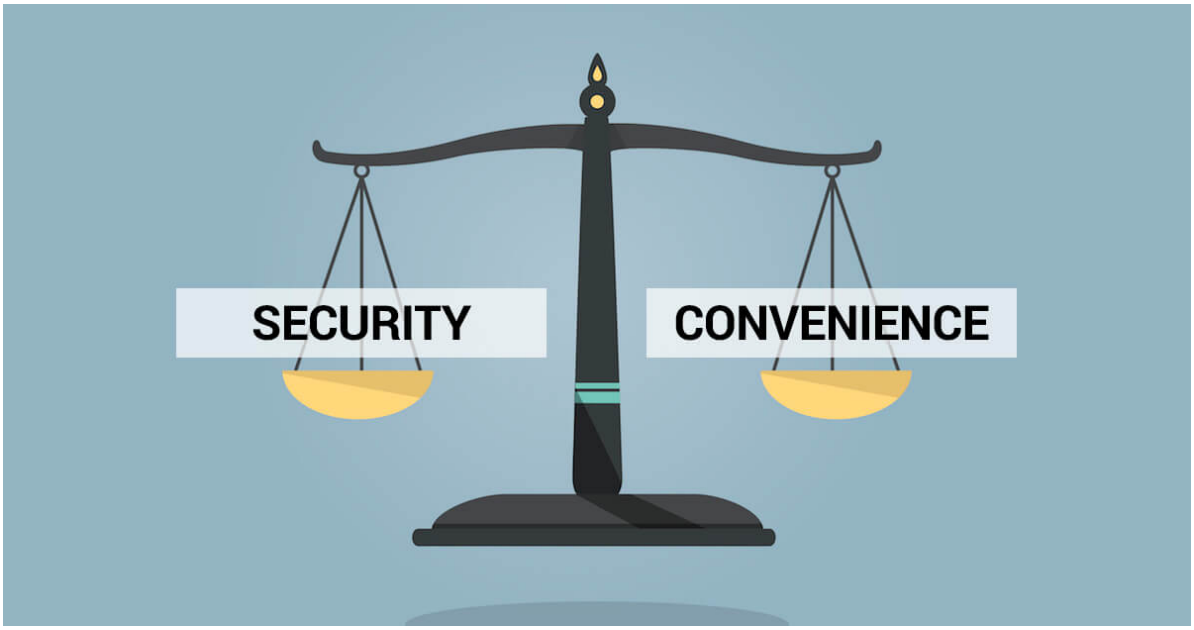
Introduction to Security

- Overview of Security
  - Information security
  - Information Systems Security
  - CIA Triad
    - Confidentiality
    - Integrity
    - Availability
  - AAA of Security
    - Authentication
    - Authorisation
    - Accounting
  - Security Threats
    - Malware
    - Unauthorised Access
    - System Failure
    - Social Engineering
  - Mitigating Threats
    - Physical Control
    - Technical Control
    - Administrative Control
  - Hackers
    - White Hats
    - Black Hats
    - Grey Hats
    - Blue Hats
    - Elite
  - Threat Actors
    - Script Kiddies
    - Hacktivists
    - Organised Crime
    - Advanced Persistent Threats (APT)
  - Threat Intelligence and Sources
    - Timeliness
    - Relevancy
    - Accuracy
    - Confidence Levels
    - Proprietary
    - Closed-Source
    - Open-Source
    - Open-Source Intelligence (OSINT)
  - Threat Hunting
  - Attack Frameworks

        - Kill Chain
        - MITRE ATT&CK Framework
        - Diamond Model of Intrusion Analysis
- Malware
    - Viruses
    - worms
    - Trojans
    - Ransomware
    - Spyware
    - Rootkits
    - Spam
- Malware Infections
    - Common Delivery Methods
    - Botnets and Zombies
    - Active Interception & Privilege Escalation
    - Backdoor and Logic Bombs
    - Symptoms of Infection
    - Removing Malware
    - Preventing Malware
- Malware Exploitation
    - Exploit Technique
    - Dropper
    - Downloader
    - Shellcode
    - Code Injection
    - Living Off the Land
- Security Applications and Devices
    - Software Firewalls
    - IDS
- Mobile Device Security
- Hardening
- Supply Chain Assessment
- Virtualisation
- Application Security
- Secure Software Development
- Network Design
- Perimeter Security
- Cloud Security
- Workflow Orchestration
- Network Attacks
- Securing Networks
- Physical Security
- Facilities Security
- Authentication

- Access Control
- Risk Assessments
- Vulnerability Management
- Monitoring and Auditing
- Cryptography
- Hashing
- Security Protocols
- Social Engineering
- Policies and Procedures
- Incident Response Procedure

Overview of Security



Information Security

- Act of protecting data and information from unauthorised access, unlawful modification and disruption, disclosure, corruption, and destruction

Information Systems Security

- Act of protecting the systems that hold and process our critical data

CIA Triad

Information security consists of three independent branches:

- **Information confidentiality**
- **Information integrity**
- **Information Availability**

When we have all three of those, it means that our data and our information has good security. But if we lose one of those, that becomes a vulnerability.

Confidentiality

Data confidentiality ensures that data, or the information carried by the data, can be accessed only by authorised subjects.

Integrity

Data integrity ensures that the information comes from a legitimate source and hasn't been altered, deliberately or accidentally, after its creation.

Availability

Data availability ensures the timely and convenient access to data for all authorised entities.

AAA of Security

- **Authentication**
- **Authorisation**
- **Accounting**

Authentication

When a person's identity is established with proof and confirmed by a system.

We have 5 methods of authentication:

- Something you know
- Something you are
- Something you have
- Something you do
- Somewhere you are

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 network resources. Log files. Accounting allows us to go back at the data in our log files to figure out who did what and when in case of a data breach.

Non-repudiation occurs when you have *proof* that someone has taken an action. Meaning, the user can't say they didn't take the action because you have proof they did.

Security Threats

- **Malware** - Short-hand term for malicious software.
- **Unauthorised Access** - Occurs when access to a computer resources and data happens without the consent of the owner.
- **System Failure** - Occurs when a computer crashes or an individual application fails.
- **Social Engineering** - Act of manipulating users into revealing confidential information or performing other detrimental actions.

Mitigating Threats

- **Physical Controls**
- **Technical Controls**
- **Administrative Controls**

Physical Controls

Alarm systems, locks, surveillance cameras, identification cards, and security guards.

Technical Controls

Smart cards, encryption, access control lists (**ACL**), intrusion detection systems(**IDS**), and network authentication.

Administrative Controls

> Administrative controls are also referred to as managerial controls

Policies, procedures, security awareness training, contingency planning, and disaster recovery plans.

Administrative Controls can further be broken down into two categories:

- **Procedural Controls** - Organisations chooses to do on its own.
- **Legal or Regulatory Controls** - Are the ones that you have to do because the law says you must.

> User training is the most cost effective security control to utilise

Hackers

- **White Hats**
- **Black Hats**
- **Grey Hats**
- **Blue Hats**
- **Elite**

White Hats

Non-malicious hackers who attempt to break into a company's systems at their request. White hats are either on the payroll of the company or they are contracted to do this as a service.

> Other names: ethical hackers or penetration testers

Black Hats

Malicious hackers who break into computer systems and networks without authorisation or permission.

> The bad guys

Grey Hats

Hackers without any affiliation to a company that attempts to break into a company's network and risks breaking the law.

> A grey hat does not necessarily have malicious intent. They may try to hack into a company to see if they can do it. They don't want to cause harm to the company.

Blue Hats

Hackers who attempt to hack into a network with permission of the company but are not employed by the company.

> Bug bounties like on HackerOne.

Elite

Hackers who find and exploit vulnerabilities before anyone else does.

> 1 in 10,000 hackers are **elite**

Script Kiddie

Script kiddies have limited skill and only run other peoples exploits and tools.

Threat Actors

There are four main groups of threat actors:

- **Script Kiddies** - Hackers who have little to no skill who only use the tools and exploits written by others. (**Baby hackers**)
- **Hacktivists** - Hackers who are driven by a cause like social change, political agendas, or terrorism. (Example: **Anonymous**)
- **Organised Crime** - Hackers who are part of a crime group that is well-funded and highly sophisticated.
- **Advanced Persistent Threats** - Highly trained and funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal. (**APT**'s')

> Once APT's have hacked into a system, they will be sneaky and quiet for some time.

Threat Intelligence and Sources

> You have to consider the sources of your intelligence.

There are several factors that we can use:

- **Timeliness**
- **Relevancy**
- **Accuracy**
- **Confidence Level**

Timeliness

Property of an intelligence source that ensures it is up to date.

> Your report could stop being valid after some time.

Relevancy

Property of an intelligence source that ensures it matches the use case intended for it.

> What affects me and my organisation so I can defend against it.

Accuracy

Property of an intelligence source that ensures it produces effective results.

> The information needs to be valid and true

Confidence Level

Property of an intelligence source that ensures it produces qualified statements about reliability.

> Getting lots of different pieces of information and lots of different indicators, and we try to put together the best report we can.

MISP Project codifies the use of the admiralty scale for grading data and estimative language.

Three places where you can get information from:

- **Proprietary**
- **Closed-Sourced**
- **Open-Sourced**

Proprietary

Threat intelligence is very widely provided as a commercial service offering, where access to updates and research is subject to a subscription fee.

Closed-Source

Data that is derived from the provider's own research and analysis efforts, such as data from honey-nets that they operate, plus information minded from its customers' systems, suitably anonymised.

Open-Sourced

Data that is available to use without subscription, which may include threat feeds similar to the commercial providers, and may contain reputation lists and malware signature databases.

- **US-CERT**
- **UK's NCSC**
- **AT&T Security (OTX)**
- **MISP**
- **VirusTotal**
- **Spamhaus**
- **SANS ISC Suspicious Domains**

> Threat feeds are a form of **explicit** knowledge, but **implicit** knowledge from experienced practitioners is also useful.
>
> Implicit knowledge is something you know based on your experience.

Open-Source Intelligence (OSINT)

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

Threat Hunting

A cyber security technique designed to detect presence of threats that have no been discovered by normal monitoring.

> Threat hunting is potentially less disruptive than penetration testing.

To do threat hunting, we start out by a hyptohesis:

- **Establishing a hypothesis** - A hypothesis is derived from the threat modelling and is based on potential events with higher likelihood and higher impact.

- **Profiling Threat Actors and Activities** - Involves the creation of scenarios that show how a prospective attacker might attempt an intrusion and what their objectives might be.
- Threat hunting relies on the use of the tools developed for regular security monitoring and incident response.
- You need to assume that these existing rules have failed when you are threat hunting.

Windows desktops in a lot of different companies have been infected with new malware. Well, we can start threat hunting based on that threat information. What might we do? We might start with:

- **Analyse network traffic**, to determine if there's any outgoing traffic to a suspicious domain or some kind of a C2 server.
- **Analyse the executable process list**, seeing what programs and services are being run and which ones were opening that network connection.
- **Analyse other infected hosts**
- **Identify how the malicious process was executed**. What allowed it to start up? Is there a way we can block that attack vector against future compromises? Maybe we can move to a white listing system, or we can blacklist that vulnerable system until it is patched.

> **Threat hunting** consumes a lot of resources and time to conduct, but can yield a lot of benefits.

Threat hunting can:

- **Improve detection capabilities**
- **Integrate intelligence**

> Threat hunting is a great use case for correlating that external threat intelligence you've been getting with what you're seeing in your internal logs and other sources. By putting those two things together, you now have **actionable intelligence.**

- **Reduce attack surface**
- **Block attack vectors**
- **Identify critical assets**, you are going to figure out what are the best defensive options for those critical systems and data assets.

Attack Frameworks

Three different attack frameworks:

- **Lockheed Martin Kill Chain**
- **MITRE ATT&CK Framework**
- **Diamond Model of Intrusion Analysis**

Kill Chain

A model developed by Lockheed Martin that describes the stages which a threat actor progresses a network intrusion.

The **Kill Chain** has a seven-step method:

1. **Reconnaissance** - The attacker determines what methods to use to complete the phases of the attack.
2. **Weaponization** - The attacker couples payload code that will enable access with exploit code that will use a vulnerability to execute on the target system.

3. **Delivery** - The attacker identifies a vector by which to transmit the weaponized code to the target environment.
4. **Exploitation** - The weaponized code is executed on the target system by this mechanism.
5. **Installation** - This mechanism enables the weaponized code to run a remote access tool and achieve persistence on the target system.
6. **Command & Control (C2)** - The 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** - The attacker typically uses the access he has achieved to covertly 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 course-of-action matrix to counter the progress of an attack at each stage.

MITRE ATT&CK Framework

A knowledge base maintained by the MITRE Corporation for listing and explaining specific adversary tactics, techniques, and common knowledge or procedures (attack.mitre.org)

The **pre-ATT&CK** tactics matrix aligns to the reconnaissance and weaponized phases of the kill chain.

Diamond Model of Intrusion Analysis

A framework for analysing cyber security incidents and intrusions by exploring the relationships between four core features: adversary, capability, infrastructure, and victim.

> These models can be used individually or combined.

Malware

Malware is software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent.

- **Viruses**
- **Worms**
- **Trojan horses**
- **Ransomware**
- **Spyware**
- **Rootkits**
- **Spam**

Viruses

Malicious code that runs on a machine without the user's knowledge and infects the computer when executed.

- Viruses require a user action in order to reproduce and spread across your network.

The Security+ exam is going to separate viruses into 10 different types:

- **Boot sector**
- **Macro**
- **Program**
- **Multipartite**
- **Encrypted**

- **Polymorphic**
- **Metamorphic**
- **Stealth**
- **Armored**
- **Hoax**

Boot Sector Virus

Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up.

- **Difficult to detect, they are installed before the system boots up.**

Macros

Virus embedded into a document and is executed when the document is opened by the user.

Examples of where they could be:

- **Word documents**
- **Excel spreadsheets**
- **PowerPoint presentations**

By default, macros aren't malicious. Macros are used out there as a way for you to do a lot of good functions in a very short period of time.

That is a piece of code that works properly, but because we have the ability to add code to these office documents, bad guys can also add malicious code to these documents. And that's exactly what a macro virus does.

Program Virus

Program viruses infect an executable or application.

For example, if you went and loaded a virus and it was able to install itself into your Microsoft Word program, every time you opened up Word, you would be loading that virus again and again. And that's why a program virus targets programs.

Multipartite

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

Encryption

Another way that viruses try to hide them self is by using encryption. And when you have an encrypted virus, this virus is going to use a cipher to encrypt the contents of itself to avoid detection by any antivirus software. Because our antivirus providers are getting better and better all the time at understanding viruses and how they work and how to stop them, encrypted viruses are making it harder for virus makers to find these type of viruses.

Polymorphic

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

Metamorphic

Virus that is able to rewrite itself entirely before it attempts to infect a file. (Advanced version of polymorphic virus).

Stealth

Stealth viruses aren't necessarily a specific type of virus as much as a category of virus protecting itself. When we talk about encrypted and polymorphic and metamorphic viruses, these are all examples of stealth viruses. They're viruses that are using various different techniques to avoid detection by an antivirus software.

Armored

Armored viruses have a layer of protection to confuse a program or person analysing it.

Hoax

A **Hoax** is actually not a virus in the traditional sense. Instead, when we get a virus hoax, we're trying to trick a user into infecting their own machine. This might come in the form of a message or a website that pops up. It may be that we call them on the phone and pretend that we're from Microsoft tech support, and tell them that their machine has been infected. And if they just follow our steps, we'll help them get rid of it. Either way, this is a form of Social Engineering where they are just trying to trick you.

Worms

A malicious software, like a virus, but is able to replicate itself without user interaction.

- Worms are able to self-replicate and spread without user's consent or action.
- Worms can cause disruption to normal network traffic and computing activities.

Trojans

Malicious software that is disguised as a piece of harmless or desirable software.

Going back a couple of thousand years ago, Greece and Troy were at war. This lasted for about 10 years with no end in sight. After a long siege, the Greeks started getting restless and they decided that they were gonna go and try something different. So they went out and constructed a large wooden horse and they were going to give it to the city of Troy as a piece offering. This seemingly harmless gift was actually filled with Greek soldiers, and once it was wheeled inside the city, day turned to night and the soldiers from within came out of the horse. They opened up the walled city's gates and let the invading Greek army into the city and they laid waste to it. This was the first example of a Trojan Horse.

- Trojans perform desired functions and malicious functions
- **Remote Access Trojan (RAT)** - Provides the attacker with remote control of a victim computer and is the most commonly used type of trojan. Example of a **RAT** is ProRat.

Ransomware

Malware that restricts access to a victim's computer system until a ransom is received.

- Ransomware uses a vulnerability in your software to gain access and then encrypts your files.

> Making backups of your files is crucial

Spyware

Malware that secretly gathers information about the user without their consent.

- The best case is that it looks into all your files, emails, instant messages, calendar invites and whatever information you have on your system and it builds a profile of you.
- The worst case is that it may include a Keylogger too. Allowing them to record every keystroke you make.

Keylogger - Captures keystrokes made by the victim and has the ability to take screenshots that are sent to the attacker.

- Adware displays advertisements based upon its spying on you.

Adware

Adware is a specific type of spyware where it's going to display advertisements to you based on what it saw when it spied on you.

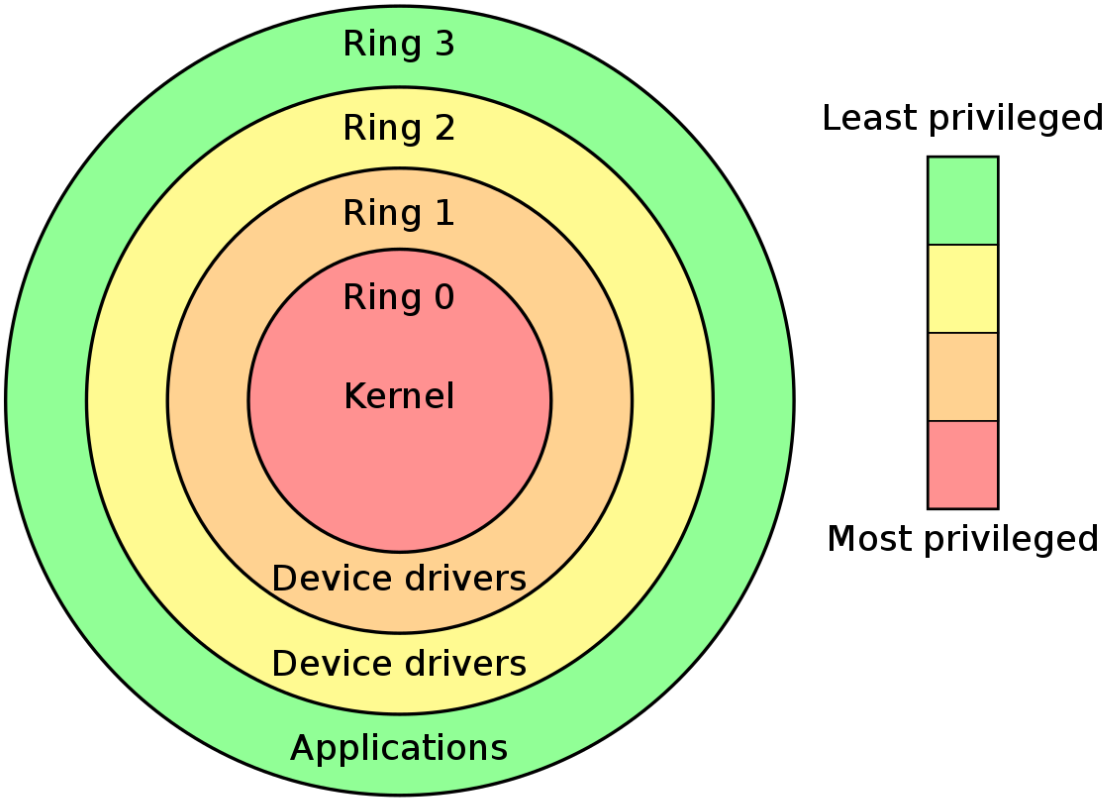
Grayware

Software that's usually used to make something behave improperly, without any serious consequences. (**jokeware**)

Rootkits

Software designed to gain administrative level control over a system without detection. Rootkits are able to perform malicious operations on a target computer at any date they want without the knowledge of the administrators or the users and even sometimes without the knowledge of the operating system them-self if they are done right. Rootkits can really get dug into your system really deeply, and when they're in there, it's really hard to detect them.

- Administrative and root permissions are ring 1
- Rootkits are trying to get into ring 0 or ring 1.



DLL Injection

Rootkits use a technique called **DLL injection**, that allows them to maintain persistent control.

A **DLL injection** is malicious code inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime.

Driver Manipulation

An attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level.

A **shim** is placed between two components to intercept calls and redirect them.

> Rootkits are activated before booting the operating system and are difficult to detect.

Spam

Activity that abuses electronic messaging systems, most commonly through email.

Most of the time it's just annoying advertisement, but sometimes there can be embedded malware in it.

Spammers often exploit a company's **open mail relays** to send their messages.

Spim

Spim is spam over instant messaging. The abuse of instant messaging systems. Aka IM spam.

Malware Infections

- **Threat Vector** - Method used by an attacker to access a victim's machine. Unpatched computers, etc.
- **Attack Vector** - Method used by an attacker to gain access to a victim's machine in order to infect it with malware.

Common Delivery Methods

- **Malware infections usually start within software, messaging, and media.**
- **Watering Holes**
    - Malware is placed on a website that you know your potential victims will access.

Botnets and Zombies

- **Botnet**
    - A collection of compromised computers under the control of a master node
    - Botnets can be utilised in other processor intensive functions and activities

Active Interception & Privilege Escalation

- **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 you are able to exploit a design flaw or bug in a system to gain access to resources that a normal user isn't able to access

Backdoors and Logic Bombs

- **Backdoors are used to bypass normal security and authentication functions**
- **Remote Access Trojan (RAT) is placed by an attacker to maintained persistent access**
- **Logic Bomb**
    - Malicious code that has been inserted inside a program and will execute only when certain conditions have been met
- **Easter Egg**
    - Non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature
- **Logic Bombs and Easter Eggs should not be used according to secure coding standards**

Symptoms of Infection

- **Your computer might have been infected if it begins to act strangely**
    - Hard drives, files, or applications are not accessible anymore.
    - Strange noises occur
    - Unusual error messages
    - Display looks strange
    - Jumbled printouts
    - Double file extensions are being displayed, such as textfile.txt.exe
    - New files and folders have been created or files and folders are missing/corrupted
    - System Restore will not function
- **Removing Malware**
    - Identify symptoms of a malware infection
    - Quarantine the infected systems
    - Disable System Restore (if using windows machine)
    - Remediate the infected system
    - Schedule automatic updates and scans
    - Enable System Restore and create a new restore point

    - Provide end user security awareness training
    - If a boot sector virus is suspected, reboot the computer from an external device and scan it.
- **Preventing Malware**
    - Viruses
    - Worms
    - Trojans
    - Ransomware
    - Spyware
    - Rootkits
    - Spam
    - Worms, Trojans, and Ransomware are best detected with anti-malware solutions
    - Scanners can detect a file containing a rootkit before it is installed...
    - ... removal of a rootkit is difficult and the best plan is to reimage the machine
    - Verify your email servers aren't configured as open mail relays or SMTP open relays
    - Remove email addresses from website
    - Use whitelists and blacklists
    - Train and educate end users
        - Update your anti-malware software automatically and scan your computer
        - Update and patch the operating system and applications regularly
        - Educate and train end users on safe Internet surfing practices.

Malware Exploitation

Exploit Technique

- Describes the specific method by which malware code infects a target host
- Most modern malware uses fileless techniques to avoid detection by signature-based security software
- **How does an APT use modern malware to operate?**
    - Dropper or downloader
    - Maintain access
    - Strengthen access
    - Actions on objectives
    - Concealment
- **Dropper**
    - Malware designed to install or run other types of malware embedded in a payload on an infected host
- **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 designed to run an exploit on the target, which may include any type of code format from scripting languages to binary code

- **Code Injection**
  - Exploit a technique that runs malicious code with the identification number of a legitimate process
    - **Masquerading**
    - **DLL injection**
    - **DLL sideloading**
    - **Process hollowing**
  - Droppers are likely to implement anti-forensics techniques to prevent detection and analysis
- **Living Off the Land**
  - Exploit techniques that use standard system tools and packages to perform intrusions
  - Detection of an adversary is more difficult when they are executing malware code within standard tools and processes

Security Applications and Devices

- **Software Firewalls**
  - **Personal Firewalls**
    - Software application that protects a single computer from unwanted Internet traffic
    - Host-based firewalls
    - Windows Firewall (Windows)
    - PF and IPFW (OS X)
    - iptables (Linux)
  - **Many anti-malware suites also contain software firewalls**
- **IDS**
  - **Intrusion Detection System**
    - Device or software application that monitors a system or network and analyses the data passing through it in order to identify an incident or attack
    - **HIDS**
      - Host-based IDS
    - **NIDS**
      - Network-based IDS
  - **Signature, Policy, and Anomaly-based detection methods**
    - Signature-based
      - A specific string of bytes triggers an alert
    - Policy-based
      - Relies on specific declaration of the security policy (i.e., `No Telnet Authorised`)
    - Anomaly-based
      - Analyses the current traffic against an established baseline and triggers an alert if outside the statistical average
  - **Type of Alerts**
    - True positive

        - Malicious activity is identified as an attack
    - False positive
        - Legitimately activity is identified as an attack
    - True negative
        - Legitimately activity is identified as legitimate traffic
    - False negative
        - Malicious activity is identified as legitimate traffic
  - **IDS can only alert and log suspicious activity...**
  - **IPS can also stop malicious activity from being executed**
  - **HIDS logs are used to recreate the events after an attack has occured**
- **Pop-up Blockers**
  - **Most web-browsers have the ability to block JavaScript created pop-ups**
  - **Users may enable pop-ups because they are required for a website to function**
  - **Malicious attackers could purchase ads (pay per click) through various networks**
    - Blocking of external files containing JavaScript, images, or web pages from loading in a browser
  - **Ensure your browser and its extensions are updated regularly**
- **Data Loss Prevention**
  - **Data Loss Prevention (DLP)**
    - Monitors the data of a system while in use, in transit, or at rest to detect attempts to steal the data
    - Software or hardware solutions
    - **Endpoint DLP System**
        - 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
    - **Network DLP System**
        - Software or hardware-based solution that is installed on the perimeter of the network to detect data in transit
    - **Storage DLP System**
        - Software installed on servers in the datacenter to inspect the data at rest
    - **Cloud DLP System**
        - Cloud software as a service that protects data being stored in cloud services
- **Securing the BIOS**
  - **Basic Input Output System**
    - Firmware that provides the computer instructions for how to accept input and send output
    - Unified Extensible Firmware Interface (UEFI)
    - BIOS and UEFI are used interchangeable in this lesson
  - **1. Flash the BIOS**
  - **2. Use a BIOS password**
  - **3. Configure the BIOS boot order**
  - **4. Disable the external ports and devices**

    - **5. Enable the secure boot option**
- **Storage Storage Devices**
    - **Removable media comes in many different formats**
        - You should always encrypt files on removable media
    - **Removable media controls**
        - Technical limitations placed on a system in regards to the utilisation of USB storage devices and other removable media
        - Create administrative controls such as policies
    - **Network Attached Storage (NAS)**
        - Storage devices that connect directly to your organisation's network
        - NAS systems often implement RAID arrays to ensure high availability
    - **Storage Area Network (SAN)**
        - Network designed specifically to perform block storage functions that may consist of NAS devices
        - **1. Use data encryption**
        - **2. Use proper authentication**
        - **3. Log NAS access**
- **Disk Encryption**
    - **Encryption scrambles data into unreadable information**
    - **Self-Encryption Drive (SED)**
        - Storage device that performs whole disk encrpytion by using embedded hardware
    - **Encryption software is most commonly used**
        - FileVault
        - BitLocker
    - **Trusted Platform Module (TPM)**
        - Chip residing on the motherboard that contains an encryption key
        - If your motherboard doesn't have TPM, you can use an external USB drive as a key
    - **Advanced Encryption Standard**
        - Symmetric key encryption that supports 128-bit and 256-bit keys
    - **Encrpytion adds security but has lower performance**
    - **Hardware Security Module (HSM)**
        - Physical devices that act as a secure cryptoprocessor during the encryption process.
- **Endpoint analysis**
    - **Anti-Virus (AV)**
        - Software capable of detecting and removing virus infections and (in most cases) other types of malware, such as worms, Trojans, rootkits, adware, spyware, password crackers, network mappers, DoS tools, and others
    - **Host-based IDS/IPS (HIDS/HIPS)**
        - A type of IDS or IPS that monitors a computer system for unexpected behaviour or drastic changes to the system's state on an endpoint.
    - **Endpoint Protection Platform (EPP)**
        - A software agent and monitoring system that performs multiple security tasks such as anti-virus, HIDS/HIPS, firewall, DLP, and file encryption

    - **Endpoint Detection and Response (EDR)**
        - A software that collects system data and logs for analysis by a monitoring system to provide early detection of threats
    - **User and Entity Behaviour Analytics (UEBA)**
        - A system that can provide automated identification of suspicious activity by user accounts and computer hosts
        - UEBA solutions are heavily dependent on advanced computing techniques like artificial intelligence (AI) and machine learning.
        - Many companies are now marketing advanced threat protection (ATP), advanced endpoint protection (AEP), and NextGen AV (NGAV) which is a hybrid of EPP, EDR, and UEBA.

Mobile Device Security

- **Mobile Device Security**
- **Securing Wireless Devices**
    - **WiFi Protected Access 2 (WPA2) is the highest level of wireless security**
    - **AES**
        - Advanced Encryption Standard
    - **Bluetooth pairing creates a shared link key to encrypt the connection**
    - **Wired devices are almost always more secure than wireless ones**
- **Mobile Malware**
    - **Ensure your mobile device is patched and updated**
    - **Only install apps from the official App Store or Play Store**
    - **Do not jailbreak/root device**
    - **Don't use custom firmware or a custom ROM**
    - **Only load official store apps**
    - **Always update your phone's operating system**
- **SIM Cloning & ID Theft**
    - **Subscriber Identity Module (SIM)**
        - Integrated circuit that securely stores the international mobile subscriber identity (IMSI) number and its related key
        - **SIM Cloning**
            - Allows two phones to utilise the same service and allows an attacker to gain access to the phone's data
            - SIM v1 cards were easy to clone but newer SIM v2 cards are much harder
            - Be careful with where you post phone numbers
- **Bluetooth Attacks**
    - **Bluejacking**
        - Sending of unsolicited messages to Bluetooth-enabled devices
    - **Bluesnarfing**
        - Unauthorised access of information from a wireless device over a Bluetooth connection
    - **Bluejacking sends information to a device**
    - **Bluesnarfing takes information from a device**

- **Mobile Device Theft**
  - **Always ensure your device is backed up**
  - **Don't try to recover your device alone if it is stolen**
  - **Remote Lock**
    - Requires a PIN or password before someone can use the device
    - **Remote Wipe**
      - Remotely erase the contents of the device to ensure the information is not recovered by the thief
- **Security of Apps**
  - **Only install apps from the official mobile stores**
  - **TLS**
    - Transport Layer Security
  - **Mobile Device Management**
    - Centralised software solution that allows system administrators to create and enforce policies across its mobile devices
  - **Turn location services off to ensure privacy**
    - **Geotagging**
      - Embedding of the geolocation coordinates into a piece of data (i.e., a photo)
    - **Geotagging should be considered when developing your organisation's security policies**
- **Bring Your Own Device**
  - **BYOD introduces a lot of security issues to consider**
  - **Storage Segmentation**
    - Creating a clear separation between personal and company data on a single device
  - **Mobile Device Management**
    - Centralised software solution for remote administration and configuration of mobile devices
  - **CYOD**
    - Choose Your Own Device
  - **MDM can prevent certain applications from being installed on the device**
  - **Ensure your organisation has a good security policy for mobile devices**
- **Hardening Mobile Devices**
  - **1. Update your device to the latest version of the software**
  - **2. Install AntiVirus**
  - **3. Train users on proper security and use of the device**
  - **4. Only install apps from the official mobile stores**
  - **5. Do not root or jailbreak your devices**
  - **6. Only use v2 SIM cards with your devices**
  - **7. Turn off all unnecessary features**
  - **8. Turn on encryption for voice and data**
  - **9. Use strong passwords or biometrics**
  - **10. Don't allow BYOD**
  - **Ensure your organisation has a good security policy for mobile devices**

Hardening

- **Hardening**
  - **Hardening**
    - Act of configuring an operating system securely by updating it, creating rules and policies to govern it, and removing unnecessary applications and services
  - **We are not guaranteed security, but we can minimise the risk...**
  - **Mitigate risk by minimising vulnerabilities to reduce exposure to threats**
- **Unnecessary Applications**
  - **Least functionality**
    - Process of configuring workstation or server to only provide essential applications and services
  - **Personal computers often accumulate unnecessary programs over time**
  - **Utilise a secure baseline image when adding new computers**
  - **SCCM**
    - Microsoft's System Center Configuration Management
- **Restricting Applications**
  - **Application Whitelist**
    - Only applications that are on the list are allowed to be run by the operating system
  - **Application Blacklist**
    - Any application placed on the list will be prevented from running while others will be permitted to run
  - **Whitelisting and blacklisting can be centrally managed**
- **Unnecessary Services**
  - **Any services that are unnedeed should be disabled in the OS**
- **Trusted Operating Systems**
  - **Trusted Operating Systems (TOS)**
    - An operating system that meets the requirements set forth by government and has multilevel security
    - Windows 7 (and newer)
    - Mac OS X 10.6 (and newer)
    - FreeBSD (TrustedBSD)
    - Red Hat Enterprise Server
  - **You need to identify the current version and build prior to updating a system Updates and Patches**
- **Updates and Patches**
  - **Patches**
    - A single problem-fixing piece of software for an operating system or application
  - **Hotfix**
    - A single problem-fixing piece of software for an operating system or application
  - **Patches and Hotfixes are now used interchangeably by most manufacturers**
  - **Categories of Updates**
    - Security Update

        - Software code that is issued for a product-specific security-related vulnerability
    - Critical Update
        - Software code for a specific problem addressing a critical, non-security bug in the software
    - Service Pack
        - A tested, cumulative grouping of patches, hotfixes, security updates, critical updates, and possibly some feature or design changes
    - Windows Update
        - Recommended update to fix a noncritical problem that users have found, as well as to provide additional features or capabilities
    - Driver Update
        - Updated device driver to fix a security issue or add a feature to a supported piece of hardware
    - Windows 10 uses the Windows Update program (wuapp.exe) to manage updates
- **Patch Management**
    - **Patch Management**
        - Process of planning, testing, implementing, and auditing of software patches
        - Planning
        - Testing
        - Implementing
        - Auditing
    - **Verifying it is compatible with your systems and plan for how you will test and deploy it**
    - **Always test a patch prior to automating its deployment**
    - **Manually or automatically deploy the patch to all your clients to implement it**
    - **Large organisations centrally manage updates through an update server**
    - **Disable the wuauserv service to prevent Windows Update from running automatically**
    - **It is important to audit the client's status after patch deployment**
    - **Linux and OSX also have built-in patch management systems**
- **Group Policies**
    - **Group Policy**
        - A set of rules or policies that can be applied to a set of users or computer accounts within the operating system
        - Access the Group Policy Editor by opening the Run prompt and enter gpedit
        - Password complexity
        - Account lockout policy
        - Software restrictions
        - Application restrictions
    - **Active Directory domain controllers have a more advanced Group Policy Editor**
    - **Security Template**
        - A group of policies that can be loaded through one procedure
    - **Group Policy objectives (GPOs) aid in the hardening of the operating system**

    - **Baselining**
        - Process of measuring changes in the network, hardware, and software environment
        - A baseline establishes what is normal so you can find deviations
- **File Systems and Hard Drives**
    - **Level of security of a system is affected by its file system type**
        - NTFS
        - FAT32
        - ext4
        - HFS+
        - APFS
    - **Windows systems can utilise NTFS or FAT32**
    - **NTFS**
        - New Technology File System is the default file system format for Windows and is more secure because it supports logging, encryption, larger partition sizes, and larger file sizes than FAT32
    - **Linux systems should use ext4 and OSX should use the APFS**
    - **All hard drives will eventually fail**
        - 1. Remove temporary files by using Disk Cleanup
        - 2. Periodic system file checks
        - 3. Defragment your disk drive
        - 4. Back up your data
        - 5. Use and practice restoration techniques

Supply Chain Assessment

- Secure working in an unsecure environment involves mitigating the risks of the supply chain
- An organisation must ensure that the operation of every element (hardware, firmware, driver, OS, and application) is consistent and tamper resistant to establish a trusted computing environment
    - **Due Diligence**
        - A legal principle identifying a subject has used best practice or reasonable care when setting up, configuring, and maintaining a system.
            - Properly resourced cyber security program
            - Security assurance and risk management processes
            - Product support life cycle
            - Security controls for confidential data
            - Incident response and forensics assistance
            - General and historical company information
        - Due diligence should apply to all suppliers and contractors
    - **Trusted Foundry**
        - A microprocessor manufacturing utility that is part of a validated supply chain (one where hardware and software does not deviate from its documented function)

        - Trusted Foundry Program is operated by the Department of Defense (DoD)
    - **Hardware Source Authenticity**
        - The process of ensuring that hardware is procured tamper-free from trustworthy suppliers
        - Greater risk of inadvertently obtaining counterfeited or compromised devices when purchasing from second-hand or aftermarket sources
- **Root of Trust**
    - **Hardware Root of Trust (ROT)**
        - A cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics
        - A hardware root of trust is used to scan the boot metrics and OS files to verify their signatures, which we can then use to sign a digital report
    - **Trusted Platform Module (TPM)**
        - A specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information
        - A TPM can be managed in Windows via the tpm.msc console or through group policy
    - **Hardware Security Module (HSM)**
        - An appliance for generating and storing cryptographic keys that is less susceptible to tampering and insider threats than software-based storage
    - **Anti-Tamper**
        - Methods that make it difficult for an attacker to alter the authorized execution of software
        - Anti-tamper mechanisms include a field programmable gate array (FPGA) and a physically unclonable function (PUF)
- **Trusted Firmware**
    - A firmware exploit gives an attacker an opportunity to run any code at the highest level of CPU privilege
        - **Unified Extensible Firmware Interface (UEFI)**
            - A type of system firmware providing support for 64-bit CPU operation at boot, full GUI and mouse operation at boot, and better boot security
        - **Secure Boot**
            - A UEFI feature that prevents unwanted processes from executing during the boot operation
        - **Measured Boot**
            - A UEFI feature that gathers secure metrics to validate the boot process in an attestation report
        - **Attestation**
            - A claim that the data presented in the report is valid by digitally signing it using the TPM's private key
        - **eFUSE**
            - A means for software or firmware to permanently alter the state of a transistor on a computer chip

        - **Trusted Firmware Updates**
            - A firmware update that is digitally signed by the vendor and trusted by the system before installation
        - **Self-Encrypting Drives**
            - A disk drive where the controller can automatically encrypt data that is written to it
- **Secure Processing**
    - A mechanism for ensuring the confidentiality, integrity, and availability 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)
                  Secure Encrypted Virtualisation (SEV)
            - Intel
                - Trusted Execution Technology (TXT)
                  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**
        - The extensions allow a trusted process to create an encrypted container for sensitive data
    - **Atomic Execution**
        - Certain operations that should only be performed once or not at all, such as initializing a memory location
    - **Bus Encryption**
        - Data is encrypted by an application prior to being placed on the data bus
        - Ensures that the device at the end of the bus is trusted to decrypt the data

Virtualisation

- **Virtualization**
    - **Virtualisation**
        - Creation of a virtual resource
    - **A virtual machine is a container for an emulated computer that runs an entire operating system**
    - **VM Types**
        - System Virtual Machine
            - Complete platform designed to replace an entire physical computer and includes a full desktop/server operating system
        - Processor Virtual Machine
            - Designed to only run a single process or application like a virtualised web browser or a simple web server

    - **Virtualisation continues to rise in order to reduce the physical requirements for data centres**
- **Hypervisors**
    - **Hypervisor**
        - Manages he distribution of the physical resources of a host machine (server) to the virtual machines being run (guests)
        - Type I (bare metal) hypervisors are more efficient that Type II
    - **Container-based**
        - Application Containerisation
            - A single operating system kernel is shared across multiple virtual machines but each virtual machine receives its own user space for programs and data
            - Containerisation allows for rapid and efficient deployment of distributed applications
    - **Docket**
    - **Parallels Virtuozzo**
    - **OpenVZ**
- **Threats to VMs**
    - **VM Escape**
        - An attack that allows an attacker to break out of a normally isolated VM by interacting directly with the hypervisor
        - Elasticity allows for scaling up or down to meet user demans
    - **Data Remnants**
        - Contents of a virtual machine that exists as deleted files on a cloud-based server after deprovisioning of a virtual machine.
    - **Privilege Escalation**
        - Occurs when a user is able to grant themselves the ability to run functions as a higher-level user
    - **Live migration occurs when a VM is moved from one physical server to another over the network**
- **Securing VMs**
    - **Uses many of the same security as a physical server**
        - Limit connectivity between the virtual machine and the host
        - Remove any unnecessary pieces of virtual hardware from the virtual machine
        - Using proper patch management is important to keeping your guest's operating system secure
    - **Virtualisation Sprawl**
        - Occurs when virtual machines are created, used, and deployed without proper management or oversight by the system admins

Application Security

- **Application Security**
- **Web Browser Security**
    - **Ensure your web browser is up-to-date with patches...**

        - But don't adopt the newest browser immediately
    - **Which web browser should I use?**
    - **General Security for Web Browsers**
        1. Implement Policies
            - Create and implement web browsing policies as an administrative control or technical control
        2. Train Your Users
            - User training will prevent many issues inside your organisation
        3. Use Proxy & Content Filter
            - Proxies cache the website to reduce requests and bandwidth usage
            - Content filters can be used to blacklist specific websites or entire categories of sites
        4. Prevent Malicious Code
            - Configure your browsers to prevent ActiveX controls, Java applets, JavaScript, Flash, and other active content
- **Web Browser Concerns**
    - **Cookies**
        - Text files placed on a client's computer to store information about the user's browsing habits, credentials, and other data
    - **Locally Shared Object (LSO)**
        - Also known as Flash cookies, they are stored in your Windows user profile under the Flash folder inside of your AppData folder
    - **Add-Ons**
        - Smaller browser extensions and plugins that provide additional functionality to the browser
    - **Advanced Security Options**
        - Browser configuration and settings for numerous options such as SSL/TLS settings, local storage/cache size, browsing history, and much more
- **Securing Applications**
    - **Use passwords to protect the contents of your documents**
    - **Digital signatures and digital certificates are used by MS Outlook for email security**
    - **User Account Control**
        - Prevent unauthorised access and avoid user error in the form of accidental changes

Secure Software Development

- **Software Development**
    - **SDLC**
        - Software Development Life Cycle
        - SDLC is an organised process of developing a secure application throughout the life of the project
    - **Agile**

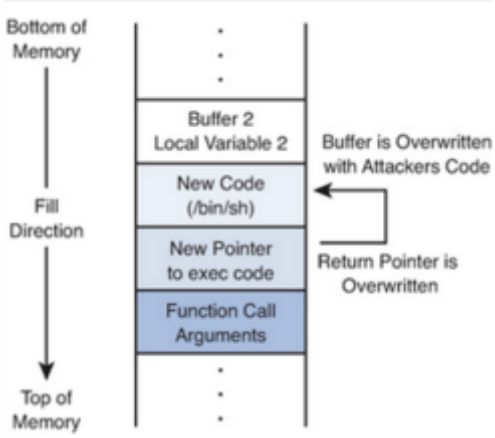
        - Software development is performed in time-boxed or small increments to allow more adaptivity to change
    - **DevOps**
        - Software development and information technology operations
- **SDLC Principles**
    - **Developers should always remember confidentiality, integrity, and availability**
        - Confidentiality
            - Ensures that only authorised users can access the data
        - Integrity
            - Ensures that the data is not modified or altered without permission
        - Availability
            - Ensuring that data is available to authorised users when it is needed
    - **Threat modelling helps to prioritise vulnerability identification and patching**
    - **Least Privilege**
        - Users and processes should be run using the least amount of access necessary to perform a given function
    - **Defense in Depth**
        - Layering of security controls is more effective and secure than relying on a single control
    - **Never Trust User Input**
        - Any input that is received from a user should undergo input validation prior to allowing it to be utilised by an application
    - **Minimise Attack Surface**
        - Reduce the amount of code used by a program, eliminate unneeded functionaility, and require authentication prior to running additional plugins
    - **Create Secure Defaults**
        - Default installations should include secure configurations instead of requiring an administrator or user to add in additional security
    - **Authenticity and Integrity**
        - Applications should be deployed using code signing to ensure the program is not changed inadvertently or maliciously prior to delivery to an end user
    - **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
    - **Rely on Trusted SDKs**
        - SDKs must come from trusted source to ensure to malicious code to being added
- **Testing Methods**
    - **System Testing**
        - Black-box Testing
            - Occurs when a tester is not provided with any information about the system or program prior to conducting the test

        - White-box Testing
            - Occurs when a tester is provided full details of a system including the source code, diagrams, and user credentials in order to conduct the test
    - **Structured Exception Handling (SEH)**
        - Provides control over what the application should do when faced with a runtime or syntax error
    - **Programs should use input validation when taking data from users**
        - Input Validation
            - Applications verify that information received from a user matches a specific format or range of values
        - Example

```
get $ssn

if ($ssn >=000-00-0000 and
$ssn <= 999-99-9999)

then [do function]

else [conduct error handling]
```

    - **Static Analysis**
        - Source code of an application is reviewed manually or with automatic tools without running the code
    - **Dynamic Analysis**
        - Analysis and testing of a program occurs while it is being executed or run
    - **Fuzzing**
        - Injection of randomised data into a software program in an attempt to find system failures, memory leaks, error handling issues, and improper input validation
- **Software Vulnerabilities and Exploits**
    - **Backdoors**
        - Code placed in computer programs to bypass normal authentication and other security mechanisms
        - Backdoors are a poor coding practice and should not be utilised
    - **Directory Traversal**
        - Method of accessing unauthorised directories by moving through the directory structure on a remote server
    - **Arbitrary Code Execution**
        - Occurs when an attacker is able to execute or run commands on a victim computer
    - **Remote Code Execution (RCE)**
        - Occurs when an attacker is able to execute or tun commands on a remote computer
    - **Zero Day**
        - Attack against a vulnerability that is unknown to the original developer or manufacturer
- **Buffer Overflows**

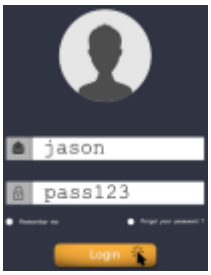
- **Buffer Overflow**
  - Occurs when a process stores data outside the memory range allocated by the developer
- **Buffer**
  - A temporary storage area that a program uses to store data
  - Over 85% of data breaches were caused by a buffer overflow
- **Let's get technical...**
  - Stack
    - Reserved 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 until it finds the attacker's code to run.
  - Address Space Layout Randomization
    - Method used by programmers to randomly arrange the different address spaces used by a program or process to prevent buffer overflow exploits
- **Buffer overflows attempt to put more data into memory than it is designed to hold**

- **XSS and XSRF**
  - **Cross-Site Scripting (XSS)**
    - Occurs when an attacker embeds malicious scripting commands on a trusted website
    - Stored/Persistent
      - Attempts to get data provided by the attacker to be saved on the web server by the victim
    - Reflected
      - Attempts to have a non-persistent effect activated by a victim clicking a link on the site
    - DOM-based
      - Attempt to exploit the victim's web browser
    - Prevent XSS with output encoding and proper input validation
  - **Cross-Site Request Forgery (XSRF/CSRF)**
    - Occurs when an attacker forces a user to execute actions on a web server for which they are already authenticated

        - Prevent XSRF with tokens, encryption, XML file scanning, and cookie verification
- **SQL Injection**
    - **SQL Injection**
        - Attack consisting of the insertion or injection of an SQL query via input data from the client to a web application
    - **Injection Attack**
        - Insertion of additional information or code through data input from a client to an application
            - SQL
            - HTML
            - XML
            - LDAP
        - Most common type is an SQL Injection
    - **How does a normal SQL request work?**



    - **How does an SQL injection work?**

        - SQL injection is prevented through input validation and using least privilege when accessing a database
        - If you see ` OR 1=1; on the exam, it's an SQL injection
- **XML Vulnerabilities**
    - 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
        - XML External Entity (XXE)
            - An attack that embeds a request for a local resource
            - To prevent XML vulnerabilities from being exploited, use proper input validation
- **Race Conditions**
    - A 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 of intended by the developer.

    - A race condition vulnerability is found where multiple threads are attempting to write a variable or object at the same memory location
        - Dereferencing
            - A software vulnerability that occurs when the code attempts to remove the relationship between a pointer and the thing it points to.
            - Race conditions are difficult to detect and mitigate
            - Race conditions can also be used against databases and file systems
    - Time of Check to Time of Use (TOCTTOU)
        - The potential vulnerability that occurs when there is a change between when an app checked a resource and when the all used the resource
        - How can you prevent race conditions and TOCTTOU?
            - Develop applications to not process things sequentially if possible
            - Implement a locking mechanism to provide app with exclusive access
- **Design Vulnerabilities**
    - Vulnerabilities often arise from the general design of the software code
        - Insecure Components
            - Any code that is used or invoked outside the main program development process
                - Code Reuse
                - Third-party Library
                - Software Development Kit (SDK)
        - Insufficient Logging and Monitoring
            - Any program that does not properly record or log detailed enough information for an analyst to perform their job
            - Logging and monitoring must support your use case and answer who, what, when, where, and how
        - Weak of Default Configurations
            - Any program that uses ineffective credentials or configurations, or one in which the defaults have not be changed for security
            - Many application choose to simply run as root or as a local admin
            - Permissions may be too permissive on files or directories due to weak configurations
    - BEST PRACTICE: Utilise scripted installations and baseline configuration templates to secure applications during installation

Network Design

- **Network Security**
    - **OSI Model**
        - Used to explain network communications between a host and remote device over a LAN or WAN
    - **Physical Layer**
        - Represents the actual network cables and radio waves used to carry data over a network
        - Bits
    - **Data Link layer**

        - Describes how a connection is established, maintained, and transferred over the physical layer and uses physical addressing (MAC addresses)
        - Frames
    - **Network Layer**
        - Uses logical address to route or switch information between hosts, the network, and the internetworks
        - Packets
    - **Transport Layer**
        - Manages and ensures transmission of the packets occurs from a host to a destination using either TCP or UDP
        - Segments (TCP) or Datagrams (UDP)
    - **Session Layer**
        - Manages the establishment, termination, and synchronisation of a session over the network
    - **Presentation Layer**
        - Translates the information into a format that the sender and receiver both understand
    - **Application Layer**
        - Layer from which the message is created, formed, and originated
        - Consists of high-level protocols like HTTP, SMTP, and FTP
- **Switches**
    - **Switches are the combined evolution of hubs and bridges**
    - **MAC Flooding**
        - Attempt to overwhelm the limited switch memory set aside to store the MAC addresses for each port
        - Switches can fail-open when flooded and begin to act like a hub
    - **MAC Spoofing**
        - Occurs when an attacker masks their own MAC address to pretend they have the MAC address of another device
        - MAC Spoofing is often combined with ARP spoofing attack
        - Limit static MAC addresses accepted
        - Limit duration of time for ARP entry on hosts
        - Conduct ARP inspection
    - **Physical Tampering**
        - Physical tampering occurs when an attacker attempts to gain physical access
- **Routers**
    - **Routers operate at Layer 3**
        - **Routers**
            - Used to connect two or more networks to form an internetwork
            - Routers rely on a packet's IP Addresses to determine the proper destination
            - Once on the network, it conducts an ARP request to find final destination
        - **Access Control List**
            - An ordered set of rules that a router uses to decide whether to permit or deny traffic based upon given characteristics
            - IP Spoofing is used to trick a router's ACL

- **Network Zones**
  - **Any traffic you wish to keep confidential crossing the internet shouls use a VPN**
  - **De-militarised Zone (DMZ)**
    - Focused on providing controlled access to publicly available servers that are hosted within your organoisational network
    - Sub-zones can be crated to provide additional protection for some servers
  - **Extranet**
    - Specialised type of DMZ that is created for your partner organisations to access over a wide network
    - **Intranets are used when only one company is involved**
- **Jumpbox**
  - **Internet-facing Host**
    - Any host that accepts inbound connections from the internet
  - **Demilitarised Zone (DMZ)**
    - 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
  - **Bastion Hosts**
    - Hosts or servers in the DMZ which are not configured with any services that run on the local network
    - To configure devices with the DMZ, a jumpbox is utilised
    - **Jumpbox**
      - A hardened server that provides access to other hosts within the DMZ
      - An administrator connects to the jumpbox and the jumpbox connects to hosts in the DMZ
      - The jumpbox and management workstation should only have the minimum required software to perform their job and be well hardened
- **Network Access Control**
  - **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 a device fails the inspection, it is placed into digital quarantine
  - **Persistent Agents**
    - A piece of software that scan the device remotely or is installed and subsequently removed after the scan
  - **NAC can be used as a hardware or software solution**
  - **IEEE 802.1x standard is used in port-based NAC**
- **VLANs**
  - **Segment the network**
  - **Reduce collisions**
  - **Organise the network**
  - **Boost performance**
  - **Increase security**

    - **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
    - **Double Tagging**
        - Attacker adds an additional VLAN tag to create an outer and inner tag
        - Prevent double tagging by moving all ports out of the default VLAN group
- **Subnetting**
    - **Subnetting**
        - Act of creating subnetworks logically through the manipulation of IP addresses
        - Efficient use of IP addresses
        - Reduced broadcast traffic
        - Reduced collisions
        - Compartmentalised
    - **Subnet's policies and monitoring can aid in the security of your network**
- **Network Address Translation**
    - **Network Address Translation (NAT)**
        - Process of changing an IP address while it transits across a router
        - Using NAT can help us to 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
    - **Class A**
        - 10.0.0.0 to 10.255.255.255
    - **Class B**
        - 172.16.0.0 to 172.31.255.255
    - **Class C**
        - 192.168.0.0 to 192.168.255.255
- **Telephony**
    - **Telephony**
        - Term used to describe devices that provide voice communication to users
    - **Modem**
        - A device that could modulate digital information into an analog signal for transmission over a standard dial-up phone line
    - **War Dialing**
        - Protect dial-up resources by using callback feature
    - **Public Branch Exchange (PBX)**
        - Internal phone system used in large organisations
    - **Voice Over Internet Protocol (VoIP)**
        - Digital phone service provided by software or hardware devices over a data network
    - **Quality of Service (QoS)**

Perimeter Security

- **Perimeter Security**

    - Security devices focused on the boundary between the LAN and the WAN in your organisation's network
    - Perimeter security relies on several different devices
- **Firewalls**
    - **Firewalls screen traffic between two portions of a network**
        - Software
        - Hardware
        - Embedded
    - **Packet Filtering**
        - Inspects each packet passing through the firewall and accepts or rejects it based on the rules
        - Stateless Packet Filtering
        - Stateful packet filtering tracks the requests leaving the network
    - **NAT Filtering**
        - Filters traffic based upon the ports being utilised and type of connection (TCP or UDP)
    - **Application-layer gateway conducts an in-depth inspection based upon the application being used**
    - **Circuit-Level gateway**
        - Operates at the session layer and only inspects the traffic during the establishment of the initial session over TCP or UDP
    - **MAC Filtering**
    - **Explicit Allow**
        - Traffic is allowed to enter or leave the network because there is an ACL rule that specifically allows it
        - Example: allow TCP 10.0.0.2 any port 80
    - **Explicit Deny**
        - Traffic is denied the ability to enter or leave the network because there is an ACL rule that specifically denies it
        - Example: deny TCP any any port any
    - **Most operate at Layer 3 (blocking IP addresses) and Layer 4 (blocking ports)**
    - **Web Application Firewall**
        - Firewall installed to protect your server by inspecting traffic being sent to a web application
        - A WAF can prevent a XSS or SQL injection
- **Proxy Server**
    - **Proxy Server**
        - A device that acts as a middle man between a device and a remote server
        - IP Proxy
            - IP Proxy is used to secure a network by keeping its machines anonymous during web browsing
        - Caching Proxy
            - Attempts to serve client requests by delivering content from itself without actually contacting the remote server
            - Disable Proxy Auto-Configure (PAC) files for security

        - Internet Content Filter
            - Used in organisations to prevent users from accessing prohibited websites and other content
        - Web Security Gateway
            - A go-between device that scans for viruses, filters unwanted content, and performs data loss prevention functions
- **Honeypots and Honeynets**
    - **Honeypots and honeynets are used to attract and trap potential hackers**
    - **Honeypot**
        - A single computer (or file, group of files, or IP range) that might be attractive to an attacker
        - **Honeynet**
            - A group of computers, servers, or networks used to attract an attacker
        - **Honeypots are normally used in security research**
- **Data Loss Prevention**
    - **Data Loss Prevention**
        - Systems designed to protect data by conducting content inspection of data being sent out of the network
        - Also called Information Leak Protection (ILP) or Extrusion Prevention Systems (EPS)
        - DLP is used to ensure your private data remains secure
- **NIDS bs NIPS**
    - **Network Intrusion Detection Systems**
        - Attempts to detect, log, and alert on malicious network activities
        - NIDS use promiscuous mode to sell network traffic on a segment
    - **Network Intrusion Prevention Systems**
        - Attempts to remove, detain, or redirect malicious traffic
        - NIPS should be installed in-line of the network traffic flow
        - Should a NIPS fail open or fail shut?
        - NIPS can also perform functions as a protocol analyser
- **Unified Threat Management**
    - **Relying on a firewall is not enough**
    - **Unified Threat Management**
        - Combination of network security devices and technologies to provide more defence in depth within a single device
        - UTM may include a firewall, NIDS/NIPS, content filter, ant-malware, DLP, and VPN
        - UTM is also known as a Next Generation Firewall (NGFW)

Cloud Security

- **Cloud Computing**
    - **Cloud Computing**
        - A way of offering on-demand services that extend the traditional capabilities of a computer or network
        - Cloud computing relies on virtualisation to gain efficiencies and cost savings

    - **Hyperconvergence allows providers to fully integrate the storage, network, and servers**
    - **Virtual Desktop Infrastructure (VDI)**
        - VDI allows a cloud provider to offer a full desktop operating system to an end user from a centralised server
    - **Secure Enclaves and Secure Volumes**
- **Cloud Types**
    - **Public Cloud**
        - A service provider makes resources available to the end users over the Internet
    - **Private Cloud**
        - A company creates its own cloud environment that only it can utilise as an internal enterprise resource
        - A private cloud should be chosen when security is more important than cost
    - **Hybrid**
    - **Community Cloud**
        - Resources and costs are shared among several different organisations who have common service needs
- **As a Service**
    - **Software as a Service (SaaS)**
        - Provides all the hardware, operating system, software, and applications needed for a complete service to be delivered
    - **Infrastructure as a Service (IaaS)**
        - Provides all the hardware, operating system, and backend software needed in order to develop your own software or service
    - **Platform as a Service (PaaS)**
        - Provides your organisation with the hardware and software needed for a specific service to operate
    - **Security as a Service (SECaaS)**
        - Provides your organisation with various types of security services without the need to maintain a cybersecurity staff
        - Anti-malware solutions were one of the first SECaaS products
    - **Some solutions may not scan all the files on your system**
    - **Cloud-based vulnerability scans can better provide the attacker's perspective**
    - **Your vulnerability data may not be stored on the cloud provider's server**
    - **Sandboxing**
        - Utilises separate virtual networks to allow security professionals to test suspicious or malicious files
    - **Data Loss Prevention (DLP)**
    - **Continuous Monitoring**
    - **Access Control**
    - **Identity Management**
    - **Business Continuity**
    - **Disaster Recovery**

- **Cloud Security**
  - **Collocated data can become a security risk**
  - **Configure, manage, and audit user access to virtualised servers**
  - **Utilising the cloud securely requires good security policies**
  - **Data remnants may be left begin after deprovisioning**
- **Defending Servers**
  - **File Servers**
    - Servers are used to store, transfer, migrate, synchronise, and archive files for your organisation
  - **Email servers are a frequent target of attacks for the data they hold**
  - **Web servers should be placed in your DMZ**
  - **FTP Server**
    - A specialised type of file server that is used to host files for distribution across the web
    - FTP servers should be configured to require TLS connections
  - **Domain Controller**
    - A server that acts as a central repository of all the user accounts and their associated passwords for the network
  - **Active Directory is targeted for privilege escalation and lateral movement**
- **Cloud-based Infrastructure**
  - Cloud-based infrastructure must be configured to provide the same level of security as a local solution
- **Virtual Private Cloud (VPC)**
  - A private network segment made available to a single cloud consumer within a public cloud
  - The consumer is responsible for configuring the IP address space and routing within the cloud
  - VPC is typically used to provision internet-accessible applications that need to be accessed from geographically remote sites
  - On-premise solutions maintain their servers locally within the network
  - Many security products offer cloud-based and on-premise versions
  - Consider compliance or regulatory limitations of storing data in a cloud-based security solution
  - Be aware of the possibility of vendor lock in
- **CASB**
  - **Cloud Access Security Broker (CASB)**
    - Enterprise management software designed to mediate access to cloud services by users across all types of devices
      - Single sign-on
      - Malware and rogue device detection
      - Monitor-audit user activity
      - Mitigate data exfiltration
    - Cloud Access Service Brokers provide visibility into how clients and other network nodes use cloud services
      - **Forward Proxy**

        - A security appliance or host positioned at the client network edge that forwards user traffic to the cloud network if the contents of that traffic comply with policy
        - WARNING: Users may be able to evade the proxy and connect directly
    - **Reverse Proxy**
        - An appliance positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with policy
        - WARNING: This approach can only be used if the cloud application has proxy support
    - **Application Programming Interface (API)**
        - A method that uses the brokers connections between the cloud service and the cloud consumer
        - WARNING: Dependant on the API supporting the functions that your policies demans
- **API**
    - **Application Programming Interface (API)**
        - A library of programming utilities used to enable software developers to access functions of another application
        - APIs allow for the automated administration, management, and monitoring of a cloud service
    - **curl**
        - A tool to transfer data from or to a server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP, FILE)
- **FAAS and Serverless**
    - **Function as a Service (FAAS)**
        - A cloud service model that supports serverless software architecture by provisioning runtime containers in which code is executed in a particular programming language
    - **Serverless**
        - A software architecture that runs functions within virtualised runtime containers in a cloud rather than on dedicated server instances
        - Everything in serverless is developed as a function or microservice
        - Serverless eliminates the need to manage physical or virtual servers
            - No patching
            - No administration
            - No file system monitoring
        - The underlying architecture is managed by the cloud service provider
        - Ensure that the clients accessing the services have not been compromised
        - Serverless depends on orchestration
- **Cloud Threats**
    - **Insecure Application Programming Interface (API)**
        - WARNING: An API must only be used over an encrypted channel (HTTPS)
        - Data received by an API must pass service-side validation routines
        - Implement throttling/rate-limiting mechanisms to protect from a DoS
    - **Improper Key Management**

        - APIs should use secure authentication and authorisation such as SAML or OAuth/OIDC before accessing data
        - WARNING: Do not hardcode or embed a key into the source code
        - Do not create one key with full control to access an application's functions
        - Delete unnecessary keys and regenerate keys when moving into a production environment
    - **Insufficient Logging and Monitoring**
        - WARNING: Software as a service may not supply access to log files or monitoring tools
        - Logs must be copied to non-elastic storage for long-term retention
    - **Unprotected Storage**
        - Cloud storage containers are referred to as buckets or blobs
        - WARNING: Access control to storage is administered through container policies, IAM authorisations, and object ACLs
        - Incorrect permissions may occur due to default read/write permissions leftover from creation
        - Incorrect origin settings may occur when using content delivery networks
    - **Cross Origin Resource Sharing (CORS) Policy**
        - A content delivery network policy that instructs the browser to treat requests from nominated domains as safe
        - WARNING: Weak CORS policies expose the site to vulnerabilities like XSS

Workflow Orchestration

- **Orchestration**
    - The automation of multiple steps in a deployment process
    - Orchestration is the automation of the automations
    - Rapid elasticity in cloud computing would not be possible without orchestration
        - Resource Orchestration
        - Workload Orchestration
        - Service Orchestration
    - Third-Party orchestration platform is protection from vendor lock in
        - Chef
        - Puppet
        - Ansible
        - Docker
        - Kubernetes
        - GitHub
- **CI/CD**
    - Development
    - Testing/Integration
    - Staging
    - Production
    - **Continuous Integration**
        - A software development method where code updates are tested and committed to a development or build server/code repository rapidly

        - Continuous Integration can test and commit updates multiple times per day
        - Continuous integration detects and resolves development conflicts early and often
    - **Continuous Delivery**
        - A software development method where application and platform requirements are frequently tested and validated for immediate availability
    - **Continuous Development**
        - A software development method where application and platform updates are committed to production rapidly
        - Continuous delivery focuses on automated testing of code in order to get it ready for release
        - Continuous development focuses on automated testing and release of code in order to get it into the production environment more quickly
- **DevSecOps**
    - **DevOps**
        - An organisational culture shift that combines software development and systems operations by referring to the practice of integrating the two disciplines within a company
        - Operations and developers can build, test, and release software faster and more reliably
    - **DevSecOps**
        - A combination of software development, security operations, and systems operations by integrating each discipline with the others
        - DevSecOps utilises a shift-left mindset
            - Integrate security from the beginning
            - Test during and after development
            - Automate compliance checks
- **IAC**
    - **Infrastructure as Code (IaC)**
        - A provisioning architecture in which deployment of resources is performed by scripted automation and orchestration
        - IaC allows for the use of scripted approaches to provisioning infrastructure in the cloud
        - Robust orchestration can lower overall IT costs, speed up deployments, and increase security
    - **Snowflake Systems**
        - Any system that is different in its configuration compared to a standard template within an infrastructure as code architecture
        - Lack of consistency leads to security issues and inefficiencies in support
    - **Idempotence**
        - A property of IaC that an automation or orchestration action always produces the same result, regardless of the component's previous state
        - IaC uses carefully developed and tested scripts and orchestration runbooks to generate consistent builds
- **Machine Learning**
    - **Artificial Intelligence (AI)**

        - The science of creating machines with the ability to develop problem solving and analysis strategies without significant human direction or intervention
    - **Machine Learning (ML)**
        - A component of AI that enables a machine to develop strategies for solving a task given a labelled dataset where features have been manually identified but without further explicit instructions
        - Machine learning is only as good as the datasets used to train
    - **Artificial Neural Network (ANN)**
        - An architecture of input, hidden, and output layers that can perform algorithmic analysis of a dataset to achieve outcome objectives
        - A machine learning system adjusts its neural network to reduce errors and optimise objectives
    - **Deep Learning**
        - A refinement of machine learning that enables a machine to develop strategies for solving a task given a labelled dataset and without further explicit instructions
        - Deep learning uses complex classes of knowledge defined in relation to simpler classes of knowledge to make more informed determinations about environment

Network Attacks

- **Network Attacks**
    - **Denial of Service**
    - **Spoofing**
    - **Hijacking**
    - **Replay**
    - **Transitive Attacks**
    - **DNS attacks**
    - **ARP Poisoning**
    - **Ports and protocols will be tested on the security+ exam**
- **Ports and Protocols**
    - **Port**
        - A logical communication endpoint that exists on a computer or server
    - **Inbound Port**
        - A logical communication opening on a server that is listening for a connection from a client
    - **Outbound Port**
        - A logical communication opening created on a client in order to call out to a server that is listening for a connection
    - **Ports can be any number between 0 and 65,535**
    - **Well-Known Ports**
        - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)
    - **Registered Ports**
        - Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols
    - **Dynamic or Private Ports**

        - Ports 49,152 to 65,535 can be used by any application without being registered with IANA
- **Memorisation of Ports**
    - **65,536 ports are available for use**
- **Unnecessary Ports**
    - **65,536 ports available**
    - **35 ports to memorise**
    - **Unnecessary Port**
        - Any port that is associated with a service or function that is non-essential to the operation of your computer or network
    - **Any open port represents a possible vulnerability that might be exposed**
    - **Inbound Port**
        - A logical communication opening on a server that is listening for a connection
    - **C:\ net stop service**
    - **# sudo stop service**
- **Denial of Service**
    - **Denial of Service (DoS)**
        - Term used to describe many different types of attacks which attempt to make a computer or server's resources unavailable
            - Flood Attacks
            - Ping of Death
            - Teardrop Attack
            - Permanent DoS
            - Fork Bomb
    - **Flood Attack**
        - A specialised type of DoS which attempts to send more packets to a single server or host than they can handle
    - **Ping Flood**
        - An attacker attempts to flood the server by sending too many ICMP echo request packets (which are known as pings)
    - **Smurf Attack**
        - Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (victim server), using up bandwidth and processing
    - **Fraggle Attack**
        - Attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets
    - **SYN Flood**
        - Variant of a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions but never completes the 3-way handshake
        - Food guards, time outs, and an IPS can prevent SYN Floods
    - **XMAS Attack**
        - A specialised network scan that sets the FIN, PSH, and URG flags set and can cause a device to crash or reboot
    - **Ping of Death**

        - An attacker that sends an oversized and malformed packet to another computer or server
    - **Teardrop Attack**
        - Attack that breaks apart packets into IP fragments, modifies them wth overlapping and oversized payload, and sends them to a victim machine
    - **Permanent Denial of Service**
        - Attack which exploits a security flaw permanently break networking device by refreshing its firmware
    - **Fork Bomb**
        - Attack that creates a large number of processes to use up the available processing power of a computer
- **DDoS**
    - **Distributed Denial of Service**
        - A group of compromised systems attack simultaneously a single target to create a Denial of Service (DOS)
    - **DNS Amplification**
        - Attack which relies on the large amount of DNS information that is sent in response to a spoofed query on behalf of the victimised server
- **Stopping a DDoS**
    - **GitHub suffered a 1.35 Tbps DoS**
    - **Blackholing or Sinkholing**
        - Identifies any attacking IP addresses and routes all their traffic to a non-existent server through the null interface
    - **An IPS can prevent a small-scale DDoS**
    - **Specialised security services cloud providers can stop DDoS attacks**
- **Spoofing**
    - **Spoofing**
        - Occurs when an attacker masquerades as another person by falsifying their identity
        - Anything that uniquely identifies a user or system can be spoofed
        - Proper authentication is used to detect and prevent spoofing
- **Hijacking**
    - **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
        - TCP/IP hijacking
        - Blind hijacking
        - Clickjacking
        - Man-in-the-Middle
        - Man-in-the-Browser
        - Watering hole
        - Cross-site scripting
    - **Session Theft**

        - Attacker guesses the session of ID for a web session, enabling them to take over the already authorised session of the client
    - **TCP/IP Hijacking**
        - Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access
    - **Blind Hijacking**
        - Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not
    - **Clickjacking**
        - Attack that uses multiple transparent layers to trick a user into clicking on a button or link on a page when they were intending to click on the actual page
    - **Man-in-the-Middle (MITM)**
        - Attack that causes data to flow through the attacker's computer where they can intercept or manipulate the data
    - **Man-in-the-Browser (MITB)**
        - Occurs when a Trojan infects a vulnerable web browser and modifies the web pages or transactions being done within the browser
    - **Watering Hole**
        - Occurs when malware is places on a website that the attacker knows his potential victims will access
- **Replay Attack**
    - **Replay Attack**
        - Network-based attack where a valid data transmission is fraudulently or malicious rebroadcast, repeated, or delayed
        - Multi-factor authentication can help prevent successful replay attacks
- **Transitive Attacks**
    - **Transitive Attacks aren't really an attack but more of a conceptual method**
    - **When security is sacrificed in favour of more efficient operations, additional risk exists**
- **DNS Attacks**
    - **DNS Poisoning**
        - Occurs when the name resolution information is modified in the DNS server's cache
        - If the cache is poisoned, then the user can be redirected to a malicious website
    - **Unauthorised Zone Transfer**
        - Occurs when an attacker requests replication of the DNS informaiton to their systems for use in planning future attacks
    - **Altered Hosts File**
        - Occurs when an attacker modifies the host file to have the client bypass the DNS server and redirects them to an incorrect or malicious website
        - Windows stores the hosts file in the following directory:

          \%systemroot%\system 32\drivers\etc
    - **Pharming**

        - Occurs when an attacker redirects one website's traffic to another website that is bogus or malicious
    - **Domain Name Kiting**
        - Attack that exploits a process in the registration process for a domain name that keeps the domain name in limbo and cannot be registered by an unauthenticated buyer
- **ARP Poisoning**
    - **ARP Poisoning**
        - Attack that exploits the IP address to MAC resolution in a network to steal, modify, or redirect frames within the local area network
        - Allows an attacker to essentially take over any sessions within the LAN
        - ARP Poisoning is prevented by VLAN segmentation and DHCP snooping

Securing Networks

- **Securing Networks**
    - **Wired and wireless networks are vulnerable to attacks**
- **Securing Network Devices**
    - **Network devices include switches, routers, firewalls, and more**
    - **Default Accounts**
        - A user or administrator-level account that is installed on a device by the manufacturer during production
    - **Weak Passwords**
        - A password should be long, strong, and complex. This should require at least 14 characters with a mix of uppercase, lowercase, numbers, and special characters
            - password
            - PaSSworD
            - Pa55w0rd
            - P@$5w0rd
    - **Privilege Escalation**
        - Occurs when a user is able to gain the rights of another user or administrator
        - Vertical Privilege Escalation
        - Horizontal Privilege Escalation
    - **Backdoor**
        - A way of bypassing normal authentication in a system
    - **An IPS, proper firewall configs, network segmentation, and firmware updates are the keys to having network security**
- **Securing Network Media**
    - **Network Media**
        - Copper, fiber optic, and coaxial cabling used as the connectivity method in a wired network
    - **Electromagnetic Interference (EMI)**
        - A disturbance that can affect electrical circuits, devices, and cables due to radiation or electromagnetic conduction

        - EMI can be caused by TVs, microwaves, cordless phones, motors, and other devices
        - Shielding the cables (STP) or the source can minimize EMI
    - **Radio Frequency Interference (RFI)**
        - A disturbance that can affect electrical circuits, devices, and cables due to AM/FM transmissions or cell towers
        - RFI causes more problems for wireless networks
    - **Crosstalk**
        - Occurs when a signal transmitted on one copper wire creates an undesired effect on another wire
        - UTP is commonly used more than STP
    - **Data Emanation**
        - The electromagnetic field generated by a network cable or device when transmitting
        - A Faraday cage can be installed to prevent a room from emanating
        - Split the wires of a twisted-pair connection
    - **Protected Distribution Systems (PDS)**
        - Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats
- **Securing Wi-Fi Devices**
    - **Service Set Identifier (SSID)**
        - Uniquely identifies the network and is the name of the WAP used by the clients
        - Disable the SSID broadcast in the exam
    - **Rogue Access Point**
        - An unauthorised WAP or Wireless Router that allows access to the secure network
    - **Evil Twin**
        - A rogue, counterfeit, and unauthorised WAP with the same SSID as your valid one
- **Wireless Encryption**
    - **Encryption of data in transit is paramount to security**
    - **Pre-Shared Key**
        - Same encryption key is used by the access point and the client
    - **Wired Equivalent Privacy**
        - Original 802.11 wireless security standard that claims to be as secure as a wired network
        - WEP's weakness is its 24-bit IV (Initialisation Vector)
    - **Wi-Fi Protected Access (WPA)**
        - Replacement for WEP which uses TKIP, Message Integrity Check (MIC), and RC4 encryption
        - WPA is flawed, so it was replaced by WPA2
    - **Wi-Fi Protected Access version 2 (WPA2)**
        - 802.11i standard to provide better wireless security featuring AES with a 128-bit key, CCMP, and integrity checking
        - WPA2 is considered the best wireless encryption abailable

Question	Answer

Question	Answer
Open	No security or protection provided
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

    - **If we make operations easier, then security is reduced**
    - **Wi-Fi Protected Setup (WPS)**
        - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable
        - Always disable WPS
    - **Encryption and VPNs are always a good idea**
- **Wireless Access Points**
    - **Wireless security also relies upon proper WAP placement**
    - **Wireless B, G, and N use a 2.4GHz signal**
    - **Wireless A, N, and AC use a 5.0GHz signal**
    - **2.4 GHz signals can travel further than 5 GHz**
    - **Jamming**
        - Intentional radio frequency interference targeting your wireless network to cause a denial of service condition
        - Wireless site survey software and spectrum analysers can help identify jamming and interference
    - **AP Isolation**
        - Creates network segment for each client when it connects to prevent them from communicating with other clients on the network
- **Wireless Attacks**
    - **War Driving**
        - Act of searching for wireless networks by driving around until you find them
        - Attackers can use wireless survey or open source attack tools
    - **War Chalking**
        - Act of physically drawing symbols in public places to denote the open, closed, and protected networks in range
        - War chalking digitally is becoming more commonplace
    - **IV Attack**
        - Occurs when an attacker observes the operation of a cipher being used with several different keys and finds a mathematical relationship between those keys to determine the clear text data
        - This happened with WEP and makes it easy to crack
    - **Wi-Fi Disassociation Attack**
        - Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects
        - Used as part of an attack WPA/WPA2
    - **Bruce Force Attack**

        - Occurs when an attacker continually guesses a password until the correct one is found
        - Brute force will always find the password...eventually!
- **WPA3**
    - Wi-Fi Protected Access 3 (WPA3) was introduced in 2018 to strengthen WPA2
    - WPA3 has an equivalent cryptographic strength of 192-bits in WPA3 - Enterprise Mode
    - WPA3 - Enterprise mode
        - Uses AES-256 encryption with a SHA-384 hash for integrity checking
    - WPA3 - Personal Mode
        - Uses CCMP-128 as the minimum encryption required for secure connectivity
        - Largest improvement in WPA3 is the removal of the Pre-Shared Key (PSK) exchange
    - Simultaneous Authentication of Equals (SAE)
        - A secure password-based authentication and password-authenticated key agreement method
        - Simultaneous Authentication of Equals (SAE) provides forward secrecy
    - Perfect Forward Secrecy or Forward Secrecy
        - A feature of key agreement protocols (like SAE) that provides assurance that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised
            - The AP and the client use a public key system to generate a pair of long-term keys
            - The AP and the client exchange a one-time use session key using a secure algorithm like Diffie-Hellman
            - The AP sends the client messages and encrypts them using the session key created in Step 2
            - Client decrypts the messages received using the same one-time use session key
            - The process repeats for every message being sent, starting at Step 2 to ensure forward secrecy
        - This concept is a review of how key exchange protocols work from your Network+ studies
- **Other Wireless Technologies**
    - **Bluejacking**
        - Sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets
    - **Bluesnarfing**
        - Unauthorised access of information from a wireless device through a Bluetooth connection
    - **Bluejacking sends information**
    - **Bluesnarfing takes information**
    - **Don't allow Bluetooth devices to use default PINs for pairing**
    - **Radio Frequency Identification (RFID)**
        - Devices that use a radio frequency signal to transmit identifying information about the device or token holder
        - RFID can operate from 10 cm to 200 meters depending on the device

    - **Near Field Communication (NFC)**
        - Allows two devices to transmit information when they are within close range through automated pairing and transmission
        - NFC devices are operated within 4 cm from each other

Physical Security

- **Physical Security**
    - **If an attacker can physically touch your devices, they can own your devices**
- **Surveillance**
    - **Closed Circuit TV (CCTV)**
    - **Pan Tilt Zoom (PTZ)**
- **Door Locks**
    - **Door locks can use keys, pins, wireless signals, or biometrics**
    - **Mantrap**
        - Area between two doorways that holds people until they are identified and authenticated
- **Biometric Readers**
    - **Biometrics**
        - Relies on the physical characteristics of a person to identify them
        - Biometrics is considered "something you are"
    - **False Acceptance Rate (FAR)**
        - Rate that a system authenticates a user as authorised or valid when they should not have been granted access to the system
    - **False Rejection Rate (FRR)**
        - Rate that a system denies a user as authorised or valid when they should have been granted access to the system
    - **Crossover Error Rate (CER)**
        - An equal error rate (ERR) where the false acceptance rate and false rejection rate are equal
        - CER measures the effectiveness of a biometric system

Facilities Security

- **Facility Security**
- **Fire Suppression**
    - **Fire Suppression**
        - Process of controlling and/or extinguishing fires to protect an organisation's employees, data equipment, and buildings
    - **Handheld**
        - Class A, B, C, D, K
    - **Sprinklers**
        - Wet Pipe Sprinkler System
            - Pipes are filled with water all the way to the sprinkler head and are just waiting for the bulb to be melted or broken

        - Dry Pipe Sprinkler System
            - Pipes are filled with pressurised air and only push water into the pipes when needed to combat the fire
        - A pre-action sprinkler system will activate when heat or smoke is detected
    - **Special Hazard Protection**
        - Clean Agent System
            - Fire suppression system that relies upon gas (HALON, FM-200, or CO2) instead of water to extinguish a fire
    - **If you hear a loud alarm in the server room… GET OUT!**
- **HVAC**
    - **HVAC**
        - Heating, Ventilation, and Air Conditioning
    - **Humidity should be kept around 40%**
    - **HVAC systems may be connected to ICS and SCADA network**
- **Shielding**
    - **Shielded Twisted Pair (STP) adds a layer of shielding inside the cable**
    - **Faraday Cage**
        - Shielding installed around an entire room that prevents electromagnetic energy and radio frequencies from entering or leaving the room
    - **TEMPEST**
        - U.S. Government standards for the level of shielding required in a building to ensure emissions and interference cannot enter or exit the facility
        - TEMPEST facilities are also resistant to EMPs (electromagnetic pulses)
- **Vehicular Vulnerabilities**
    - Vehicles connect numerous subsystems overs a controller area network (CAN)
        - Controller Area Network (CAN)
            - A digital serial data communications network used within vehicles
            - The primary external interface is the Onboard Diagnostics (OBD-II) module
            - No concept of source addressing or message authentication in a CAN bus
                - Attach the exploit OBD-II
                - Exploit over onboard cellular
                - Exploit over onboard Wi-Fi
- **IoT Vulnerabilities**
- Internet of Things (IoT)
    - A group of objects (electronic or not) that are connected to the wider Internet by using embedded electronic components
    - Most smart devices use an embedded version of Linux or Android as their OS
    - Devices must be secured and updated when new vulnerabilities are found
- **Embedded System Vulnerabilities**
    - **Embedded Systems**
        - A computer system that is designed to perform a specific, dedicated function
        - Embedded systems are considered static environments where frequent changes are not made or allowed

        - Embedded systems have very little support for identifying and correcting security issues
    - **Programmable Logic Controller (PLC)**
        - A type of computer designed for deployment in an industrial or outdoor setting that can automate and monitor mechanical systems
        - PLC firmware can be patched and reprogrammed to fix vulnerabilities
    - **System-on-Chip (SoC)**
        - A processor that integrates the platform functionality of multiple logical controllers onto a single chip
        - System-on-Chip are power efficient and used with embedded systems
    - **Real-Time Operating System (RTOS)**
        - A type OS that prioritises deterministic execution of operations to ensure consistent response for time-critical tasks
        - Embedded systems typically cannot tolerate reboots or crashes and must have response times that are predictable to within microsecond tolerances
    - **Field Programmable Gate Array (FPGA)**
        - A processor that can be programmed to perform a specific function by a customer rather than at the time of manufacture
        - End customer can configure the programming logic to run a specific application instead of using an ASIC (Application-Specific Integrated Circuit)
- **ICS and SCADA Vulnerabilities**
    - **Operational Technology (OT)**
        - A communications network designed to implement an industrial control system rather than data networking
        - Industrial systems prioritise availability and integrity over confidentiality
    - **Industrial Control Systems (ICS)**
        - A network that manages embedded devices
        - ICS used for electrical power stations, water suppliers, health services, telecommunications, manufacturing, and defence needs
    - **Fieldbus**
        - Digital serial data communications used in operational technology networks to link PLCs
    - **Human-Machine Interface (HMI)**
        - Input and output controls on a PLC to allows a user to configure and monitor the system
        - ICS manages the process automation by linking together PLCs using a fieldbus to make changes in the physical world (values, motors, etc)
    - **Data Historian**
        - Software that aggregates and catalogs data from multiple sources within an industrial control system
    - **Supervisory Control and Data Acquisition (SCADA)**
        - A type of industrial control system that manages large-scale, multiple-site devices and equipment spread over geographic region
        - SCADA typically run as software on ordinary computers to gather data from and manage plant devices and equipment with embedded PLCs
    - **Modbus**

        - A communications protocol used in operational technology networks
        - Modbus gives control servers and SCADA hosts the ability to query and change the configuration of each PLC
- **Mitigating Vulnerabilities**
    - Four key controls for mitigating vulnerabilities in specialised system
        - Establish administrative control over Operational technology networks by recruiting staff with relevant expertise
        - Implement the minimum network links by disabling unnecessary links, services
        - Develop and test a patch management program for Operational Technology Network
        - Perform regular audits of logical and physical access to systems to detect possible vulnerabilities and intrusion
    - Warning: Enumeration tools and vulnerability scanners can cause problems on Operational Technology Network
- **Premise System Vulnerabilities**
    - **Premise Systems**
        - Systems used for building automation and physical access security
        - Many system designs allow the monitoring to be accessible from the corporate data network or even directly from the Internet
    - **Building Automation System (BAS)**
        - Components and protocols that facilitate the centralised configuration and monitoring of mechanical and electrical systems within offices and data centres
            - Process and memory vulnerabilities in PLC
            - Plaintext credentials or keys in application code
            - Code injection via web user interface
        - Denial of Service conditions could be caused by affecting building automation systems like HVAC
- **Physical Access Control System (PACS)**
    - Components and protocols that facilitate the centralised configuration and monitoring of security mechanisms within offices and data centres
    - PACS can either be implemented as part of a building automation system or a separate system
    - WARNING: PACS are often installed and maintained by an external supplier and are therefore omitted from risk and vulnerability

Authentication

Authentication

- **Multi-factor Authentication**
    - Use of two or more authentication factors to prove a user's identity
        - Knowledge
        - Ownership
        - Characteristic
        - Location
        - Action
    - Username and password are only considered single-factor authentication

- **One-Time Passwords**
    - Time-based One Time Password (TOTP)
        - A password is computed from a shared secret and current time
    - HMAC-based One Time Password (HTOP)
        - A password is computed from a shared secret and is synchronised between the client and the server
- **Authentication Models**
    - **Context-aware Authentication**
        - Process to check the user's or system's attributed or characteristics prior to allowing it to connect
        - Restrict authentication based on the time of day or location
    - **Single Sign-On (SSO)**
        - A default user profile for each user is created and linked with all of the resources needed
        - Compromised SSO credentials
    - **Federated Identity Management (FIdM)**
        - A single identity is created for a user and shared with all of the organisations in a federation
        - Cross-Certification
            - Utilises a web of trust between organisations where each one certifies others in the federation
        - Trusted Third-Party
            - Organisations are able to place their trust in a single third-party (also called the bridge model)
            - Trusted third-party model is more efficient than a cross certification or web of trust model
        - Security Assertion Markup Language (SAML)
            - Attestation model built upon XML used to share federated identity management information between systems
        - OpenID
            - An open standard and decentralised protocol that is used to authenticate users in a federated identity management system
            - User logs into an Identity Provider (IP) and uses their account at Relying Parties (RP)
            - OpenID is easier to implement than SAML
            - SAML is more efficient than OpenID
- **802.1x**
    - **802.1x**
        - Standardised framework used for port-based authentication on wired and wireless networks
        - RADIUS
        - TACACS+
        - 802.1x can prevent rogue devices
    - **Extensible Authentication Protocol (EAP)**

        - A framework of protocols that allows for numerous methods of authentication including passwords, digital certificates, and public key infrastructure
        - EAP-MD5 uses simple passwords for its challenge-authentication
        - EAP-TLS uses digital certificates for mutual authentication
        - EAP-TTLS uses a server-side digital certificate and a client-side password for mutual authentication
    - **EAP-FAST**
        - Provides flexible authentication via secure tunneling (FAST) by using a protected access credential instead of a certificate for mutual authentication
    - **Protected EAP (PEAP)**
        - Supports mutual authentication by using server certificates and Microsoft's Active Directory to authenticate a client's password
    - **LEAP is proprietary to Cisco-based networks**
- **LDAP and Kerberos**
    - **Lightweight Directory Access Protocol (LDAP)**
        - A database used to centralise information about clients and objects on the network
        - Unencrypted
            - Port 389
        - Encrypted
            - Port 636
        - Active Directory is Microsoft's version
    - **Kerberos**
        - An authentication protocol used by Windows to provide for two-way (mutual) authentication using a system of tickets
        - Kerberos
            - Port 88
        - A domain controller can be a single point of failure for Kerberos
- **Remote Desktop Services**
    - **Remote Desktop Protocol (RDP)**
        - Microsoft's proprietary protocol that allows administrators and users to remotely connect to another computer via a GUI
        - RDP doesn't provide authentication natively
    - **Virtual Network Computing (VNC)**
        - Cross-platform version of the Remote Desktop Protocol for remote user GUI access
        - VNC requires a client, server, and protocol be configured
    - **RDP**
        - Port 3389
    - **VNC**
        - Port 5900
- **Remote Access Services**
    - **Password Authentication Protocol (PAP)**

        - Used to provide authentication but is not considered secure since it transmits the login credentials unencrypted (in the clear)
    - **Challenge Handshake Authentication Protocol (CHAP)**
        - Used to provide authentication by using the user's password to encrypt a challenge string of random numbers
        - Microsoft's version of CHAP is MS-CHAP
    - **PAP and CHAP used mostly with dial-up**
- **VPN**
    - **Virtual Private Network (VPN)**
        - Allows end users to create a tunnel over an untrusted network and connect remotely and securely back into the enterprise network
        - Client-to-Site VPN or Remote Access VPN
    - **VPN Concentrator**
        - Specialised hardware device that allows for hundreds of simultaneous VPN connections for remote workers
    - **Split Tunneling**
        - A remote worker's machine diverts internal traffic over the VPN but external traffic over their own internet connection
        - Prevent split tunneling through proper configuration and network segmentation
- **RADIUS and TACACS+**
    - **Remote Authentication Dial-In User Service (RADIUS)**
        - Provides centralised administration of dial-up, VPN, and wireless authentication services for 802.1x and the Extensible Authentication Protocol (EAP)
        - RADIUS operates at the application layer
            - AAA
            - Standard Ports
                - Authentication port 1812
                - Authorisation port 1813
            - Proprietary Variation
                - Authentication port 1645
                - Authorisation port 1646
    - **Cisco's TACACS+ is a proprietary version of RADIUS**
        - TACACS+
            - Port 49 (TCP)
- **Authentication Summary**
    - **802.1x**
        - IEEE standard that defines Port-based Network Access Control (PNAC) and is a data link layer authentication technology used to connected devices and to a wired or wireless LAN
    - **LDAP**
        - Application layer protocol for accessing and modifying directory services data (Active Directory uses it)
    - **Kerberos**

        - Authentication protocol used in Windows to identify clients to a server using mutual authentication (Uses tickets)
    - **Remote Access Services (RAS)**
        - Services that enables dial-up and VPN connections to occur from remote clients
    - **Challenge Handshake Protocol (CHAP)**
        - Authentication scheme that is used in dial-up connections
    - **RADIUS**
        - Centralisation administration system for dial-up, VPN, and wireless authentication that uses either ports 1812/1813 (UDP) or 1645/1646 (UDP)
    - **TACACS+**
        - Cisco's proprietary version of RADIUS that provides separate authentication and authorisation functions over port 49 (TCP)
- **Authentication Attacks**
    - Spoofing
        - A software-based attack where the goal is to assume the identity of a user, process, address, or other unique identifier
    - Man-in-the-Middle Attack
        - An attack where the attacker sits between two communicating hosts and transparently captures, monitors, and relays all communication between the hosts
        - Man-in-the-browser (MitB) is an attack that intercepts API calls between the browser process and its DLLs
        - Online password attacks involve entering guessing directly to a service
        - Restricting the number or rate of login attempts can prevent online password attacks
    - Password Spraying
        - Brute force attack in which multiple user accounts are tested with a dictionary of common passwords
    - Credential Stuffing
        - Brute force attack in which stolen user account names and passwords are tested against multiple websites
        - Credential stuffing can be prevented by not reusing passwords across different websites
    - Broken Authentication
        - A software vulnerability where the authentication mechanism allows an attacker to gain entry
            - Weak password credentials
            - Weak password reset methods
            - Credential exposure
            - Session hijacking

Access Control

Access Control

- Methods used to secure data and information by verifying a user has permissions to read, write, delete, or otherwise modify it

Access Control Models

- Discretionary Access Control (DAC)
    - The access control policy is determined by the owner
    - DAC is used commonly
    - 1. Every object in a system must have an owner
    - 2. Each owner determines access rights and permissions for each object
- Mandatory Access Control (MAC)
    - An access control policy where the computer system determines the access control for an object
    - The owner chooses the permissions in DAC but in MAC, the computer does
    - MAC relies on security labels being assigned to every user (called a subject) and every file/folder/device or network connection (called an object)
    - Data labels create trust levels for all subjects and objects
    - To access something, you need to meet the minimum level and have a "need-to-know"
    - MAC is implemented through the Rule-based and the Lattice-based access control methods
- 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
- Lattice-based Access Control
    - Utilises complex mathematics to create sets of objects and subjects to define how they interact
    - Mandatory Access Control is a feature in FreeBSD & SELinux
    - Only in high security systems due to its complex configuration
- Role-Based Access Control (RBAC)
    - An access model that is controlled by the system (like MAC) but utilises a set of permissions instead of a single data label to define the permission level
    - Power Users is a role-based permission
- Attribute-Based Access Control (ABAC)
    - An access model that is dynamic and context-aware using IF-THEN statements
    - If Jason is in HR, then give him access to \\fileserver\HR

Best Practices

- **Best Practices**
    - The access control policy is determined by the owner
    - Best Practices for Access Control
- **Implicit Deny**
    - All access to a resource should be denied by default and only be allowed when explicitly stated
- **Least Privilege**
    - Users are only given the lowest level of access needed to perform their job functions
    - Does everyone in the company need to know employee salary data?
- **Separation of Duties**
    - Requires more than one person to conduct a sensitive task or operation
    - Separation of duties can be implemented by a single user with a user and admin account
- **Job Rotation**

- Occurs when users are cycled through various jobs to learn the overall operations better, reduce their boredom, enhance their skill level, and most importantly, increase our security
- Job rotation helps the employee become more well-rounded and learn new skills
- Job rotation also helps the organisation identify theft, fraud, and abuse of position

Users and Groups

- **Computers can have multiple users and groups**
    1. Right-click on an empty area in the Users folder of ADUC and select Create New User
    2. Create a new user within the Organisational Unit (OU) within Active Directory
- **User Rights**
    - Permissions assigned to a given user
- **Groups**
    - Collection of users based on common attributes (generally work roles)
- **Permissions in Windows**
    - Permissions are broken down into Read, Write, and Execute inside Linux
        - Full Control
        - Modify
        - Read & Execute
        - List Folder Contents
        - Read
        - Write
    - Permissions are assigned to Owners (U), Groups (G), and All Users (O or A)
- **chmod**
    - Program in Linux that is used to change the permissions or rights of a file or folder using a shorthand number system
- **R (Read) = 4**
- **W (Write) = 2**
- **X (Execute) = 1**
- **# chmod 760 filename**
- **7 = Owner can RWX**
- **6 = Group can RW**
- **0 = All Users (no access)**
- **777 allows everyone to Read, Write, and Execute**

  Privilege Creep
    - Occurs when a user gets additional permission over time as they rotate through different positions or roles
    - Privilege creep violates the principles of least privilege

  User Access Recertification
    - Process where each user's rights and permissions are revalidated to ensure they are correct
        - Hired
        - Fired

        - Promoted

Permissions

- **Permissions are inherited by default from the parent when a new folder is created**
- **Any permissions added/removed from the parent folder will pass to the child by default too!**

  Propagation

    - Occurs when permissions are passed to a subfolder from the parent through inheritance
- **Use Groups for roles and do not assign users directly to a folder's permissions**
- **Review Note: CompTIA A+**
- **If you copy a folder, then permissions are inherited from the parent folder it is copied into**

Usernames and Passwords

- **first.last@yourcompany.com**
- **Strong Passwords**
    - Contain uppercase letters, lowercase letters, numbers, special characters, and at least 8 characters or more (preferably 14 or more)
    - 1. Always require the user to change the default password when the account is created
    - 2. Require that the password is changed frequently (every 90 days)
    - 3. Always change the default Administrator or Root password
    - 4. Disable the Guest account on your systems
    - 5. Enable CTRL+ALT+DEL for logging into the system
        - Turn this on in the Advanced tab of the User Accounts dialogue box
    - 6. Use good, strong policies in regards to your passwords

User Account Control (UAC)

- A security component in Windows that keeps every user in standard user mode instead of acting like an administrative user

  *Only exception is the Administrator account *

- 1. Eliminates unnecessary admin-level requests for Windows resources
- 2. Reduces risk of malware using admin-level privileges to cause system issues
- UAC can be disabled from the Control Panel

Risk Assessments

Risk Assessments

- A process used inside of risk management to identify how much risk exists in a given network or system

Risk

- The probability that a threat will be realised

Vulnerabilities

- Weaknesses in the design or implementation of a system

Threat

- Any condition that could harm, loss, damage, or compromise to our information technology systems
- Threats are external and beyond your control
- What can we do about the threats we identified?

Risk management is used to minimise the likelihood of a negative outcome from occurring

Risk Avoidance

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

Risk Transfer

- A strategy that passes the risk to a third party

Risk Mitigation

- A strategy that seeks to minimise the risk to an acceptable level

Risk Acceptance

- A strategy that seeks to accept the current level of risk and the costs associated with it if the risk were realised

Residual Risk

- The risk remaining after trying to avoid, transfer, or mitigate the risk
- **Identify assets**
- **Identify vulnerabilities**
- **Identify threats**
- **Identify the impact**

Qualitative Risk

- **Qualitative analysis uses intuition, experience, and other methods to assign a relative value to risk**
- **Experience is critical in qualitative analysis**

Quantitative Risk

- **Quantitative analysis uses numerical and monetary values to calculate risk**
- **Quantitative analysis can calculate a direct cost for each risk**

  Magnitude of Impact

  - An estimation of the amount of damage that a negative risk might achieve
  - Single Loss Expectancy (SLE)
  - Cost associated with the realisation of each individualised threat that occurs

    Asset Value x Exposure Factor

    SLE = AV x EF

    SLE = $10,000 x 20%

    SLE = $2,000
  - Annualised Rate of Occurrence (ARO)

    - Number of times per year that a threat is realised
    - Annualised Loss Expectancy (ALE)

      ALE = SLE x ARO

      ALE = $2000 x 3

      ALE = $6,000

        - Expected cost of a realised threat over a given year
- **If it costs $200,000 to build a server room that never loses power, then it would take 33 years to recover the building costs instead of losing power 3x year!**
- **Hybrid approaches that combine quantitative and qualitative analysis are commonly used**

Methodologies

- **Security Assessments**
    - Verify that the organisation's security posture is designed and configured properly to help thwart different types of attacks
    - Assessments might be required by contracts, regulations, or laws
    - Assessments may be active or passive
        - Active Assessments
            - Utilise more intrusive techniques like scanning, hands-on testing, and probing of the network to determine vulnerabilities
        - Passive Assessments
            - Utilise open source information, the passive collection and analysis of the network data, and other unobtrusive methods without making direct contact with the targeted systems
            - Passive techniques are limited in the amount of detail they find

Security Controls

- **Security Controls**
    - Methods implemented to mitigate a particular risk
- **Security controls are categorised as physical, technical, or administrative**
    - Physical Controls
        - Any security measures that are designed to deter or prevent unauthorised access to sensitive information or the systems that contain it
    - Technical Controls
        - Safeguards and countermeasures used to avoid, detect, counteract, or minimise security risks to our systems and information
    - Administrative Controls
        - Focused on changing the behaviour of people instead of removing the actual risk involved

    NIST categories are management, operational, and technical

    - Management Controls
        - Security controls that are focused on decision-making and the management of risk
    - Operational Controls

        - Focused on the things done by people
    - Technical Controls
        - Logical controls that are put into a system to help secure it

    Presentative, Detective, or Corrective controls

    Preventative Controls

    - Security controls that are installed before an event happens and are designed to prevent something from occurring

    Detective Controls

    - Used during the event to find out whether something abd might be happening

    Corrective Controls

    - Used after an event occurs

    A single control can be categorised into multiple types or categories

    Compensating Control

    - Used whenever you can't meet the requirement for a normal control
    - Residual risk not covered by a compensating control is an accepted risk

Types of Risks

External Risks

- Risks that are produced by a non-human source and are beyond human control

Internal Risk

- Risks that are formed within the organisation, arise during normal operations, and are often forecastable

Legacy Systems

- An old method, technology, computer system, or application program which includes an outdated computer system still in use

Multiparty

- A risk that refers to the connection of multiple systems or organisations with each bringing their own inherent risks

IP Theft

- Risk associated with business assets and property being stolen from an organisation in which economic damage, the loss of a competitive edge, or a slowdown in business growth occurs

Software Compliance/Licensing

- Risk associated with a company not being aware of what software or components are installed within its network

Vulnerability Management

Vulnerability Management

Vulnerability Assessment

- Seeks to identify any issues in a network, application, database, or other systems prior to it being used that might compromise the system
- Defines, identifies, and classifies vulnerabilities within a system

Vulnerability Management

- Practice of finding and mitigating the vulnerabilities in computers and networks

These 3 questions can help to scope your assessments

- 1. What is the value of the information?
- 2. What is the threat your system is facing?
- 3. What is the mitigation that could be deployed?

Nessus, Qualysguard, and AlienVault are used for vulnerability assessments

- 1. Define the desired state of security
- 2. Create a baseline
- 3. Prioritise the vulnerabilities
- 4. Mitigate vulnerabilities
- 5. Monitor the network and systems
- **Scan, Patch, Scan, ...**

Penetration Testing

- **Penetration tests look at a network's vulnerabilities from the outside**
- **Metasploit and CANVAS are commonly used**
- **Get permissions and document info**
- **Conduct reconnaissance**
- **Enumerate the targets**
- **Exploit the targets**
- **Document the results**

  Vulnerability Assessment

  - Seeks to identify any issues in a network, application, database, or other systems prior to it being used that might compromise the system

  Pivot

  - Occurs when an attacker moves onto another workstation or user account

  Persistence

  - Ability of an attacker to maintain a foothold inside the compromised network
- **A pentester can also simulate an insider threat**

Training and Exercises

Tabletop Exercise (TTX)

- Exercise that uses an incident scenario against a framework of controls or a red team
- A tabletop exercise is a discussion of simulated emergency situations and security incidents

Penetration Test

- A test that uses active tools and security utilities to evaluate security by simulating an attack on a system to verify that a threat exists, actively test it, bypass security controls, and then finally exploit vulnerabilities on a given system

    - Test the system to discover vulnerabilities or prove security controls work
    - Examine the system to identify any logical weaknesses
    - Interview personnel to gather information

A pentest must be properly scoped and resourced before it can begin

Red Team

- The hostile or attacking team in a penetration test or incident response exercise

Blue Team

- The defensive team in a penetration test or incident response exercise

White Team

- Staff administering, evaluating, and supervising a penetration test or incident response exercise

OVAL

Open Vulnerability and Assessment Language (OVAL)

- A standard designed to regulate the transfer of secure public information across networks and the Internet utilising any security tools and services available
- OVAL is comprised of a language and an interpreter

OVAL Language

- An XML schema used to define and describe the information being created by OVAL to be shared among the various programs and tools

OVAL Interpreter

- A reference developed to ensure the information passed around by these programs complies with the OVAL schemas and definitions used by the OVAL language

Vulnerability Assessments

Baselining of the network to assess the current security state of computers, servers, network devices, and the entire network in general

Network Mapping

- Discovery and documentation of physical and logical ocnnectivity that exists in the network
- Commercial and free network mapping software is available

Vulnerability Scanning

- A technique that identifies threats on the network without exploiting them

  Banner Grabbing

    - A technique used to gain information about servers and inventory the systems or services

      Nessus and Qualysguard are commercial vulnerability scanners

Network Sniffing

- The process of finding and investigating other computers on the networks by analysing the network traffic or capturing the packets being sent
- Network sniffer, packet sniffing, and protocol analyser can conduct packet capture

Protocol Analyser

- Software tool that allows for the capture, reassembly, and analysis of packets from the network

Password Analysis

- A tool used to test the strength of your passwords to ensure your password policies are being followed

  Password Cracker

  - Uses comparative analysis to break passwords and systematically continues guessing until the password is determined
  - Cain & Abel and John the Ripper

  Password Guessing

  - Occurs when a weak password is simply figured out by a person

  Dictionary Attack

  - Method where a program attempts to guess the password by using a list of possible passwords

  Brute-Force Attack

  - Method where a program attempts to try every possible combination until it cracks the password

  Increasing complexity exponentially increases the time required to brute-force a password

  Cryptanalysis Attack

  - Comparing a precomputed encrypted password to a value in a lookup table

  Rainbow Table

  - List of precomputed values used to more quickly break a password since values don't have to be calculated for each password being guessed

  Rubber Hose Attack

  - Attempt to crack a password by threatening or causing a person physical harm in order to make them tell you the password

Monitoring and Auditing

Monitoring Types

- **Signature-based**
  - Network traffic is analysed for prefetermined attack patterns
- **Anomaly-based**
  - A baseline is established and any network traffic that is outside of the baseline is evaluated
- **Behaviour-based**
  - Activity is evaluated based on the previous behaviour of applications, executables, and the operating system in comparison to the current activity of the system
- **Methods may be combined into a hybrid approach in some IDS/IPS systems**

Performance Baselining

- **Baselining**

    - Process of measuring changes in networking, hardware, software, and applications
- **Baseline Reporting**
    - Documenting and reporting on the changes in a baseline
- **Security Posture**
    - Risk level to which a system or other technology element is exposed
- **Perfmon.exe is the Windows program for Performance Monitor**

Protocol Analysers

- **Protocol analysers are used to capture and analyse network traffic**
- **Promiscuous Mode**
    - Network adapter is able to configure all of the packets on the network, regardless of the destination MAC address of the frames carrying them
- **Non-promiscuous Mode**
    - Network adapter can only capture the packets directly addressed to itself
- **To capture the most information, you need to be in promiscuous mode**
- **Port Mirroring**
    - One or more switch ports are configured to forward all of their packets to another port on the switch
- **If you cannot configure a SPAN port, then you can use a network tap**
    - Network Tap
        - A physical device that allows you to intercept the traffic between two points on the network

SNMP

- **Simple Network Manager Protocol (SNMP)**
    - A TCP/IP protocol that aids in monitoring network-attached devices and computers
    - SNMP is incorporated into a network management and monitoring system
- **Managed Devices**
    - Computers and other network-attached devices monitored through the use of agents by a network management system
- **Agents**
    - Software that is loaded on a managed device to redirect information to the network management system
- **Network Management System (NMS)**
    - Software running on one or more servers to control the monitoring of network-attached devices and computers
- **SNMP v1/v2 are insecure due to the use of community strings to access a device**
- **SNMP v3**
    - Version of SNMP that provides integrity, authentication, and encryption of the messages being sent over the network
- **Management should be conducted on an out-of-band network to increase security**

Auditing

- A technical assessment conducted on applications, systems, or networks
- Auditing is a detective control

    - Security logs
    - ACLs
    - User rights/permissions
    - Group policies (GPOs)
    - Vulnerability scans
    - Written organisational policies
    - Interviewing personnel
- Software tools are also used to help contact audits

Logging

- **Logs**
    - Data files that contain the accounting and audit trail for actions performed by a user on a computer or network
- **Security, System, and Application logs should be audited on a Windows system**
    - Security Logs
        - Logs the events such as successful and unsuccessful user logins to the system
    - System logs
        - Logs the events such as a system shutdown and driver failures
    - Application Logs
        - Logs the events for the operating system and third-party applications
- **To consolidate all the logs into a single repository, you can use SYSLOG**
    - SYSLOG
        - A standardised format used for computer message logging that allows for separation of the software that generates messages, the system that stores them, and the software that reports and analyses them
        - SYSLOG uses port 514 over UDP

Log Files

- **Log files are important to your ability to reconstruct an event after it occurs**
- **Log File Maintenance**
    - Actions taken to ensure the proper creation and storage of a file, such as the proper configuration, saving, back up, security, and encryption of the log files.
    - Log files should be saved to a different partition or an external server
- **Overwrite Events**
    - When a maximum log size is reached, the system can begin overwriting the oldest events in the log files to make room.
- **Logs should be archived and backed up to ensure they are available when required**
- **Write Once Read Many (WORM)**
    - Technology like a DVD-R that allows data to be written only once but read unlimited times

SIEM

- **Log review is a critical part of security assurance**
- **SIEM**

    - A solution that provides real-time or near-real-time analysis of security alerts generated by network hardware and applications
        - SIEM solutions can be implemented as software, hardware appliances, or outsourced managed services
        - Log all relevant events and filer irrelevant data
        - Establish and document scope of events
        - Develop use cases to define a threat
        - Plan incident response to an event
        - Establish a ticketing process to track events
        - Schedule regular threat hunting
        - Provide auditors and analysts an evidence trail
- There are many commercial and open-source SIEM solutions available
- **Splunk**
    - A market-leading big data information gathering and analsysis tool that can import machine-generated data via a connector or visibility add-on
    - Splunk may be installed locally or as a cloud-based solution
- **ELK/Elastic Stack**
    - Collection of free and open-source SIEM tools that provides storage, search, and analysis functions
        - Elasticsearch (query/analysis)
        - Logstash (log collection/normalisation)
        - Kibana (visualisation)
        - Beats (endpoint collection agents)
    - ELK Stack may be installed locally or as a cloud-based solution
- **ArcSight**
    - A SIEM log management and analytics software that can be used for compliance reporting for legislation and regulations like HIPPA, SOX, and PCI DSS
- **QRadar**
    - A SIEM log management, analytics, and compliance reporting platform created by IBM
    - Alien Vault and OSSIM (Open-Source Security Information Management)
    - A SIEM solution originally developed by Alien Vault, now owned by AT&T, and rebranded as AT&T Cybersecurity
    - OSSIM can integrate other open-source tools, such as the Snort IDS and OpenVAS vulnerability scanner, and provide an integrated web administrative tool to manage the whole security environment
- **Gralog**
    - An open-source SIEM with an enterprise version focused on compliance and supporting IT operations and DevOps

Syslog

- A protocol enabling different appliances and software applications to transmit logs or event records to a central server
- Syslog follows a client-server model and is the de facto standard for logging and events from distributed systems
- Syslog runs on most operating systems and network equipment using Port 514 (UDP) over TCP/IP

- A syslog message contains a PRI code, a header, and a message portion
- A PRI code is calculated from the facility and security level of the data
- A header contains the timestamp of the event and the hostname
- The message portion contains the source process of the event and related content
- **ORIGINAL DRAWBACKS TO SYSLOG:**
    - Since syslog relied on UDP, there can be delivery issues within congested networks
    - Basic security controls like encryption and authentication are not included by default within syslog

Due to these security issues, newer syslog implementations added new features and capabilities

- Newer implementations can use port 1468 (TCP) for consistent delivery
- Newer implementations can TLS to encrypt messages sent to servers
- Newer implementations can use MD-5 or SHA-1 for authentication and integrity
- Some newer implementations can use message filtering, automated log analysis, event response scripting, and alternate message formats

The newer version of the server is called syslog-ng or rsyslog

Syslog can refer to the protocol, the server, or the log entries themselves

SOAR

- **Security Orchestration, Automation, and Response (SOAR)**
    - A class of security tools that facilitates incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment
    - SOAR is primarily used for incident response
- **Next-gen SIEM**
    - A security information and event monitoring system with an integrated SOAR
        - Scans security/threat data
        - Analyse it with ML
        - Automate data enrichment
        - Provision new resources
- **Playbook**
    - A checklist of actions to perform to detect and respond to a specific type of incident
- **Runbook**
    - An automated version of a playbook that leaves clearly defined interaction points for human analysis

Cryptography

Cryptography

- The practice and study of writing and solving codes in order to hide the true meaning of information

Encryption

- Process of converting ordinary information (plaintext) into an unintelligible form (ciphertext)
- Encryption protects data at rest, data in transit, or data in use
    - Data at Rest

        - Inactive data that is archived, such as data resident on a hard disk drive
    - 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
- Encryption strength comes from the key, not the algorithm
    - Key
        - The essential piece of information that determines the output of a cipher

Symmetric vs Assymmetric

- **Symmetric Algorithm (Private Key)**
    - Encryption algorithm in which both the sender and the receiver must know the same secret using a privately-held key
    - Confidentiality can be assured with symmetric encryption
    - Key distribution can be challenging with symmetric encryption
    - Symmetric Algorithms
        - DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6
- **Asymmetric Algorithm (Public Key)**
    - Encryption algorithm where different keys are used to encrypt and decrypt the data
    - Asymmetric Algorithms
        - Diffie-Hellman, RSA, and ECC
- **Symmetric is 100-1000x faster than asymmetric**
- **Hybrid Implementation**
    - Utilises asymmetric encryption to securely transfer a private key that can be then used with symmetric encryption
- **Stream Cipher**
    - Utilises a keystream generator to encrypt data bit by bit using a mathematical XOR function to create the ciphertext
- **Block Cipher**
    - Breaks the input into fixed-length blocks of data and performs the encryption on each block
    - Block ciphers are easier to implement through a software solution

Symmetric Algorithms

- DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6
- **Data Encryption Standard (DES)**
    - Encryption algorithm which breaks the input into 64-bit blocks and uses transposition and substitution to create ciphertext using an effective key strength of only 56-bits
    - DES used to be the standard for encryption
- **Triple DES (3DES)**
    - Encryption algorithm which uses three separate symmetric keys to encrypt, decrypt, then encrypt the plaintext into ciphertext in order to increase the strength of DES
- **International Data Encryption Algorithm (IDEA)**
    - Symmetric block which uses 64-bit blocks to encrypt plaintext into ciphertext

- **Advanced Encryption Standard (AES)**
  - Symmetric block cipher that uses 128-bit, 192-bit, or 256-bit blocks and a matching encryption key size to encrypt plaintext into ciphertext
  - AES is the standard for encryption sensitive U.S. Government data
- **Blowfish**
  - Symmetric block cipher that uses 64-bit blocks and a variable length encryption key to encrypt plaintext into ciphertext
- **Twofish**
  - Symmetric block cipher that replaced blowfish and uses 128-bit blocks and a 128-bit, 192-bit, or 256-bit encryption key to encrypt plaintext into ciphertext
- **Rivest Cipher (RC4)**
  - Symmetric stream cipher using a variable key size from 40-bits to 2048-bits that is used in SSL and WEP
- **Rivest Cipher (RC5)**
  - Symmetric block cipher with a key size up to 2048-bits
- **Rivest Cipher (RC6)**
  - Symmetric block cipher that was introduced as a replacement for DES but AES was chosen instead
- **Exam Tips**
  - RC4 is the only stream cipher covered

Public Key Cryptography

- **Asymmetric algorithms are also known as Public Key Cryptography**
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation

    Jason's plaintext > Encrypted by Jason's Private Key > Decrypted by Jason's Public Key for Mary.
  - Organisations want both confidentiality and non-repudiation
- **Digital Signature**
  - A hash digest of a message encrypted with the sender's private key to let the recipient know the document was created and sent by the person claiming to have sent it
- **PKI**
  - Public Key Infrastructure
- **Exam Tips**
  - Asymmetric encryption is also known as public key cryptography
  - Two keys are used in public key cryptography

Asymmetric Algorithms

- Diffie-Hellman, RSA, and ECC
- **Diffie-Hellman (DH)**
  - Used to conduct key exchanges and secure key distribution over an unsecured network
  - Diffie-Hellman is used for the establishment of a VPN tunnel using IPSec

- **RSA (Rivest, Shamir, and Adleman)**
    - Asymmetric algorithm that relies on the mathematical difficulty of factoring large prime numbers
    - RSA is widely used for key exchange, encryption, and digital signatures
    - RSA can use key sizes of 1024-bits to 4096-bits

Elliptic Curve Cryptography (ECC)

- Algorithm that is based upon the algebraic structure of elliptic curves over finite fields to define the keys
- ECC with a 256-bit key is just as secure as RSA with a 2048-bit key
- ECDH
    - Elliptic Curve Diffie-Hellman
- ECDHE
    - Elliptic Curve Diffie-Hellman Ephemeral
- ECDSA
    - Elliptic Curve Digital Signature Algorithm
- ECC is most commonly used for mobile devices and low-power computing device

Pretty Good Privacy (PGP)

- An encryption program used for signing, encrypting, and decrypting emails
- The IDEA algorithm is used by PGP

Symmetric functions use 128-bit or higher keys and the asymmetric functions use 512-bit to 2048-bit key sizes

GNU Privacy Guard (GPG)

- A newer and updated version of the PGP encryption suite that uses AES for its symmetric encryption functions
- GPG has cross-platform availability

Key Management

- Refers to how an organisation will generate, exchange, store, and use encryption keys
- **The strength of an encryption system lies in the key strength**
- **Keys must be securely stored**
- **Periodically change your keys**

One-Time Pad

- A stream cipher that encrypts plaintext information with a secret random key that is the same length as the plaintext input
- **There are no such thing as truly random numbers in computers**
- **Pseudo-Random Number Generator (PRNG)**
    - A simulated random number stream generated by a computer that is used in cryptography, video games, and more
- **One-time pads are not commonly used**

Steganography

- The science and art of hiding messages within other messages

- Steganography is a form of obfuscation, not encryption

Cryptography Considerations

- **Blockchain**
  - A shared, immutable ledger for recording transactions, tracking assets and building trust
  - Most famous example of the blockchain is those used in cryptocurrencies
- **Public Ledger**
  - 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
  - A permissioned blockchain is used for business transactions and promotes new levels of trust and transparency using an immutable public ledger
- **Quantum Computing**
  - A computer that uses quantum mechanics to generate and manipulate quantum bits (qubits) in order to access enormous processing powers
- **Quantum Communication**
  - A communications network that relies on qubits made of photons (light) to send multiple combinations of 1s and 0s simultaneously which results in tamper resistant and extremely fast communications
- **What is a qubit?**
  - A quantum bit composed of electrons or photons that can represent numerous combinations of 1s and 0s at the same time through superposition
  - Cryptography is used to secure our communications and data by relying on how difficult a math problem is to compute...
  - Asymmetric encryption algorithms have been mathematically proven to be broken by quantum computers
- **Post-quantum Cryptography**
  - A new kind of cryptography algorithm that can be implemented using today's classical computers but is also impervious to attacks from future quantum computers
  - One method is to increase the key size to increase the number of permutations needed to be brute forced
  - Researchers are working on a wide range of approaches, including lattice-based cryptography and supersingular isogeny key exchange
- **Ephemeral**
  - A cryptographic key that is generated for each execution of a key establishment process
  - Ephemeral keys are short-lived and used in the key exchange for WPA3 to create a perfect forward secrecy
- **Homomorphic Encryption**
  - An encryption method that allows calculations to be performed on data without decrypting it first
  - Homomorphic encryption can be used for privacy-preserving outsourced storage and computation

Hashing

Hashing

- A one-way cryptographic function which takes an input and produces a unique message digest

Message Digest 5 (MD5)

- Algorithm that creates a fixed-length 128-bit hash value unique to the input file

Collision

- Condition that occurs when two different files create the same hash digest

Secure Hash Algorithm (SHA-1)

- Algorithm that creates a fixed-length 160-bit hash value unique to the input file

Secure Hash Algorithm (SHA-2)

- Family of algorithms that creates hash digests between 224-bits and 512-bits

Secure Hash Algorithm (SHA-3)

- Family of algorithms that creates hash digests between 224-bits and 512-bits

RACE Integrity Primitive Evaluation Message Digest (RIPEMD)

- An open-source hash algorithm that creates a unique 160-bit, 256-bit, or 320-bit message digest for each input file

Hash-based Message Authentication Code (HMAC)

- Uses a hash algorithm to create a level of assurance as to the integrity and authenticity of a given message or file
    - HMAC-MD5
    - HMAC-SHA1
    - HMAC-SHA256

Digital signatures prevent collisions from being used to spoof the integrity of a message

- Digital signatures use either DSA, RSA, ECDSA, or SHA
- **Code Signing**
    - Uses digital signatures to provide an assurance that the software code has not been modified after it was submitted by the developer
- **LANMAN (LM Hash)**
    - Original version of password hashing used by windows that uses DES and is limited to 14 characters
- **NT LAN Manager Hash (NTLM Hash)**
    - Replacement for LM Hash that uses RC4 and was released with Windows NT 3.1 in 1993
- **NTLMv2 Hash**
    - Replacement for NTLM Hash that uses HMAC-MD5 and is considered difficult to crack
    - NTLMv2 is used when you do not have a domain with Kerberos for authentication
- **Exam Tips**
    - Instantly match integrity and hashing on the exam
    - MD5 and SHA are the most common hash functions used

Hashing Attacks

- **Pass the Hash**

    - A 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
    - Pass the Hash is difficult to defend against
    - Mimikatz
        - A penetration testing tool used to automate the harvesting of hashes and conducting the Pass the Hash attack
    - Only use a trusted OS
    - Patch/update workstations
    - Use multifactor authentication
    - Use least privilege
- **Birthday Attack**
    - Technique used by an attacker to find two different messages that have the same identical hash digest
    - 99% chance of finding a matching birthday in a 57-person group
    - 50% chance of finding a matching birthday in a 23-person group
    - Collision
        - Occurs when two different inputs to a hash create an identical hash digest output

Increasing Hash Security

- **Key Stretching**
    - A technique that is used to mitigate a weaker key by increasing the time needed to crack it
    - WPA, WPA2, PGP, bcrypt, and other algorithms utilise key stretching
- **Salting**
    - Adding random data into a one-way cryptographic hash to help protect against password cracking techniques
    - A "nonce" is used to prevent password reuse

Public Key Infrastructure

Public Key Infrastructure (PKI)

- An entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption
- **PKI and public key encryption are related by they are not the same thing**
- **PKI is the entire system and just uses public key cryptography to function**

Digital Certificates

- **Certificates**
    - Digitally-signed electronic documents that bind a public key with a user's identity
- **X.509**
    - Standard used PKI for digital certificates and contains the owner/user's information and the certificate authority's information
- **Wildcard Certificates**

    - Allow all of the subdomains to use the same public key certificate and have it displayed as valid
    - Wildcard certificates are easier to manage
- **Subject Alternative Name (SAN)**
    - Allows a certificate owner to specify additional domains and IP addresses to be supported
- **Single-sided certificates only require the server to be validated**
    - Dual-sided certificates require both the server and the user to be validated
- **X.609 uses BER, CER, and DER for encoding**
- **Basic Encoding Rules (BER)**
    - The original ruleset governing the encoding of data structures for certificates where several different encoding types can be utilised
- **Canonical Encoding Rules (CER)**
    - A restricted version of the BER that only allows the use of only one
- **Distinguished Encoding Rules (DER)**
    - Restricted version of the BER which allows one encoding type and has more restrictive rules for length, character strings, and how elements of a digital certificate are stored in X.509
- **PEM**
- **CER**
- **CRT**
- **KEY**
- **P12**
- **PFX**
- **P7B**
- **Privacy-enhanced Electronic Mail**
    - .pem, .cer, .crt, or .key
- **Public Key Cryptographic System #12 (PKCS#12)**
    - .p12
- **Personal Information Exchange**
    - .pfx
- **Public Key Cryptographic Systems #7 (PKCS#7)**
    - .p7b
- **Remember, these file types are associated with PKI**

Certificate Authorities

- **Registration Authority**
    - Used to verify information about a user prior to requesting that a certificate authority issue the certificate
- **Certificate Authority**
    - The entity that issues certificates to a user
    - Verisign, Digisign, and many others act as Root CA
- **Certificate Revocation List (CRL)**
    - An online list of digital certificates that the certificate authority has revoked

- **Online Certificate Status Protocol (OCSP)**
    - A protocol that allows you to determine the revocation status of a digital certificate using its serial number
- **OCSP Stapling**
    - Allows the certificate holder to get the OCSP record from the server at regular intervals and include it as part of the SSL or TLS handshake
- **Public Key Pinning**
    - Allows an HTTPS website to resist impersonation attacks by presenting a set of trusted public keys to the user's web browser as part of the HTTP header
- **Key Escrow and Key Recovery Agent**
    - Key Escrow
        - Occurs when a secure copy of a user's private key is held in case the user accidently loses their key
    - Key Recovery Agent
        - A specialised type of software that allows the restoration of a lost or corrupted key to be performed
- **All of CA's certificates must be revoked if it is compromised**

Web of Trust

- A decentralised trust model that addresses issues associated with the public authentication of public keys within a CA-based PKI system
- A peer-to-peer model
- Certificates are created as self-signed certificates
- Pretty Good Privacy (PGP) is a web of trust

Security Protocols

Security Protocols

- **Emails**
- **Websites**
- **Remote control**
- **Remote access**

S/MIME

- **Secure/Multipurpose Internet Mail Extensions (S/MIME)**
    - A standard that provides cryptographic security for electronic messaging
- **Authentication**
- **Integrity**
- **Non-repudiation**
- **S/MIME can encrypt emails and their contents ...including malware**

SSL and TLS

- **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**
    - Cryptographic protocols that provide secure Internet communications for web browsing, instant messaging, email, VoIP, and many other services
    - We already covered how TLS works in the PKI lesson

- **Downgrade Attack**
    - A protocol is tricked into using a lower quality version of itself instead of a higher quality version
- **Break and Inspect**

SSH

- **Secure Shell (SSH)**
    - A protocol that can create a secure channel between two computers or network devices to enable one device to control the other device
    - SSH requires a server (daemon) to be run on one device and a client on the other
    - Port 22 (SSH)
    - SSH2 2.0 uses Diffie-Hellman key exchange and MACs

VPN Protocols

- **Virtual Private Networks**
    - A secure connection between two or more computers or device that are not on the same private network
- **Point-to-Point Tunneling Protocol (PPTP)**
    - A protocol that encapsulates PPP packets and ultimately sends data as encrypted traffic
    - PPTP can use CHAP-based authentication, making it vulnerable to attacks
- **Layer 2 Tunneling Protocol (L2TP)**
    - A connection between two or more computers or device that are not on the same private network
    - L2TP is usually paired with IPSec to provide security
- **IPSec**
    - A TCP/IP protocol that authenticates and encrypts IP packets and effectively securing communications between computers and devices using this protocol
    - IPSec 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**
- **Aggressive**
- **Quick**
- **Security Association (SA)**
    - Esablishment of secure connections and shared security information using certificates or cryptographic keys
- **Authentication Header (AH)**
    - Protocol used in IPSec that provides integrity and authentication
- **Encapsulating Security Payload (ESP)**
    - Provides integrity, confidentiality, and authenticity of packets by encapsulating and encrypting them
    - Transport Mode

        - Host-to-host transport mode only uses encryption of the payload of an IP packet but not its header
        - Transport mode is used for transmission between hosts on a private network
    - Tunnel Mode
        - A network tunnel is created which encrypts the entire IP packet (payload and header)
        - Tunnel mode is commonly used for transmission between networks

Planning for the Worst

Planning for the Worst

- **Redundancy usually refers to when you have something extra or unnecessary**
- **Redundancy helps ensure fault-tolerance to continue operations**
- **Single Point of Failure**
    - The individual elements, objects, or parts of a system that would cause the whole system to fail if they were to fail

Redundant Power

- **Redundant Power Supply**
    - An enclosure that provides two or more complete power supplies
    - A redundant power supply mitigates a single point of failure
- **Surge**
    - An unexpected increase in the amount of voltage provided
- **Spike**
    - A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike
- **Sag**
    - An unexpected decrease in the volume of voltage provided
- **Brownout**
    - Occurs when the voltage drops low enough that it typically causes the lights to dim and can cause a computer to shut off
- **Blackout**
    - Occurs when there is a total loss of power for a prolonged period

Backup Power

- **Uninterruptible Power Supply (UPS)**
    - Combines the functionality of a surge protector with that of a battery backup
- **Backup Generator**
    - An emergency power system used when there is an outage of the regular electric grid power
    - Portable gas-engine
    - Permanently installed
    - Batter-inverter
- **How do you decide which to use?**

Data Redundancy

- **Redundant Array of Independent Disks (RAID)**
- Allows the combination of multiple physical hard disks into a single logical hard disk rive that is recognised by the operating system
- **RAID 0**
  - Provides data striping across multiple disks to increase performance
- **RAID 1**
  - Provides redundancy by mirroring the data identically on two hard disks
- **RAID 5**
  - Provides redundancy by stripping data and parity data across the disk drives
- **RAID 6**
  - Provides redundancy by stripping and double parity data across the disk drives
- **RAID 10**
  - Creates a striped RAID of two mirrored RAIDs (combines RAID 1 & RAID 0)
- **Fault-resistant RAID**
  - Protects against the loss of the array's data if a single disk fails (RAID 1 or RAID 5)
- **Fault-tolerant RAID**
  - Protects against the loss of the array's data if a single component fails (RAID 1, RAID 5, RAID 6)
- **Disaster-tolerant RAID**
  - Provides two independent zones with full access to the data (RAID 10)
- **RAIDs provide redundancy and high-availability**

Network Redundancy

- **Focused on ensuring that the network remains up**
- **Redundant Internet connections**

Server Redundancy

- **Cluster**
  - Two or more servers working together to perform a particular job function
- **Failover Cluster**
  - A secondary server can take over the function when the primary one fails
- **Load-balancing Cluster**
  - Servers are clustered in order to share resources such as CPU, RAM, and hard disks

Redundant Sites

- **Host Site**
  - A near duplicate of the original site of the organisation that can be up and running within minutes
- **Warm Site**
  - A site that has computers, phones, and servers but they might require some configuration before users can start working
- **Cloud Site**

    - A site that has tables, chairs, bathrooms, and possibly some technical items like phones and network cabling
- **How do you choose the type of site?**

Data Backup

- **Maintaining a good backup is crucial to disaster recovery**
- **Full Backup**
    - All of the contents of a drive are backed up
- **Incremental Backup**
    - Only conducts a backup of the contents of a drive that have changed since the last full or incremental backup
- **Differential Backup**
    - Only conducts a backup of the contents of a drive that has changed since the last full backup
    - Differential backups take more time to create but less time to restore

Tape Rotation

- **10 Tape Rotation**
    - Each tape is used once per day for two weeks and then the enitre set is reused
- **Grandfather-Father-Son**
    - Three sets of backups tapes are defined as the son (daily), the father (weekly), and the grandfather (monthly)
- **Towers of Hanoi**
    - Three sets of backup tapes (like the grandfather-father-son) that are rotated in a more complex system
- **Snapshot Backup**
    - Type of backup primarily used to capture the entire operating system image including all applications and data
    - Snapshots are also commonly used with virtualised systems

Disaster Recovery Planning

- **Disaster Recovery Planning**
    - The development of an organised and in-depth plan for problems that could affect the access of data or the organisation's building
        - Fire
        - Flood
        - Long-term Power Loss
        - Theft or Attack
        - Loss of Building
- **Disaster Recovery Plan (DRP) should be written down**
    - Contact Information
    - Impact Determination
    - Recovery Plan
    - Business Continuity Plan (BCP)
    - Copies of Agreements
    - Disaster Recovery Exercises

    - List of Critical Systems and Data
- **Business Impact Analysis (BIA)**
    - A systematic activity that identifies organisational risks and determines their effect on ongoing, mission critical operations
    - Business impact analysis is governed by metrics that express system availability
- **Maximum Tolerable Downtime (MTD)**
    - The longest period of time a business can be inoperable without causing irrevocable business failure
    - Each business process can have its own MTD, such as a range of minutes to hours for critical functions, 24 hours for urgent functions, or up to 7 days for normal functions
    - MTD sets the upper limit on the recovery time that system and asset owners need to resume operations
    - If the power grid is out for more than 60 minutes, our primary Internet connection via our cable provider dies
    - What is MTD for our support devices
- **Recovery Time Objective (RTO)**
    - The length of time it takes an event to resume normal business operations and activities
- **Work Recovery Time (WRT)**
    - The length of time in addition to the RTO of individual systems to perform reintegration and testing of a restores or upgraded system following an event
- **Recovery Point Objective (RPO)**
    - The longest period of time that an organisation can tolerate lost data being unrecoverable
    - Recovery Point Objective (RPO) is focused on how long can you be without your data
    - MTD and RPO help to determine which business functions are critical and to specify appropriate risk countermeasures
    - Designing your disaster recovery and continuity of operations plans requires an understanding of your availability and reliability levels
- Disasters can be caused by internal or external forces
    - **Mean Time To Repair (MTTR)**
        - Measures the average time it takes to repair a network device when it breaks
    - **Mean Time Between Failures (MTBF)**
        - Measures the average time between failures of a device

Social Engineering

Social Engineering

- Manipulates a user into revealing confidential information that are detrimental to that user or the security of our systems

Insider Threats

- **Most dangerous threats to organisational security**
- **Insider Threat**
    - A person who works for or with your organisation but has ulterior motives
    - Employees who steal your information are insider threats
    - Data Loss Prevention systems can be used to help identify insider threats

Phishing

- **Social Engineering**
  - Anytime you are trying to deceive, lie, or trick the user into doing something
- **Phishing**
  - An attempt to fraudulently obtain information from a user (usually by email)
- **Spear Phishing**
  - An attempt to fraudulently obtain information from a user, usually by email that targets a specific individual
- **Whaling**
  - A form of spear phishing that directly targets the CEO, CFO, CIO, CSO, or other high-value target in an organisation
- **Smishing**
  - Phishing conducted over text messaging (SMS)
- **Vishing**
  - Phishing conducted over voice and phone calls
- **Pharming**
  - Phishing attack to trick a user to access a different or fake website (usually by modifying hosts file)
- Phishing is a more specific type of social engineering
- Phishing is a generic category with specific techniques

Motivation Factors

- **Authority**
  - People are more willing to comply with a request when they think it is coming from someone in authority
  - Use of recognisable brand names like a bank or PayPal could be considered a form of authority
- **Urgency**
  - People are usually in a rush these days and urgency takes advantage of this fact
- **Social Proof**
  - People are most likely to click on a link through social media or based on seeing others have already clicked on it
- **Scarcity**
  - Technique that relies on the fear of missing out on a good deal that is only offered in limited quantities or a limited time
- **Likeability**
  - A technique where the social engineer attempts to find common ground and shared interests with their target
- **Fear**
  - The use of threats or demands to intimidate someone into helping you in the attack

More Social Engineering

- **Diversion Theft**
  - When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location

- **Hoax**
  - Attempt at deceiving people into believing that something is false when it is true (or vice versa)
- **Shoulder Surfing**
  - When a person uses direct observation to obtain authentication information
- **Eavesdropping**
  - When a person uses direct observation to "listen" in to a conversation
- **Dumpster Diving**
  - When a person scavenges for private information in garbage containers
- **Baiting**
  - When a malicious individual leaves malware-infected removable media such as a USB drive or optical disc lying around in plain view
- **Piggybacking**
  - When an unauthorised person tags along with an authorised person to gain entry to a restricted area
- **Watering Hole Attack**
  - When an attacker figures out where users like to go, and places malware to gain access to your organisation

Frauds and Scams

- **Fraud**
  - The wrongful or criminal deception intended to result in financial or personal gain
- **Identity Fraud**
  - The use by one person of another person's personal information, without authorisation, to commit a crime or to deceive or defraud that other person or a third person
  - Identity theft involves stealing another person's identity and using it as your own
  - Identity fraud and identity theft are commonly used interchangeably these days
- **Scam**
  - A fraudulent or deceptive act or operation
- **Invoice Scam**
  - A scam in which a person is tricked into paying for a fake invoice for a service or product that they did not order
  - Identity fraud and invoice scams are low-tech social engineering techniques
- **Prepending**
  - A technical method used in social engineering to trick users into entering their username and passwords by adding an invisible string before the weblink they click
  - The prepended string (data:text) converts the link into a Data URI (or Data URL) that embeds small files inline of documents

Influence Campaigns

- **Influence Operations**
  - The collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent
  - Influence operations is the military term, but CompTIA uses the term influence campaign
- **Hybrid Warfare**

    - A 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

User Education

- **Never share authentication information**
- **Clean Desk Policy**
    - Policy where all employees must put away everything from their desk at the of the day into locked drawers and cabinets
- **Train users how to encrypt emails and data**
- **Follow organisational data handling and disposal policies**

Policies and Procedures

Policies and Procedures

- **Governance provides a comprehensive security management framework**
- **Policies**
    - Defines the role of security in an organisation and established the desired end state of the security program
    - Policies are very broad
- **Organisational Policies**
    - Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms
- **System-Specific Policies**
    - Address the security needs of a specific technology, application, network, or computer system
- **Issue-Specific Policies**
    - Built to address a specific security issue, such as email privacy, employee termination procedures, or other specific issues
- **Policies may be regulatory, advisory, or informative**
- **Standards are used to implement a policy in an organisation**
- **Baseline**
    - Created as reference points which are documented for use as a method of comparison during an analysis conducted in the future
- **Guidelines are used to recommend actions**
- **Procedures**
    - Detailed step-by-step instructions that are created to ensure personnel can perform a given action
- **Exam Tip**
    - Policies are generic
    - Procedures are specific

Data Classifications

- **Data Classification**

    - Category based on the value to the organisation and the sensitivity of the information if it were to be disclosed
- **Sensitive Data**
    - Any information that can result in a loss of security, or loss of advantage to a company, if accesses by unauthorised persons
- **Commercial businesses and the government use different classification systems**
- **Commercial Classifications**
    - Public Data
        - Has no impact to the company if released and is often posted in the open-source environment
        - Sensitive data might have a minimal impact if released
    - Private Data
        - Contains data that should only be used within the organisation
    - Confidential Data
        - Highest classification level that contains items such as trade secrets, intellectual property data, source code, and other types that would seriously affect the business if disclosed
- **Government Classifications**
    - Unclassified data can be released to the public
    - Sensitive but Unclassified
        - Items that wouldn't hurt national security if released but could impact those whose data is contained in it
    - Confidential Data
        - Data that could seriously affect the government if unauthorised disclosure were to happen
    - Secret Data
        - Data that could seriously damage national security if disclosed
    - Top Secret Data
        - Data that could gravely damage national security if it were known to those who are not authorised for this level of information
- **Data should not be stored forever**

Data Ownership

- The process of identifying the person responsible for the confidentiality, integrity, availability and privacy of information assets
- **Data Steward**
    - A role focussed on the quality of the data and associated metadata
- **Data Custodian**
    - A role responsible for handling the management of the system on which the data assets are stored
- **Privacy officer**
    - A role responsible for the oversight of any PII/SPI/PHI assets managed by the company

PII and PHI

- **It is your responsibility to protect the data collected**

- **Personal Identifiable Information (PII)**
    - A piece of data that can be used either by itself or in combination with some other pieces of data to identify a single person
        - Full Name
        - Driver's License
        - Date of Birth
        - Place of Birth
        - Biometric Data
        - Financial Account Numbers
        - Email Addresses
        - Social Media Usernames
    - Verify with your legal team what is considered PII
- **Privacy act of 1974**
    - Affects U.S. government computer systems that collects, stores, uses, or disseminates personally identifiable information
- **Health Insurance Portability and Accountability Act (HIPAA)**
    - Affects healthcare providers, facilities, insurance companies, and medical data clearing houses
- **Sarbanes-Oxley (SOX)**
    - Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements
- **Gramm-Leach-Bliley Act (GLBA)**
    - Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers
- **Federal Information Security Management (FISMA) Act of 2002**
    - Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data
- **Payment Card Industry Security Standard (PCI DSS) is a contractual obligation**
- **Help America Vote Act (HAVA) of 2002**
    - Provides regulations that govern the security, confidentiality, and integrity of the personal information collected, stored, or processed during the election and voting process
- **SB 1386 requires any business that stores personal data to disclose a breach**

Legal Requirements

- Any type of information or asset should consider how a compromise of that information can threaten the three core security attributes of the CIA Triad
- Security controls focus on the CIA attributes of the processing system

- **Privacy**
    - A data governance requirement that arises when collecting and processing personal data to ensure the rights of the subject's data
    - Legal requirements will affect your corporate governance and the policies in regards to privacy of your user's data
- **General Data Protection Regulation (GDPR)**
    - A personal data cannot be collected, processed or retained without the individual's informed consent

    - GDPR also provides the right for a user to withdraw consent, to inspect, amend, or erase data held about them
    - GDPR requires data breach notification within 72 hours
- **WARNING: Data breaches can happen accidently or through malicious interference**

Privacy Technologies

- **Deidentification**
    - methods and technologies that remove identifying information from data before it is distributed
    - Deidentification is often implemented as part of database design
- **Data Masking**
    - Deidentification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data
- **Tokenization**
    - A deidentification method where a unique token is substituted for real data
- **Aggregation/Banding**
    - A deidentification technique where data is generalised to protect the individuals involved
- **Reidentification**
    - An attack that combines a deidentification dataset with other data source to discover how secure the deidentification method used is

Security Policies

- **Privacy policies govern the labelling and handling of data**
- **Acceptable Use Policy**
    - Defines the rules that restrict how a computer, network, or other systems may be used
- **Change Management Policy**
    - Defines the structured way of changing the state of a computer system, network, or IT procedure
- **Separation of Duties is a preventative type of administrative control**
- **Job Rotation**
    - Different users are trained to perform the tasks of the same position to help prevent and identify fraud that could occur if only one employee had the job
- **Onboarding and Offboarding Policy**
    - Dictates what type of things need to be done when an employee is hired, fired, or quits
    - Terminated employees are often not cooperative
- **Due Diligence**
    - Ensuring that IT infrastructure risks are known and managed properly
- **Due Care**
    - Mitigation actions that an organisation takes to defend against the risks that have been uncovered during due diligence
- **Due Process**
    - A legal term that refers to how an organisation must respect and safeguard personnel's rights
    - Due process protects citizens from their government and companies from lawsuits

User Education

- **Security Awareness Training**
  - Used to reinforce to users the importance of their help in securing the organisation's valuable resources
  - User security awareness training has the best return investment
- **Security Training**
  - Used to teach the organisation's personnel the skills they need to
- **Security education is generalized training (like Security+)**
- **Specialized training may be developed too**

Vendor Relationships

- **Non-Disclosure Agreement (NDA)**
  - Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship
  - NDAs are a binding contract
- **Memorandum of Understanding (MOU)**
  - A non-binding agreement between two or more organisations to detail an intended common line of action
  - MOUs can be between multiple organisations
- **Service-Level Agreement (SLA)**
  - An 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
  - SLA may promise 99.999% uptime
- **Interconnection Security Agreement (ISA)**
  - An agreement for the owners and operators of the IT systems to document what technical requirements each organisation must meet
- **Business Partnership Agreement (BPA)**
  - Conducted between two business partners that established the conditions of their relationship
  - A BPA can also include security requirements

Disposal Policies

- **Asset disposal occurs whenever a system is no longer needed**
- **Degaussing**
  - Exposes the hard drive to a powerful magnetic field which in turn causes previously-written data to be wiped from a drive
- **Purging (Sanitising)**
  - Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques
- **Clearing**
  - Removal of data with a certain amount of assurance that it cannot be reconstructed
- **Data remnants are a big security concern**
- **Possible reuse of the device will influence the disposal method**
  - 1. Define which equipment will be disposed of
  - 2. Determine a storage location until disposal

    - 3. Analyse equipment to determine disposal - reuse, resell, or destruction
    - 4. Sanitise the device and remove all its data
    - 5. Throw away, recycle, or resell the device

IT Security Frameworks

- **Sherwood Applied Business Security Architecture (SABSA) is a risk-driven architecture**
- **Control Objectives for Information and Related Technology (COBIT)**
    - A security framework that divides IT into four domains: Plan and Organise, Acquire, and Implement, Deliver and Support, and Monitor and Evaluate
- **NIST SP 800-53 is a security control framework developed by the Dept. of Commerce**
- **ISO 27000**
- **ITIL is the de facto standard for IT service management**
    - Being able to discuss ITIL will help in your job interviews

Key Frameworks

- **Center for Internet Security (CIS)**
    - Consensus-developed secure configuration guidelines for hardening (benchmarks) and prescriptive, prioritized, and simplified sets of cybersecurity best practices (configuration guides)
- **Risk Management Framework (RMF)**
    - 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 regulations
- **Cybersecurity Framework (CSF)**
    - A set of industry standards and best practices created by NIST to help organisations manage cybersecurity risks
- **ISO 27001**
- **ISO 27002**
- **ISO 27701**
- **ISO 31000**
- **System and Organisation Controls (SOC)**
    - A suite of reports produced during an audit which is used by service organisations to issue validated reports of internal controls over those information 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 (usually 9-12 months)
- **Cloud Security Alliance's 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's Reference Architecture**
  - 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 fulfill 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

Incident Response Procedure

Our systems will never be 100% secure

- **Incident Reponse**
  - A set of procedure that an investigator follows when examining a computer security incident
- **Incident Management Program**
  - Program consisting of the monitoring and detecting of security events on a computer network and the execution of proper response to those security events
    - **Preparation**
    - **Identification**
    - **Containment**
    - **Eradication**
    - **Recovery**
    - **Lesson Learned**
- **Identification**
  - Process of recognising whether an event that occurs should be classified as an incident
- **Containment** is focused on isolating the incident
- **Recovery**
  - Focused on data restoration, system repair, and re-enabling any server or networks taken offline during the incident response

Incident Response Planning

- **What is an incident response team?**
  - Key people that are available to respond to any incident that meets the severity and priority thresholds set out by the incident response plan
    - **Incident Response Manager**
    - **Security Analyst**
    - **Triage Analyst**
    - **Forensic Analyst**
    - **Threat Researcher**
    - **Cross-functional Support**
  - Your CSIRT should be the single point of contact for security incident and may be a part of the SOC or and independent team
- **Out-of-band communication**
  - Signal that is sent between two parties or two devices that are sent via a path or method different that of the primary communication between the two parties or

devices

- What is your backup plan?
    - Maintained and up-to-date contact list
        - Email
        - Web portals
        - Telephone Calls
        - In-person Updates
        - Voicemail
        - Formal Report
    - Prevent unauthorised Release of information outside the CSIRT
- **Senior leadership**
    - Executives and managers who are responsible for business operations and functional areas
- **Regulatory bodies**
    - Government organisations that oversee the compliance with specific regulations and law
- **Legal**
    - The business or organisations legal council is repsonsible for mitigating risk from civil lawsuits
- The decision to involve law enforcement must be made by senior executives with guidance from legal
- **Human Resources (HR)**
    - Used to ensure no breaches of the employment law or employee contract is made during an incident response
- **Public Relation (PR)**
    - Used to manage negative publicity from a serious incident
- CSIRT will be asked for information regarding the estimated downtime, the scope of system and data affected, and other relevant details

Investigative Data

- **Security Information and Event Monitoring (SIEM)**
    - A combination of different data sources into one tool that provides real-time analysis of security alerts generated by applications and network hardware
        - Sensor
        - Sensitivity
        - Trends
        - Alerts
        - Correlation
- **Log Files**
    - A file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software
        - Network
        - System
        - Application
        - Security
        - Web

        - DNS
        - Authentication
        - Dump Files
        - VoIP
        - Call Managers
    - **syslog / rsyslog / syslog-ng**
        - Three variations of syslog which all permit the logging of data from different types of systems in a central repository
    - **journalctl**
        - A Linux command line utility used for querying and displaying logs from journald, the systemd logging service on Linux
    - **nxlog**
        - A 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
        - nxlog is a cross-platform, open-source tool that is similar to rsyslog or syslog-ng
    - **netflow**
        - A 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
    - **sflow**
        - Short for "sampled flow", it provides a means for exporting truncated packets, together with interface counters for the purpose of network monitoring
    - **Internet Protocol Flow Information Export (IPfix)**
        - A universal standard
        - of export for Internet Protocol 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
    - **Metadata**
        - Data that describes other data by providing an underlying definition or description by summarising basic information about data that makes finding and working with particular instances of data easier
            - Email
            - Mobile
            - Web
            - File

Forensic Procedures

- Written procedures ensure that personnel handle forensics properly, effectively, and in compliance with required regulations
- **Identification**
    - Ensure the scene is safe, secure the scene to prevent evidence contamination, and identify the scope of evidence to be collected
- **Collection**

    - Ensure authorisation to collect evidence is obtained, and then document and prove the integrity of evidence as it is collected
- **Analysis**
    - Create a copy of evidence for analysis and use repeatable methods and tools during analysis
- **Reporting**
    - Create a report of the methods and tools used in the investigation and present detailed findings and conclusions based on the analysis
- **Legal Hold**
    - A process designed to preserve all relevant information when litigation is reasonably expected to occur
    - A computer or server could be seized as evidence
    - Appoint a liaison with legal knowledge and expertise who can be the point of contact with law enforcement
        - Analysis must be performed without bias
        - Analysis methods must be repeatable by third parties
        - Evidence must not be changed or manipulated
- **WARNING:** Defence attorneys will try to use any deviation from these ethics as a reason to dismiss your findings and analysis
- **Timeline**
    - A tool that shows the sequence of file system events within a source imag ein a graphical format
        - How was access to the system obtained?
        - What tools have been installed?
        - What changes to files were made?
        - What data has been retrieved?
        - Was data exfiltrated?
    - Many forensics tools can generate a timeline based on your evidence
    - If your tool doesn't support it, you can create a sequence of events within a spreadsheet to server as a timeline

Data Collection Procedures

- **Data Acquisition**
    - The method and tools used to create a forensically sound copy of data from a source device, such as system memory or a hard disk
    - Bring-your-own-device (BYOD) policies complicate data acquisition since you may not be able to legally search or seize the device
    - Some data can only be collected once the system is shutdown or the power suddenly disconnected
    - Analysts should always follow the order of volatility when collecting evidence
        - **CPU registers and cache memory**
        - **Contents of system memory (RAM), routing tables, ARP cache, process table, temporary swap files**
        - **Data on persistent mass storage (HDD/SSD/flash drive)**

        - **Remote logging and monitoring data**
        - **Physical configuration and network topology**
        - **Archival media**
- **WARNING:** While most of the Windows registry is stored on the disk, some keys like (HKLM/Hardware) are only stored in memory so you should analyse the Registry via a memory dump

Security Tools

- **Networking**
- **File Manipulation**
- **Shell and Scripts**
- **Packet Capture**
- **Forensics**
- **Exploitation**

- **WARNING:** You do not need to know how to use all of these tools, but you should be aware of what they are used for as a security professional

Networking

- **tracert/traceroute**
    - A network diagnostic command for displaying possible routes and measuring transit delays of packets across an Internet Protocol network
- **nslookup/dig**
    - Utility used to determine the IP address associated with a domain name, obtain the mail server settings for a domain, and other DNS information
- **ipconfig/ifconfig**
    - Utility that displays all the network configurations of the currently connected network devices and can modify the DHCP and DNS settings
- **nmap**
    - An open-source network scanner that is used to discover hosts and services on a computer network by sending packets and analysing their responses
- **ping/pathping**
    - Utility used to determine if a host is reachable on an Internet Protocol network
- **hping**
    - An open-source packet generator and analyser for the TCP/IP protocol that is used for security auditing and testing of firewalls and networks
- **netstat**
    - Utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics
- **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

driven by other programs and scripts

- **arp**
  - Utility for viewing and modifying the local Address Resolution Protocol (ARP) cache on a given host or server
- **route**
  - Utility that is used to view and manipulate the IP routing table on a host or server
- **curl**
  - A command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE)
- **the harvester**
  - A python script that is used to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN database
- **sn1per**
  - An automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities across a network
- **scanless**
  - Utility that is used to create an exploitation website that can perform Open port scans in a more stealth-like manner
- **dnsenum**
  - Utility that is used for DNS enumeration to locate all DNS servers and DNS entries for a given organization
- **Nessus**
  - A proprietary vulnerability scanner that can remotely scan a computer or network for vulnerabilities
- **Cuckoo**
  - An open source software for automating analysis of suspicious files

File Manipultion

- **head**
  - A command-line utility for outputting the first ten lines of a file provided to it
- **tail**
  - A command-line utility for outputting the last ten lines of a file provided to it
- **cat (concatenate)**
  - A command-line utility for outputting the contents of a file to the screen
- **grep**
  - A command-line utility for searching plain-text data sets for lines that match a regular expression or pattern
- **chmod**
  - A command-line utility used to change the access permissions of file system objects
- **logger**
  - Utility that provides an easy way to add messages to the /var/log/syslog file from the command line or from other files

Shell and Scripts

- **SSH**
  - Utility that supports encrypted data transfer between two computers for secure logins, file transfers, or general purpose connections
- **PowerShell**
  - A task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language
- **Python**
  - An interpreted, high-level and general-purpose programming language
- **OpenSSL**
  - A software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end

Packet Capture

- **tcpdump**
  - A command line utility that allows you to capture and analyse network traffic going through your system
- **tcpreplay**
  - A suite of free open source utilities for editing and replaying previously captured network traffic
- **Wireshark**
  - A popular network analysis tool to capture network packets and display them at a granular level for real-time or offline analysis

Forensics

- **dd**
  - A command line utility used to copy disk images using a bit by bit copying process
- **FTK Imager**
  - A data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is needed
- **Memdump**
  - A command line utility used to dump system memory to the standard output stream by skipping over holes in memory maps
- **WinHex**
  - A commercial disk editor and universal hexadecimal editor used for data recovery and digital forensics
- **Autopsy**
  - A digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools

Exploitation

- **Metasploit (MSF)**
  - A computer security tool that offers information about software vulnerabilities, IDS signature development, and improves penetration

testing

- **Browser Exploitation Framework (BeEF)**
  - A tool that can hook one or more browsers and can use them as a beachhead of launching various direct commands and further attacks against the system from within the browser context
- **Cain & Abel**
  - A password recovery tool that can be used through sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, and analysing routing protocols
- **Jack the Ripper**
  - An open source password security auditing and password recovery tool available for many operating systems

- **Exam Tricks**
  1. **Use a Cheat Sheet**
  2. **Skip the Simulations**
  3. **Take a Guess**
  4. **Pick the best time**
  5. **Be confident**