup Language |
| XOR | Exclusive OR |
| XSRF | Cross-site Request Forgery |
| XSS | Cross-site Scripting |