netwrix

# CompTIA Security+ Exam Study Guide

# Table of Contents

# Introduction

This study guide covers the entire Security+ certification exam. It isn't designed to be somebody's only preparation material. Instead, it is designed to complement other study material, such as a book or hands-on lab practice. Additionally, you should have some real-world experience. Officially, the exam is aimed at people with at least two years of IT experience with a focus on security. That doesn't have to be on an Information Security team specifically. But, you should have experience dealing with security. For example, maybe you work with Active Directory, firewalls, or manage end user devices. In such cases, you will routinely work on the security-related aspects of IT.

The Security+ exam has the following characteristics:

- There are up to 90 questions.
- Some questions are multiple choice and others are performance-based.
- You have 90 minutes to complete the exam.
- A passing score is 750 (out of 900).

The exam covers the following 6 domains:

1. Threats, Attacks, and Vulnerabilities (21%)
2. Technologies and Tools (22%)
3. Architecture and Design (15%)
4. Identity and Access Management (16%)
5. Risk Management (14%)
6. Cryptography and PKI (12%)

This guide has a section for each domain, covering each of the topics listed in the exam objectives. There are two basic ways to use this guide:

- Read it first, before you do any other studying, to determine which areas you are strong in and which areas need more attention, so you can study more effectively.

- Study for the exam and then use this guide to assess your level of expertise. If you find yourself learning a lot from this guide, you're probably not ready to take the exam.

# 1. Threats, Attacks and Vulnerabilities

This domain has six sections.

## 1.1 Given a scenario, analyze indicator of compromise and determine the type of malware

For this topic, you should be prepared to figure out what type of malware is on a computer in a given scenario. The exam objective outlines the following 13 types of malware:

**Viruses**

A virus is a malicious program designed to replicate itself. Viruses are typically attached to legitimate files, such as documents or installation program. Not all viruses are designed to do damage to a computer; sometimes they are humorous or pranks, and other times, they are written by hackers trying to achieve infamy. There are a ton of different types of viruses — macro viruses, boot-sector viruses and so on — but you don't need to know about all the different types for this exam.

**Crypto-malware**

Crypto-malware is a type of ransomware that uses encryption to block access to data. It is difficult to overcome without paying the ransom or having a backup of the data.

**Ransomware**

Ransomware is malware designed to hold a computer or data hostage until a ransom is paid. This might be by blocking access to the data, changing the computer enough to make it hard to use or encrypting the data (this is known as crypto-malware, which is the next bullet item). Once a ransom is paid to the attackers, the data is usually released to the user.

**Worm**

A worm is a type of malware whose sole purposes is to spread. Often, worms don't cause any damage to a computer or data. However, because of the rapid spread of a worm, it can cause issues on a network (consuming most or all of the available bandwidth, for example). Occasionally, a worm will have a malicious payload that causes problems, such as deleting data on a computer.

**Trojan**

Like a Trojan horse, a Trojan is a malicious application that misleads users. Trojans are often hidden in installer — for example, when a user installs a photo editing program, the Trojan is installed silently in the background, unbeknownst to the user. In general, once installed, Trojans do not try to replicate or propagate; instead, they often connect to a command and control server to report in and get further instructions. Trojans are often used to install backdoors (defined later in this list) on a computer, giving the attacker remote access to the computer.

**Rootkit**

A rootkit is a type of malware designed to enable attackers to connect to and control a compromised computer remotely. Often, it gives them full control of the computer. Rootkits have been known to record audio, video (from webcams), capture keystrokes and steal data.

**Keylogger**

A keylogger, or keystroke logger, secretly captures all the keys pressed on the keyboard and either sends them to a remote server or records them to a file for later retrieval by an attacker. For example, it might capture all keystrokes by a user visiting their banking website — includes their credentials. Two-factor authentication can help protect against keyloggers, especially if it involves a entering a unique code for each logon.

**Adware**

Adware is a type of malware whose primary purpose is to display ads on your computer, earning money for their creators. Most adware attacks occur against browsers. Note that adware is different than legitimate applications that have inline advertising because such applications typically get permission from the user, often by making that part of the agreement to download the software, whereas adware displays ads without the user's permission.

**Spyware**

Spyware is malware whose primary purpose is to steal sensitive information from a computer. Methods include intercepting keystrokes, stealing data directly, and hijacking microphones or webcams. Some spyware is designed specifically to obtain banking information.

**Bots**

Computer bots come in two forms— good and bad. Good bots perform repetitive tasks, such as automating manual tasks. Bad bots take over your computer, report back to a command and control server, and wait for instructions. Often, bots are part of a botnet — a bunch of bots connected to a command and control infrastructure. Botnets are routinely used to perform denial-of-service (DoS) attacks, they but can also steal data, capture keystrokes and send unsolicited email.

**RAT**

A remote access Trojan (RAT) is a type of malware designed to create a backdoor and provide administrative control to a computer. RATs can be packaged with legitimate downloads (for example, trial programs) and gain access to a computer without a user knowing about it.

**Logic bomb**

When malware is designed to create havoc on a specific date and time or when a specific condition is met, it is known as a logic bomb. Logic bombs are often destructive, deleting data or taking applications offline. They are often associated with insider attacks. For example, a disgruntled developer might create a logic bomb, carefully configuring it to go off a while after he or she quits the company to reduce the risk of being held accountable for it.

**Backdoor**

A backdoor is a type of malware that provides a secret way to gain access to a computer. For example, suppose a web page requires you to authenticate. A backdoor might provide a way to bypass the authentication by manipulating the URL or by performing a series of clicks in the right place. Backdoors can be available to anybody who you can find them, but are sometimes established by hackers to circumvent the normal access method.

# 1.2 Compare and contrast types of attacks

This section details the various types of attacks that hackers use to try to gain unauthorized access to a network or a computer. At a minimum, you need to be familiar with each method at a high level so if you are presented with a scenario on the exam, you can determine the type of attack based on the information provided.

These attacks fall into the following categories:

- Social engineering attacks
- Application/service attacks
- Wireless attacks
- Cryptographic attacks

## Social engineering attacks

Social engineering is the art of deceiving people. Attacks happen via email, over the phone and in person. Social engineering is one of the most dangerous types of attacks because it has a high success rate. Here are the types of social engineering attacks covered by the Security+ exam:

## Phishing

Phishing is the act of trying to deceive somebody to give up personal information or sensitive information. There are three avenues for phishing attacks:

- **Email** (the most common method). Most people are familiar with the typical phishing email that pretends to be from your bank and asks you to confirm your information or reset your account. These types of phishing emails sometimes look legitimate and typically use malicious links. After clicking the malicious link, you might be directed to a fake bank website, malware might be secretly installed on your computer, or your browser might get hijacked. Email phishing typically targets many people at a time because it is easy and inexpensive.

- **Telephone** (the second most common method). Phishing by telephone is similar — a person calls from "IT support" and mentions something about your computer being infected. The person then requests for you to go to a special support website to fix your computer. However, that special support website often secretly installs malware on your computer.

- **In person** (the least common method). A phishing attack might also involve a person dressed as an electric utility employee who asks to repair your electrical infrastructure in order to gain unauthorized access to your facilities.

Defenses against phishing include employee training, internal phishing campaigns to test and educate users, and technical defenses such as anti-phishing scans before email is delivered to end users.

## Spear phishing

Spear phishing is phishing that targets an individual or a small group of people. Typically, spear phishing attacks are more sophisticated than mass phishing attacks; the attackers often know more about their targets and often stand to gain more if the target is compromised.

## Whaling

Whaling is a type of spear phishing that targets high-profile individuals, such as executives at public companies. Whaling attackers often take pains to learn a lot about their targets and successful attacks can yield much higher gains than other phishing attacks.

## Vishing

Vishing is phishing by telephone. While some people refer to this as phishing, vishing is the official term. With vishing, the goal is to gain sensitive or personal information from the person answering the phone. Often, the caller will impersonate another person, attempt to sound important and have a reason for requests to be expedited.

**Tailgating**

Tailgating is when someone follows an authorized person into a restricted area, such as a corporate office building, without providing their own credentials, such as swiping their keycard. At small companies, it is hard for an attacker to pull off a tailgating attack because everybody knows each other and no one will allow a stranger to tailgate in. However, at large companies with thousands of people, it is common not to know most of your coworkers. But tailgating still routinely occurs because in many countries people consider it common courtesy to hold the door for the person behind them, especially if they look like they belong because they are appropriately dressed, seem to be the right age and so on. Some attackers carry a large amount of stuff (such as a lunch bag, drink and backpack) and ask for help to get through the door. Tailgating attacks are dangerous because they give attackers physical access to your environment and computers. Attackers can leave infected USB sticks in key locations or attempt to take over computer. To reduce risk, some companies forbid tailgating and require each employee to swipe their badge to enter, even if they arrive at the same time as somebody else.

**Impersonation**

An impersonation attack is an attack where a malicious person attempts to impersonate a legitimate person or entity. Impersonation attacks can occur over email, over the web or in person. For example, suppose Company12345 has the domain company12345.biz — and an attacker registers a domain name that is very similar, company123456.biz; the small difference between these names might go unnoticed in email or when visiting a website. Or an attacker might dress up as a janitor, carrying a backpack vacuum and wearing gloves; they might be able to easily wander around your office building without drawing too much attention.

**Dumpster diving**

Dumpster diving has been around since before computers and the internet: Attackers simply sift through trash dumpsters looking for personal or sensitive information that they could use to carry out spear phishing or other attacks or enable them to steal somebody's identity. Attackers often look for electronic waste, too, such as disk drives, USB sticks and backup tapes. To minimize the chances of being impacted by a dumpster diving attack, you should shred all sensitive documents and physically destroy all electronic storage before you discard it.

**Shoulder surfing**

When a person secretly watches the computer screen or keyboard of another user, that person is shoulder surfing. It is an easy way to obtain passwords, logon methods and other sensitive information. It is a dangerous attack that often goes unnoticed. To protect against shoulder surfing, you can put a small mirror on your monitor or in your cubicle or office.

**Hoax**

A hoax is a false claim to entice somebody to take a desired action. For example, an attacker might claim that you have won something or that they want to buy something from you so you will provide personal information, such as your Social Security number or bank account information. To minimize the chances of a hoax being effective against you, be skeptical when you see or hear something that is too good to be true or that is unusual in some way (such as an coming at an unusual time or having an unusual sense of urgency).

**Watering hole attack**

A watering hole attack typically targets a specific company. The attacker learns of websites that the company frequents (their watering holes) and attempts to place malware on those sites in hopes that someone at the company will get infected. Lesser known watering hole attacks can occur in person — an attacker might place infected USB sticks at the IT helpdesk or support area in a box with a sign reading, "Free USB sticks."

Now that you have a good understanding of the types of social engineering attacks, let's review the main reasons these attacks are effective:

**Authority**

When the attacker conveys authority in a social engineering attack, the attack is more likely to succeed. For example, the attacker might impersonate a high-level executive or an IT support person. People often go out of their way to make such authority figures happy, which enables the attacker to gain access to sensitive information.

**Intimidation**

There are several ways that attackers use intimidation during a social engineering attack. They might attempt to scare the victim ("If you don't send me the files, then the auditing firm can't certify the company results") or threaten them ("if you don't want to validate your identity, then I'll record your refusal and report it to HR"). Intimidation often comes during an impersonation attack, where the attacker impersonates somebody in a high-level position of authority.

**Consensus**

Attacker establish consensus by claiming that others are performing the requested action. For example, to obtain sensitive auditing information from a company, an attacker might call a low -level manager and mention that his colleague was able to provide the requested information during the last audit in order to make the victim more likely to comply with the request.

**Scarcity**

When something is in short supply, it often becomes more desirable. Marketing companies often use scarcity to drive demand. Social engineering attackers also use it — for instance, during a hoax or phishing attack, an attacker might mention that a prize or giveaway has limited availability.

**Familiarity**

Familiarity can also help attacks succeed. For example, an attacker might dress like a maintenance worker and walk around a company's office building for a week. Only after being seen for a week does the attacker ask somebody to give him access to the telephone closet. Because the attacker looks familiar ("oh, he works here and fixes stuff"), employees are more likely to hold a door open for him or help him gain access to restricted areas. Similarly, an attacker might call a high-level executive on the phone and be kind and courteous to the executive assistant. After a couple of weeks of these calls, the assistant might come to think of the attacker as familiar and therefore friendly, and the attacker can then attempt to exploit the assistant.

**Trust**

Social engineering attacks sometimes involve trust. For example, an attacker might get a job at a target company. After a few months working there, the attacker is in a good position to carry out social engineering attacks against fellow employees. The attacker is trusted as "one of us," which makes employees discard their normal skepticism.

**Urgency**

A common tactic in social engineering attacks is to impart a sense of urgency. For instance, an attacker posing as a helpdesk admin might call a user and say, "Hi, Terry. This is Chris over in IT. Your computer has a virus. We must immediately install a fix on your computer. Can I email you the file now?" Such an attack can be very effective because victims often think that bad things will happen if they don't act fast.

## Application/service attacks

Application and service attacks target specific applications or services. For example, an attack might target web servers or try to reuse user credentials and authenticate as somebody else. As with the other topics, you must be able to differentiate between the various types of attacks and determine the type of attack in a scenario provided on the exam. The bullets below detail the types of application and service attacks:

**DoS**

A denial of service attack attempts to overwhelm a network, computer or another part of the IT infrastructure to degrade performance or take a service offline. Most of the well-known DoS attacks have targeted specific networks or services.

**DDoS**

A distributed denial of service attack is a large-scale DoS attack that leverages botnets made up of many computers or computing devices, often thousands of devices or more. The botnet sends network requests or other communications to the same service or network until the service or network becomes overwhelmed and unusable.

**Man-in-the-middle**

Communication over a network is typically between two parties, point A and point B. A man-in-the-middle attack spoofs one party to intercept traffic before relaying the information to the intended party. The attacker might be eavesdropping or trying to gather enough information to later circumvent authentication methods.

**Buffer overflow**

A buffer is where an application can write data to temporarily. A buffer overflow occurs when more data is written or stored than the space is allocated for. Attackers can cause overflows deliberately in order to produce errors or cause applications to crash.

**Injection**

Code injection is frequently associated with SQL injection, but can also use LDAP, SMTP and other methods. The attacker adds (injects) their malicious code into an application or service at runtime. This can cause a denial of service, data loss or complete takeover by the attacker.

**Cross-site scripting**

Cross-site scripting (XSS) is a web application vulnerability that allows attackers to inject scripts into the website or application. The script targets either a vulnerability in the web app, the server the app is running on or a plug-in associated with the app. An XSS attack exploits the trust a user has for a website or application.

**Cross-site request forgery**

A cross-site request forgery (XSRF) attack targets a website or application from a trusted user browser session. The user can (knowingly or unknowingly) transmit commands or scripts to attack an application. In contrast to an XSS attack, an XSRF attack exploits the trust a web application has in the user accessing the data.

**Privilege escalation**

The process of attacking a system to gain access to that system or other resources that are typically protected is privilege escalation. There are two types of privilege escalation: horizontal and vertical. Horizontal escalation is where a user accesses systems or resources that are meant for other systems or users. Vertical escalation is where a user accesses systems or resources using a higher-level account, such as administrative or root access.

**ARP poisoning**

The Address Resolution Protocol assists a system in identifying the hardware (MAC) address of a device. ARP poisoning is the process of spoofing or modifying that data so that information is transmitted to another device, typically one owned by the attacker, rather than to the intended recipient.

**Amplification**

An amplification attack is a type of DDoS attack that commonly targets network services such as NTP and DNS. The attacker will attempt to overwhelm the target service with a large amount of UDP traffic to render the service and infrastructure inaccessible.

**DNS poisoning**

A Domain Name System assists a system by translating friendly names to IP addresses. DNS poisoning is the process of spoofing or modifying DNS records so that when a friendly name is looked up, the wrong IP address is returned. This tactic can be used to redirect traffic in a denial of service attack, or to send the traffic to the attacker's website instead of the correct site.

**Domain hijacking**

All domain names are registered through an official IANA registrar, which controls the available top-level domains. If the registration of a domain name is stolen or compromised, that is domain hijacking. The attacker then has full control over the domain and therefore can change the name servers, contact information and more.

**Man-in-the-browser**

A man-in-the-browser attack is a type of man-in-the-middle attack in which a web browser is attacked by code on a website. The result is that the attacker takes control of the web browser and allows the browser to insert code, make application changes or modify website content without the user or website knowing.

**Zero day**

If an attacker identifies a new vulnerability and exploits it the same day, that is a zero day attack. A zero day attack is dangerous because even having the latest patches and security updates won't protect you against unknown vulnerabilities. The attack occurs before anyone is aware the exploit exists and the vendor can issue a fix.

**Replay**

A replay attack is a repeated (replayed) transmission of valid communication. The goal is to gain access to resources or data by resending a valid transmission. Using timestamps on communication can help minimize or block replay attacks. Additionally, using one-time keys or passwords for communication can also help.

**Pass the hash**

A pass the hash attack bypasses the need to know a user account's credentials by passing the hash of the previously authenticated user to the desired resource. These types of attacks are useful if passwords are not changed frequently and the resources do not require multi-factor authentication.

**Hijacking and related attacks**

- **Clickjacking.** Websites typically appear to be 2-dimensional, but attackers can conceal clickable content beneath a legitimate hyperlink or clickable image. When a user clicks what they think is a legitimate link, they also click the hidden link, which executes malicious code.
- **Session hijacking**. Most websites use cookies to identify individual sessions that have been authenticated on the website. These cookies can contain a session key. Attackers can gain access to the session by stealing the session key.
- **URL hijacking.** URL hijacking (also known as **typo squatting**) relies on users making typos and other mistakes when accessing a website; they are presented with a fake site that appears to be the real site.

**Driver manipulation**

- **Shimming.** Shims are used in programming to enable different API versions to operate in an environment. This can also create security vulnerabilities when older APIs can be used to manipulate hardware.
- **Refactoring.** In a refactoring attack, the attacker changes the underlying source code in order to gain full access to the hardware it is running on, enabling the attacker to use the hardware for other attacks.

**MAC spoofing**

All devices connected to a network have a physical address, or MAC address. MAC spoofing is the process of changing the physical address of a device. This tactic could be used to intercept traffic intended for the original device.

**IP spoofing**

If a device is connected to a layer 3 network, then it uses IP addresses to communicate with other devices. To intercept traffic, an attacker can use IP spoofing to act like another device on the network.

## Wireless attacks

Wireless attacks are specific to wireless networks. Mostly these attacks attempt to gain unauthorized access to a wireless network. These attacks are especially dangerous because they often originate from outside of your business (such as in the parking lot or from a neighboring business).

**Replay**

Like a denial of service attack, a replay attack repeatedly transmits data. However, the replay data is typically valid data to capture session information or other data to be used in an attack.

**IV**

An initialization vector (IV) attack is a method of decrypting wireless traffic. An attacker learns the plaintext of a single wireless packet, and then computes the remaining key stream of the RC4 hash. All wireless traffic that uses the same initialization vector can then be decrypted by the attacker.

**Evil twin**

An evil twin is a malicious access point that appears to be legitimate (for example, the network is named “Visitor Wi-Fi”) but that has been configured to eavesdrop and intercept wireless traffic. The access point (AP) can steal passwords, network keys and other information that is sent across the network.

**Rogue AP**

A rogue access point is an AP that has been added to the network without authorization. This is typically done by employees who want easier access or their own Wi-Fi network. These access points can bypass company security requirements as well as interfere with the available wireless channels in a physical area.

**Jamming**

Wireless networks operate on specific channels of wireless frequencies. The number of channels is determined by the specification of the wireless network. This limited number of channels makes it easy for an attacker to attack that signal range, like a denial-of-service attack to jam the network.

**WPS**

Wi-Fi Protected Setup (WPS) provide an easy way to add new devices to a wireless network — in many implementations, you don't need to enter the wireless password; you simply push a button on the AP and a button (or virtual button) on the device and automatically have the device join the network. However, this convenience comes with a security flaw — a brute-force attack on the PIN numbers used to add a device can enable other devices to authenticate to the network.

**Bluejacking**

Bluejacking is the process of using Bluetooth to send messages to Bluetooth-enabled devices in an immediate radius. Bluejacking relies on having discoverable Bluetooth-enabled devices nearby.

**Bluesnarfing**

Bluesnarfing is the process of using Bluetooth to connect to and steal data from another device. This attack relies on vulnerable Bluetooth implementations. To minimize the chances of being a victim, turn off Bluetooth in public places and keep your device up to date with the latest security updates.

**RFID**

Radio-frequency identification (RFID) is a type of wireless technology that allows for short-range communication, like Bluetooth. Several attacks can be performed specifically for RFID to spoof or disable communications.

**NFC**

Near-field communication (NFC) is a type of wireless technology that allows for nearby communication, like RFID and Bluetooth. A few attacks can be performed specifically for NFC to spoof or disable communications.

**Disassociation**

When a wireless client disconnects from a network, it performs a disassociation with the access point. An attacker can purposely disconnect other devices on the network by pretending to be those devices and disassociating them from the access point. The other devices are then not connected to the network and need to manually be joined again.

## Cryptographic attacks

Cryptographic attacks target technologies that rely on cryptographic functions. For example, cryptographic attacks often target passwords, which are often stored using encryption.

**Birthday**

A form of brute-force attack, a birthday attack uses probability theory. The attack attempts to generate and identify portions of a hash, trying to find a match.

**Known plain text/ cipher text**

When an attacker already has access to both the plaintext and the encrypted ciphertext, then this information can be used to also identify secret keys that are used to create the ciphertext and use them to decrypt other encrypted text.

**Rainbow tables**

Rainbow tables are pre-assembled tables for reversing encrypted hashes, typically password hashes. Rainbow tables are particularly effective when the plaintext target has a known or limited character length, such as a credit card number.

**Dictionary**

A dictionary attack is a brute-force attack in which the decryption key or password is found by trying every string in a custom dictionary.

**Brute force**

Brute-force attacks are repeated attempts to break the encryption of a password, file or system. **Online** brute force attacks attack a system that is on and could have other security protocols and checks enabled. **Offline** brute force attacks are performed while a system is offline, such as against a computed set of password hashes.

**Collision**

When two different inputs produce the same hash value, this is known as a collision. A collision attack attempts to find two different input values that result in the same hash.

**Downgrade**

A downgrade attack purposely uses an older, less secure protocol to communicate. Often, when clients communicate with servers, then they negotiate the communication method and security. In a downgrade attack, a client negotiates for the least security possible.

**Replay/playback**

A replay attack repeats or delays a previously valid network communication. Repeating the information can enable an attacker to receive information from a server. Delaying the communication can have the same effect as a denial of service attack.

**Weak implementations**

There are several cryptographic algorithms and protocols that can be used to encrypt data and traffic. Unfortunately, most of them have known vulnerabilities and flaws, and weak implementations of a protocol make its vulnerability more prominent. For example, PPTP is a VPN protocol that qualifies as a weak implementation of a VPN; it has known security issues, although it can still function for VPN connectivity.

# 1.3 Explain threat actor types and attributes

So far, we've looked at the types of malware and the types of attacks. Now, we are going to look at the type of people engaging in attacks. On the exam, you need to be able to identify the type of attacker based on the methods and level of sophistication in a given scenario.

## Types of actors

The following are the common actors in an attack:

**Script kiddies**

Script kiddies are new to attacks. They use existing scripts and tools to attack systems; they often lack the ability to create their own or even understand how the attack works.

**Hacktivist/ hacktivism**

A hacktivist uses an attack to promote a political message or social agenda. These attacks are more cosmetic than malicious.

**Organized crime**

Groups of hackers can come together with a common target or idea in mind as part of an organized effort. Some existing organized crime rings are turning to phishing and hacking as another way to produce income.

**Nation states/APT**

Countries and nations across the world are becoming increasingly more active in attacking other countries. Advanced persistent threats (APTs) are long-running attacks, often with a nation state directing or sponsoring the attack. These attacks can be sophisticated and dangerous, not only because the threat of physical warfare, but also because so many resources can be put behind the attacks.

**Insiders**

The most common and dangerous threat to networks and systems comes from insiders (employees, contractors, vendors). Insiders are granted access to resources or facilities, and then abuse that trust by using the access maliciously.

**Competitors**

Organizations can use phishing or other attacks to find information about a competitor and its products, such as planned features, release dates or other inside information that could help them compete against the target.

## Attributes of actors

To help figure out the type of actor in a given scenario, you can use information about how they operate:

**Internal/external**

The level of access that an attacker has can greatly increase their chances of being successful. External hackers typically have the benefit of being anonymous but must gain access through an attack, which can be difficult and comes with other risks. Internal attackers are trusted by an organization so they have the benefit of things like door badges to buildings, physical and wireless access to the network, and access to resources.

**Level of sophistication**

The level of sophistication of an attack can help determine who might be behind it. For example, targeting an old, known exploit with simple scripts or tools might indicate a script kiddy. However, exploiting relatively unknown vulnerabilities can indicate a more sophisticated attack, which might point to organized crime or a nation state.

**Resources/funding**

Although not all attacks are financially motivated, money can play a role in an attack. When you use more money and resources used for an attack, you can usually produce a more sophisticated attack.

**Intent/motivation**

The motivation behind attacks can vary. If an attack is by an internal actor, it could be an act of sabotage or revenge, or be related to a dislike of the organization. External actors are typically motivated by money, but they could also be part of a hacktivist organization, or attack because they believe the target is unethical or immoral.

## Types of intelligence

There are two primary types of intelligence:

**Open-source intelligence (OSINT)**

OSINT is gathered from publicly available sources, such as public records or from social media.

**Closed-source intelligence (CSINT)**

CSINT is gathered from covert sources.

# 1.4 Explain penetration testing concepts

Penetration testing (pen testing) involves testing the security controls of an organization. Such tests are often performed by outside companies without any inside knowledge of the network. Here are the pen testing concepts you should be familiar with:

**Active reconnaissance**

Active reconnaissance tests the controls of a security infrastructure, for example, by trying different variables and methods to purposely return errors and other information about the target.

**Passive reconnaissance**

Passive reconnaissance gathers information about the target without gaining access to the network or resources, such as information about the physical building or names and demographic information about the personnel who work there. Attackers often turn to social media and internet search engines to gain additional information.

**Pivot**

A pen tester might need to access different networks or hosts to continue the tests, for instance because of network segregation, firewalls or other logical disconnects between devices. The process of bypassing these disconnects is called a pivot.

**Initial exploitation**

Pen testing often uses multiple exploits to gain access to the target resources. The initial exploitation aims to gain access to the network. Then, additional exploits or techniques might be required to escalate privileges or move around the network.

**Persistence**

Some pen testing involves scanning and testing resources one time to ensure that they are up to date on the latest patches and have a solid security configuration. Persistent pen testing extends these tests over time, which can help identify gaps in an organization's procedures. For example, a web server might appear secure during the first pass of a pen test, but then doesn't get patched for two months; a subsequent test will reveal the missing patches.

**Escalation of privilege**

Privilege escalation is one of the most common methods of gaining access to resources. Attackers try to work their way up from a guest account with few rights to a user account to an account with complete administrative access.

**Black box**

Block box pen testing mimics what a real attacker faces: The black box tester has no knowledge of the target system and is not provided with any additional information about the organization, architecture or goals. Therefore, black box pen testing relies heavily on public-facing resources and information. If the tester is unable to breach the public-facing devices, then internal devices are not tested.

**White box**

White box testing is the opposite of black box testing: The tester is given full access to the entire environment to perform testing, potentially including the source code of applications. This provides the most comprehensive set of testing but can also be the most time-consuming and complicated.

**Gray box**

Gray box testing is like an attack by an internal actor. The tester has minimal knowledge of the architecture and the access level of a standard user account. Gray box testing allows for testing of both internal and external resources.

**Penetration testing vs. vulnerability scanning**

Vulnerability scanning is a more passive act than penetration testing. For instance, a scan might determine only whether a port is open on a firewall, while a penetration test will attempt to exploit an open port and connect to resources.

# 1.5 Explain vulnerability scanning concepts

Compared to pen testing, vulnerability scans are a passive approach to ensuring that devices and systems are up to date. These scans can identify open ports on devices and firewalls, assess whether network segregation and firewall rules are working as expected, and check whether systems have the latest patches installed. Here are the vulnerability scanning concepts you should know about:

**Passively test security controls**

As indicated by the name, passively testing security controls attempts only to identify any weaknesses or vulnerabilities in the target being scanned. Unlike a penetration test, which attempts to exploit a weakness, a passive test simply collects information about the target.

**Identify vulnerability**

Different types of targets have different vulnerabilities. Web servers might have vulnerabilities in code execution and data access. Firewall vulnerabilities can include misconfigurations in segregation or an access vulnerability to the firewall administration controls.

**Identify lack of security controls**

Part of vulnerability scanning is to identify any components that might be lacking security controls. One example is a guest Wi-Fi network that is open to anyone but is on a network that is not fully segregated from an organization's resources. Another example is a shared folder that everybody can read and write to.

**Identify common misconfigurations**

Vulnerability scanning can also help find common misconfigurations for firewalls and other devices on a network. Misconfigurations are often simple, such as leaving the default Administrator account open or not limiting Remote Desktop to only those who require access. In the cloud, configuring a storage location to be public when it is meant to be private is also a common misconfiguration.

**Intrusive vs. non-intrusive**

Typically, vulnerability scans are non-intrusive because they attempt only to identify a weakness, not to exploit it. However, depending on the target system, scanning can inadvertently become intrusive. For instance, if the target system is listening on a port for a connection, the vulnerability scan could see the open port and delay or deny a legitimate resource from connecting. Additionally, the additional traffic of vulnerability scans can add to the amount of data the network devices have to work with, causing issues for a network that is already congested.

**Credentialed vs. non-credentialed**

Like black box vs. gray box penetration testing, you can perform a credentialed or non-credentialed vulnerability scan. A non-credentialed scan is the easiest and quickest; it reports back only the open services on the network. A credentialed scan goes further by attempting to connect to a resource with a set or list of credentials supplied before the scan. This scan requires getting an accurate list of credentials but provides better insight into insider attacks.

**False positive**

Since vulnerability scans attempt to identify only whether there is a risk, the rate of false positives can be high. For instance, if the scan identifies open ports that are used for a critical application, the scan might report that the device is vulnerable. However, because the application requires those ports to be open and the organization has taken other steps to mitigate the risk of the ports being open, the report might be a false positive.

## 1.6 Explain the impact associated with types of vulnerabilities

Each vulnerability can have different risks or impacts associated with it. Not all organizations will treat each vulnerability the same, either — different security teams might categorize each risk separately and plan to either mitigate the risk or document why they chose not to.

**Race conditions**

A race condition occurs when a process produces an unexpected result due to timing. Race condition flaws are rare, and they are difficult to test for because they are often difficult to reproduce on demand. Race condition vulnerabilities can often go undetected for long periods of time, leaving organizations at risk.

**Vulnerabilities due to:**

- **End-of-life systems**. Systems past the vendor's end-of-life date typically no longer receive security or functionality updates. When a vulnerability or exploit in an operating system or hardware is identified, it might not be possible to mitigate it in older devices and therefore organizations might have to scramble to update systems or replace old hardware. The risk increases over time.
- **Embedded systems**. Devices that are embedded into other systems can be hard to update. For example, a manufacturing device that has a built-in operating system might not be on the same update schedule as other systems managed by the security team. Organizations might have to put other security measures in place to mitigate issues, such as auditing or disabling functionality.
- **Lack of vendor support**. If an application or device is no longer supported or rarely receives patches or updates from the vendor, even if it is not at its end of life, it will be become more riskier over time to use it as more vulnerabilities are discovered. Organizations might need to replace such systems to reduce risk.

| | |
|---|---|
| **Improper input handling** | Applications and websites that do not handle user input properly can make the website and the data behind it vulnerable. For example, if a website that uses a SQL database allows special characters without first parsing them, a SQL injection attack could be performed to obtain or delete data from the database. |
| **Improper error handling** | As with input handling, improper error handling can impact the availability of an application or website. Repeated errors can cause a memory leak, buffer overflow or other issue that could result in downtime. |
| **Misconfiguration/weak configuration** | The misconfiguration or weak configuration of a device can have drastic results. If an attacker can bypass a security control because of a bad configuration, then the attacker might be able to take over the entire network. |
| **Default configuration** | Using a default configuration typically has the same effect as having no security control in place at all. The default passwords and access information for just about any device or system can be found through a quick web search. |
| **Resource exhaustion** | Resource exhaustion attacks attempt to exploit a software bug or design flaw or inundate a system with a large number of requests in order to crash the system or render it unavailable for the time it takes to restart it. For example, an attacker might download a file from a web site, not just once, but thousands of times, potentially from thousands of different clients (whether legitimate or bogus clients). |
| **Untrained users** | The less aware users are about security controls, the more likely they are to use software improperly, fall for social engineering attacks and make other mistakes. |
| **Improperly configured accounts** | Like default configurations, accounts that have weak passwords or more privilege than needed are vulnerabilities to the systems they can access. |
| **Vulnerable business processes** | Poor user account management, security updates, change control and other business processes can also be a vulnerability. Even a simple checklist can help prevent a system from becoming out of date and vulnerable to the latest exploits. |
| **Weak cipher suites and implementations** | Implementing weak cipher suites typically has the same effect as using no security at all. Weak cipher implementations might be easy identified by an attacker and have known vulnerabilities and exploits. The data encrypted with these ciphers could then be decrypted by attackers. |

**Memory/buffer vulnerabilities**

- **Memory leak**. A memory leak typically results in an application beginning to run slowly and eventually crashing when the system runs out of available memory.
- **Integer overflow**. In applications that use integers, it is possible to overflow a variable by calculating a number that is higher or lower than the variable accepts. Like other application vulnerabilities, this can cause the system to hang or crash if the overflow wasn't planned for.
- **Buffer overflow**. Like an integer overflow, if a data buffer overflows with more data than it was sized for, then it can cause an application to hang or crash. Buffer overflows can be prevented by validation prior to any data being written to memory.
- **Pointer dereference**. Pointers within application code are just that — references that point to the variable that stores the data. A vulnerability that can de-reference the pointer can cause the variable to store the wrong type of data, be a null value or have some other impact that can cause an error in the application.
- **DLL injection**. DLLs are typically trusted by the system that they are running on. By injecting a DLL, attackers can run their code within the address space of a trusted process, which enables them to easily take over the system under the guise of the trusted process.

**System sprawl/ undocumented assets**

The more sprawl that exists in a system design, the easier it is to either forget about certain components or have systems that are not properly managed. Additionally, undocumented assets make planning for updates, pen tests and vulnerability assessments difficult.

**Architecture/design weaknesses**

A weak architecture or design behind a process or system can translate to additional vulnerabilities.

**New threats/zero day**

New threats and zero-day attacks are hard to plan for. Even system that are managed and patched regularly are vulnerable to these threats.

**Improper certificate and key management**

Many certificates and their keys protect encrypted data, whether it is stored on a disk or in transit. Failing to manage these critical certificates and keys properly can result in an attacker having full access to the data.

# 2. Technologies and Tools

There are 6 sections in this domain, each with its own material.

## 2.1 Install and configure network components, both hardware-and software-based, to support organizational security

This is a hands-on section, so you will have to install and configure assets. You won't need to deal with design decisions but you must be familiar with the details of implementing the given technology. Of course, these technologies are vendor agnostic, so you don't need to familiarize yourself with all the various vendor implementations.

### Firewall

A firewall is a hardware device or a software solution that inspects and then permits or denies network communications. Be familiar with the following firewall concepts:

- **ACL**. An access control list (ACL) is a single entry in a firewall that dictates whether specific communication is permitted (allowed) or denied (blocked).
- **Application-based vs. network-based**. An application-based firewall is specialized to protect specific application vulnerabilities. For example, an application-based firewall can protect database servers against SQL injection attacks. If configured in active mode, application-based firewalls can block malicious traffic; in passive mode, they only log malicious activity. A network-based firewall is a general firewall that sits at the network layer and inspects network traffic without application-specific knowledge. It permits or denies traffic based on pre-defined rules.
- **Stateful vs. stateless**. A stateful firewall watches communications and maintains knowledge of the connections. A stateful firewall excels at identifying malicious traffic but cannot handle as much traffic as a stateless firewall. A stateless firewall permits or denies communication based on source, destination, protocol or port. A stateless firewall excels at handling large volumes of traffic.
- **Implicit deny**. An implicit deny is a statement in a firewall that dictates that all traffic not permitted or denied in existing ACLs is denied (or treated as suspicious).

## VPN concentrator

A VPN concentrator is a device that facilitates VPN connections. It listens for connections from clients, authenticates the connections, and then provides access to the network.

- **Remote access vs. site-to-site**. A remote access VPN enables users to connect to the organization's network from a remote location. A site-to-site VPN enables two sites to connect to each other. For example, a site-to-site VPN could connect a branch office with a main office.
- **IPSec**. An IPSec VPN uses IPSec for connections. Devices require a VPN client to connect to the network (which is the major drawback). Once connected, clients are just another device on the network and don't realize that they any different than a locally connected device.
  - **Tunnel mode**. Tunnel mode is the default IPSec VPN mode. With this mode, the entire communication is protected by IPSec.
  - **Transport mode**. Transport mode is mostly used for peer-to-peer communications, such as when a client device remotely connects to a server (such as using RDP). Transport mode can enhance peer-to-peer communication by encrypting it.
  - **Authentication Header (AH)**. This protocol provides for authentication of the entire packet. It doesn't provide data confidentiality.
  - **Encapsulating Security Payload (ESP)**. This protocol provides for data confidentiality and authentication. Authentication occurs only for the IP datagram portion, though.
- **Split tunnel vs. full tunnel**. A split tunnel enables users to connect to a VPN and access resources on that network while also maintaining connectivity to the internet or another network. For example, if you are at home, you can VPN to your corporate network while still maintaining internet access through your home internet connection. A full tunnel is one that sends all communication through the VPN. For example, if you are connected to a full tunnel VPN and go to an internet-based web site, the request will go out through the VPN network, not the local network.
- **TLS**. A TLS VPN operates over TCP port 443 and can be connected to via a browser (such as through a portal) or through a VPN client. A TLS VPN simplifies the firewall configuration because only a single port is required. It can also be helpful for organizations that want to use only a portal and avoid the deployment and maintenance of VPN client software.
- **Always-on VPN**. Historically, VPN connections were initiated on demand — when you wanted to connect to your company network, you manually connected. With an always-on VPN, your computer is always connected to your company network. It happens automatically when the computer is connected to the internet. An always-on VPN provides an enhanced user experience and can increase productivity by having people always connected.

## NIPS/NIDS

A network intrusion prevention system (NIPS) is a type of IDS that sits inside the network to protect the network from malicious traffic. It is an active solution that can block certain types of malicious communications. A network intrusion detection system (NIDS) is a type of IDS that is placed inside the network to monitor network communications for malicious behavior. It is a passive solution that provides detection and alerting.

- **Signature-based**. When monitoring network traffic, a signature-based approach is common. Signatures are pre-created based on known attack patterns. While this approach is common and effective, it has limitations. For example, it cannot detect zero-day attacks.

- **Anomaly**. With anomaly-based detection, the solution creates your organizational baseline. When traffic is too far outside of the baseline, action can be taken or an alert can be generated. Baselines are critically important for detecting anomalies. Baselines often look at traffic patterns, bandwidth usage and communication details (protocols and ports).

- **Heuristic/behavioral**. Like anomaly-based detection, heuristic-based detection looks for traffic outside of the norm, based on established patterns of usage at your organization. But instead of relying on baselines, heuristic detection looks at behavior-related factors such as the speed at which activities take place, the location from which activities occur, and the type of hardware or software used in a request.

- **Inline vs. passive**. An inline solution is situated on the network, often between two key distribution points. An inline solution inspects traffic live. A passive solution receives traffic through mirroring or another method and is often used for detection purposes only.

- **In-band vs. out-of-band**. In-band is synonymous with inline. Out-of-band is synonymous with passive.

- **Rules**. Rules are used to determine whether traffic is malicious or should be allowed, and whether it generates an alert. Rules are precise and detailed. You can include sources, destination, ports and other options. A rule can trigger an alert or another action. For example, you might decide not to act on every port scan. But you might act if you see an internal IP address communicating over FTP to a country where you don't do business.

- **Analytics**. IPS and IDS solutions can generate a lot of alerts. Often, there is information overload and alerts get ignored. Solutions use analytics to make sense of the large influx of data with the goal of showing security teams only what they want or need to see. Two key concepts are:

    - **False positive**. False positives are alerts that indicate an attack is taking place when there isn't one. Having too many of these can be dangerous because teams start ignoring them and then miss a real alert.

    - **False negative**. A false negative is when malicious traffic is deemed to be benign. False negatives are dangerous because the malicious traffic is often ignored and thought to be safe.

## Router

A router is a hardware- or software-based device that enables communication between different networks. In today's networks, many hardware-based routers are multi-purpose devices and perform switching and firewall duties too.

- **ACLs**. ACLs on a router provide less functionality than ACLs on a firewall, although they can block or permit some of the same traffic. ACLS on routers can be used for stateless inspection decisions to block specific traffic when necessary but they are not meant to replace firewall functionality.

- **Antispoofing**. Attackers sometimes try to mask their real source address by spoofing other addresses. Routers can block spoofing attempts by using ACLs. While it is common to use ACLs for antispoofing, it would be in addition to antispoofing on a firewall.

## Switch

A switch is a hardware- or software-based device that connects computers or other switches together. Switches can be standalone devices that provide only switching functionality or they can bundled with routing and firewall functionality.

- **Port security**. By default, you can connect any computer to any port on a switch. With port security, you configure the switch to accept connections from known clients only. For example, a port can be configured to allow only a client with a specific MAC address. If a client with a different MAC address attempts to connect to the port, the connection is denied. You can configure all ports on a switch for port security (whitelisting known clients). Port security is an optional feature that enhances network security.

- **Layer 2 vs. Layer 3**. Traditional switching operates on layer 2, which relies on destination MAC addresses. Layer 3 routing relies on destination IP addresses. Most switches today provide features at layer 2 and layer 3, with each layer handling the appropriate duties (for example, layer 3 handling VLAN to VLAN communication).

- **Loop prevention**. In a layer 2 network, you have a loop if there are multiple paths between two endpoints. In such a scenario, packets get re-forwarded and broadcast storms can occur. The primary methods to prevent loops are using Spanning-Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

- **Flood guard**. A flood can occur when a MAC table is forced out of a switch. Without the MAC table, switches must send packets out on all ports instead of just to an intended port. To minimize the chances of a flood, you can implement port security.

## Proxy

A proxy is a hardware appliance or software that is used to make requests on behalf of users, whether the users are going from an internal network to the internet, or from the internet to an internal resource.

- **Forward and reverse proxy**. A forward proxy is often used to proxy web requests for clients on a LAN. All internet traffic goes to the proxy. The proxy serves the requests via cache or goes out to the internet to request the website. For web servers, all requests from your company appear to come from a single computer, the forward proxy. Forward proxies enhance security because they can be configured with filters for malicious sites, for sites based on categories and for malformed communications. Reverse proxies enable you to make internal resources available to the internet. For example, you might use a reverse proxy to enable users to get to your intranet site or to check their email from home. A reverse proxy enhances security by checking for valid requests, optionally authenticating users prior to passing the request to an internal resource, and using anti-malware features.

- **Transparent**. A transparent proxy sits inline on the network and performs proxy duties without you or your device being aware of it. With a non-transparent proxy, browsers are configured to contact the proxy server (and such configurations can be enforced). With a transparent proxy, proxying occurs without a browser configuration.

- **Application/multipurpose**. An application proxy is a specialized proxy, often used for scenario-based deployments instead of general web surfing or web publishing scenarios. Some application proxies provide single sign-on (SSO) capabilities, others provide reverse proxy functionality, and some are tied to specific software solutions.

### Load balancer

A load balancer is a network device (hardware-based or software-based) that listens for inbound requests and then directs those requests to back-end servers, often in a way that balances the requests across multiple back-end servers evenly. For example, if you have a load balancer in front of 5 web servers, the first request might get directed to Server1, the second request to Server2 and so on.

- **Scheduling**. Load balancer scheduling is the method by which requests get directed to the back-end servers. There are 2 common methods:

  - **Affinity**. Suppose you have 3 web servers and a load balancer. Sending each inbound request to a random web server could create problems for some web applications. For example, if the initial connection has a user log on to the web application and the user's next request is sent to another web server, that web server won't know about the user's logon and will request the user to log on again. Affinity solves this problem by keeping the user on a single server throughout the duration of their web application usage. You can do this by source IP address (although that has limitations — for example, an entire company might use a proxy or NAT and everyone will end up on the same server when they go to the web application). There are other affinity methods, too, such as using cookies.

  - **Round-robin**. Round robin is one of the simplest load balancing methods. It forwards the first request to the first server, the second request to the second server, etc. When it reaches the last server, it starts over again. Some round robin implementations offer weighted round robin — back-end servers are assigned a weight to more evenly balance requests across them.

- **Active-passive**. With active-passive load balancing, one load balancer performs the load balancing and a separate one is on standby. The standby load balancer performs load balancing only if the primary load balancer becomes unavailable or has performance issues.

- **Active-active**. In active-active load balancing, there are two or more load balancers and all of them actively participate in the load balancing, each handling a portion of the requests. An active-active configuration offers better performance than an active-passive configuration; however, you lose some flexibility for maintenance. For example, if you want to upgrade the software on one of the load balancers, you must first drain it (that is, allow current clients to seamlessly finish their existing sessions while new sessions are directed to other nodes), whereas with an active-passive strategy, you could upgrade the passive load balancer, switch traffic over to it and then upgrade the primary load balancer.

- **Virtual IPs**. In load balancing, a virtual IP is used to direct all requests. For example, you might have a DNS entry for your website's FQDN pointing to a virtual IP on the load balancer. The load balancer is configured to load balance to the private IPs on the individual web servers. The individual web servers are not configured with the virtual IP.

### Access point

An access point is a device (usually hardware, although it could be software) that is used to provide access to a network (usually a wireless network). There are several important configuration items in an access point:

- **SSID**. The Service Set Identifier (SSID) is how a wireless access point is identified. It is a unique identifier that facilitates communication on the network. It can contain text and be up to 32 characters in length.

- **MAC filtering**. An optional feature of many wireless access points is filtering by MAC address. With MAC filtering, you can specify the MAC addresses that can join the network. This was originally introduced as a security feature, but it offers a very limited amount of security. Many operating systems enable you to set your MAC address; by setting it to the address of a valid client, you could potentially gain access to the network (presuming the passphrase was also known). MAC addresses are transmitted with each packet, so you can easily find MAC addresses by capturing traffic, too.

- **Signal strength**. The strength of a wireless signal is measured in decibel milliwatts (dBm). A stronger signal provides better performance. If the signal is too weak, you might not be able to connect or the performance might be abysmal.

- **Band selection/width**. Wireless networks often offer multiple bands. For example, you might have a band at 2.4 GHz and a band at 5.2 GHz. The 2.4 GHz band is well suited for longer range but offers less performance. The 5.2 GHz band is well suited for open spaces and offers best-in-class performance. Sometimes, you can switch bands if one is heavily congested.

- **Antenna types and placement**. There are a few types of antennas, each with different characteristics. For example, an omni-directional antenna provides 360 degrees of coverage; these are the most common in use in homes and offices. Larger installations, such as on a campus, might use multiple directional antennas that all point to a central omni-directional antenna. Placement of antennas is important to overall coverage and importance. For a campus environment, you want to maximize line of sight between antennas. In a two-story home, you want to centralize the antenna as much as possible. In a large office building, you should place antennas on the ceiling and spaced out to ensure appropriate coverage.

- **Fat vs. thin**. Thin access points are entry-level and have limited feature sets, or can't be configured because they are part of a larger system that is centrally managed, or offload key tasks somewhere else. Fat access points offer enhanced features typically seen in enterprise environments. Completely standalone access points are also fat access points.

- **Controller-based vs. standalone**. Simple wireless networks have one standalone access point; it doesn't require any other devices and other devices don't require it. Larger environments require many wireless access points. For example, a building with 250 wireless access points can be time-consuming to manage; using a centralized control system simplifies the management of all the access points. For example, if you want to make a configuration change across all APs, you can do that from a central management system.

## SIEM

A security information and event management (SIEM) solution is a centralized repository of your logs and activities. For example, it might contain your server event logs, access logs and alerts generated from a cloud vendor. Many SIEM solutions offer advanced searching, reporting and data analytics.

- **Aggregation**. Aggregation is a foundational functionality of SIEM solutions. A SIEM solution gathers together all log files; the goal is to have everything in the SIEM.

- **Correlation**. When your SIEM solution has information from a variety of sources, you need a way to correlate the events. For instance, if a user logs on to their client workstation, downloads a file from a website and then transfers that file to a cloud-based storage service, you need a way to tie those events together into a single incident or chain of actions. Without correlation, it is difficult to see the big picture of what transpired. Many SIEM solutions offer correlation. Some offer correlation using machine learning and artificial intelligence; and other even offer cloud-based correlation.

- **Automated alerting and triggers**. In addition to being a repository for information, a SIEM solution can also generate alerts based on triggers or specific activities to notify teams of activities in near real-time (although due to performance concerns, alerting is sometimes delayed by a few minutes).

- **Time synchronization**. Time synchronization is important on a network. From a SIEM perspective, it is critically important, especially for correlation. If the clock on a web server is off by a few minutes compared to the clock on a database server, you might have trouble correlating related events.

- **Event deduplication**. Deduplication helps improve the efficiency of storing information. It is commonly used by storage platforms. It is also used by SIEM solutions to merge identical alerts and to reduce the amount of storage required to store log data.

- **Logs/WORM**. In a high-security environment, you can use write once read many (WORM) storage to ensure that data is never overwritten, whether accidentally or purposely. Sometimes, you need to do this for compliance or auditing reasons. Other times, you might do this for security reasons. Without WORM storage, you need to have a solid backup in place to ensure you don't lose data.

## DLP

Data loss prevention (DLP) is a service that checks for misuse of data, often focusing on data leaving the company by way of email, file transfer or other methods. DLP is most commonly associated with email but it is also used for databases and intranets. Many DLP technologies can block misuse of data (such as putting personally identifiable customer information in SharePoint). Additionally, DLP solutions can often automatically protect information by encrypting it or applying other data protection methods, such as by using digital rights management.

- **USB blocking**. Many DLP solution can block the use of USB ports for removable media. This eliminates the possibility of a user taking sensitive data outside the company on a portable drive. Blocking the use of USB is important, especially if you don't have a way to monitor and block potentially sensitive data from being copied to portable drives.

- **Cloud-based**. While DLP solutions initially protected on-premises data only, they are quickly expanding to the cloud. As organizations move data to the cloud, they need the same DLP protections as they have on premises; in some cases, organizations want expanded protection for the cloud. Cloud-based DLP solutions integrate with public cloud providers to scan and protect their storage services and other compatible services.

- **Email**. DLP, as related to email, is a service that checks inbound and outbound email for specific data, especially private or personal data that your organization doesn't want sent via email ordoesn't want sent out to the internet. When it detects specific email, a DLP solution can block the email, log a violations, notify the security team or take other actions. Common items that are checked for include Social Security numbers, credit card numbers, account numbers and other personally identifiable information.

## NAC

Network access control (NAC) is a service that ensures network clients meet minimum requirements before being allowed on the network. For example, a NAC solution might check a computer to see if it has up-to-date anti-virus software, has the latest security patches, or is running a legacy version of an operating system. If everything checks out, the client can join the network. If not, the client is denied network access or is directed to a remediation network to download security patches, obtain the latest anti-virus updates or install necessary security software.

- **Dissolvable vs. permanent**. A dissolvable agent is downloaded and installed when you attempt to gain access to the network; the agent performs checks and then it is removed. A permanent (or persistent) agent is a traditional agent that is installed and stays on a computer indefinitely. You must manage the deployment and maintenance of permanent agents, which is a downside.

- **Host health checks**. As part of gaining access to a NAC-protected network, your device must pass a host health check. Checks are configurable. Simple checks might involve checking to see if the host has the latest security updates and an anti-virus product running. Advanced checks might look deeper, such as whether the computer has the latest anti-virus definitions, specific security patches or a specific Windows registry entry, or whether a specific user is signed in.

- **Agent vs. agentless**. Some NAC solutions don't use agents. For example, Microsoft offered a NAC solution that was integrated with Active Directory and was able to perform checks without an agent. With an agent, you often can perform deeper checks. Plus, the initial check can be faster than having to install a dissolvable agent or have an agentless scan performed. However, agents require management overhead for deployment, upgrades and maintenance.

## Mail gateway

A mail gateway is a device that sends and receives email. Often, a mail gateway is used on the edge of a network to enhance the security of the email environment. It can authenticate and validate traffic before the traffic reaches internal email servers.

- **Spam filter**. A spam filter is a service that checks inbound and outbound email for spam. There are many anti-spam detection methods and many spam filters use several methods to maximize their effectiveness. A spam filter usually sits in the DMZ so that spam doesn't reach the internal network.

- **DLP**. DLP, as related to an email gateway, checks inbound and outbound email for specific data, especially private or personal data that the organization doesn't want sent via email ordoesn't want sent out to the internet. A DLP solution at the mail gateway often checks only outbound email to the internet and email inbound from the internet but might not check internal (user to user) email.

- **Encryption**. Email servers and gateways can encrypt communications. While the default configuration across disparate email hosts does not encrypt communications, you can opt to encrypt communication with specific partners or specific domains, or to encrypt everything whenever possible. Encryption can also be on demand. For example, some gateways support the encryption of email when an email message meets specific criteria, such as containing a word like "private" in the subject).

**Bridge**

A bridge is a network device that connects two or more networks together. When a router connects networks together, those networks remain separate. But when a bridge connects networks, they become a single network. A switch is a multi-port bridge with some enhanced features that a simple bridge doesn't offer, such as hardware separation of ports.

**SSL/TLS accelerators**

SSL/TLS accelerators. SSL and TLS accelerators are devices that aim to improve the performance of web servers by offloading cryptographic operations to the accelerator. In addition, many accelerators can inspect incoming traffic and block malicious traffic.

**SSL decryptors**

SSL decryptors. SSL decryptors decrypt encrypted traffic, and often inspect it and block malicious traffic. These are like SSL accelerators but often aren't designed to improve web server performance as a primary goal.

**Media gateway**

Media gateway. A media gateway is a device that translates different media streams, typically on a telephony network.

**Hardware security module (HSM)**

Hardware security module (HSM). A hardware security module is a device dedicated to creating and managing digital keys used in public key infrastructures, cloud infrastructures and other scenarios. An HSM is considered a must-have for organizations where security is of utmost importance. An HSM is typically used across large enterprises and is rarely used in small environments due to the complexity and cost.

# 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

This section of the exam focuses on testing the security of an existing network. You should be familiar with the tools and methods so that you can choose an appropriate tool or method based on the requirements and goals.

### Protocol analyzer

A protocol analyzer, often called a sniffer or packet capture utility, is a tool to capture and analyze network communications. You can run a protocol analyzer on a computer, mobile phone or many other devices. You can also use a protocol analyzer to analyze captured packets, such as packets from a previous session.

### Network scanners

A network scanner scans a network or a series of devices to find open ports and specific types of web applications, figure out whether devices are responding, and find vulnerabilities.

- **Rogue system detection**. A rogue device is an unknown and unauthorized device that is plugged into the network. Being able to detect and remove them is essential because they can be malicious or create problems on the network. Many scanners can help detect rogue systems with special functionality. Other times, you can do it manually by comparing operating system information, versions and running services.
- **Network mapping**. Mapping a network involves figuring out all the devices on the network and how they are connected. Often, a network mapping exercise ends with a series of diagrams showing all the devices and connectivity.

### Wireless scanner

Wireless scanners scan for wireless networks in range, whether they are hidden or visible to everybody. They report high-level information about the networks, such as the SSIDs, signal strength, manufacturer, MAC address and channel.

### Wireless cracker

Wireless cracker. A cracker is a tool that tries to obtain access to a wireless network without authorization, for example, by attempting to crack the keys or brute-force the passphrase.

**Password cracker**

A password cracker tries to convert hashed passwords into plain text. It can work against operating systems, directories, databases or other systems that store passwords in hashed format. Password crackers are generally used in an offline model, running for a long period of time against the hashes.

**Vulnerability scanner**

A vulnerability scanner is used to find missing patches, known vulnerabilities and insecure configurations on a network, on a host or across a series of devices. It is regularly updated to expand the number of vulnerabilities it can detect. Scanners are often used in pen tests, and internal IT teams sometimes use them to check the network for vulnerabilities.

**Configuration compliance scanner**

A configuration compliance scanner is like a vulnerability scanner, but instead of looking for vulnerabilities, it looks for specific configuration settings dictated by the user. For example, a configuration compliance scanner can determine whether an organization's web servers are configured in accordance with its standards.

**Exploitation frameworks**

Exploitation frameworks are tools to facilitate exploits. They enable you to choose the exploit and what happens after you gain control of the device via the exploit. For example, a framework might try to exploit a known buffer overflow vulnerability. These tools are useful for hackers but also for internal IT security teams to test their systems.

**Data sanitization tools**

When you need to dispose of storage devices, you need a way to securely erase the data first. Data sanitization tools can securely erase data so that it cannot be recovered. Many of the tools overwrite data in several passes, sometimes with random data. With each additional overwriting pass, the erasing becomes more permanent and therefore more secure. In addition to sanitizing data, you can sanitize entire hard drives too.

**Steganography tools**

With a steganography tool, you can hide data inside other files (carrier files). Commonly, picture and video files are used to hide data. It is a good practice to choose a carrier file with the appropriate size for the data you want to hide. For example, if you want to hide 500KB of data, you should have a file that is at least 5MB in size. If you try to hide 500KB of data in a carrier file that was originally 10KB, it might raise suspicions. For example, if you open a large video file only to find that the video is a few seconds long, that would seem odd, because you would expect the video to be longer since the file is large.

**Honeypot**

A honeypot is a computer system configured to attract attackers. You can use a honeypot to figure out if a network is under constant surveillance or attack. Deploying a honeypot can provide information about the types of attacks the network is facing.

### Backup utilities

Backup utilities make copies of data, usually on a separate storage device, such as a tape, or into another network, such as a public cloud. Some backups are not encrypted. Sometimes, backups are stored off site. When assessing the security of an environment, you should review the backup procedures to see if the backup data is at risk when being backed up, stored or transported.

### Banner grabbing

When you connect remotely to an FTP server, email server or other service, the service often responds with a banner that indicates what software is running, the version of the software and the supported features. Some attackers use banner grabbing tools to grab all the banners on a network and then they scan the banners to look for older software versions or vulnerable software. While some services allow for the modification of the banner, that often doesn't reduce the risk because there are ways to identify the software and versions other than grabbing the banner. For example, you can sometimes use SNMP to query a device for hardware and software information, use fingerprinting tools (which rely on the details of ping responses, open ports and other proprietary methods), or gain physical access to devices (which often have identifying information on the back or bottom).

### Passive vs. active

A passive device sits outside the direct path of communication, or is on standby, ready to become active upon request. Passive devices are sometimes at risk because an attacker could target them without being noticed. Active devices are typically live on the network, in the direct path of communications, or actively participating in a service. Passive and active also come into play in scanning. Active scanning is scanning that connects to services and obtains as much information as possible. Active scanning can often be picked up by an IDS or other security solutions. Passive scanning is slower and sometimes doesn't obtain as much information, but passive scanning can be harder to detect, so an attacker might be able to passively scan an environment without anybody noticing.

### Command-line tools

Command-line tools are run without a graphical user interface. You can run them on a variety of computers and sometimes even on smartphones.

- **Ping.** The Ping command is a multi-platform utility, originally written for UNIX, that uses ICMP to communicate with remote hosts. It is often used to see whether the remote hosts are reachable on the network, whether the remote hosts are running, and how far away the remote hosts are (by seeing how long it takes for the ICMP packets to return).

- **Netstat.** The Netstat command enables you to look at the current network communications on a host. You can use it to look for listening ports and established connections. It is a good troubleshooting tool, especially when you are trying to find out if a host is listening on a specific port.

- **Tracert.** The Tracert command, often called "traceroute," is a cross-platform tool used to show the route from the current host to a remote host, while also measuring delays in the path along the way. It relies on ICMP and doesn't work well across firewalls (depending on the configuration).

- **Nslookup/Dig**. If you want to query a DNS server, you can use the Nslookup command on Windows or the Dig command on Linux. You can query for individual DNS records. For example, you can ask for the IP address of www.google.com. You can also use it to ask for all DNS records in a domain, although that is often blocked due to security concerns.

- **Arp**. The Arp command is used to display the ARP table on a host. It can also be used to delete ARB entries in a table.

- **Ipconfig/ip/Ifconfig**. To obtain the network information about a host, you can use the Ipconfig command on Windows or the Ifconfig command on Linux. The commands will display the IP address, subnet mask, gateway, DNS servers and other details about your network configuration. You can also use these commands to clear the host's DNS cache.

- **Tcpdump**. Tcpdump is a command-line packet analyzer that can capture communications on the network. It is a cross-platform tool that is very useful for troubleshooting.

- **Nmap**. Nmap is an open-source security scanner. You can use it to scan hosts for vulnerabilities, scan for open ports, or fingerprint remote hosts to find out which operating systems they run. This tool is very useful for analyzing an environment.

- **Netcat**. Netcat is a network tool that can be used to perform network troubleshooting, explore networks or scan for open ports. It is flexible and can be used in many ways. In its simplest form, it can be used to initiate a connection to any port using UDP or TCP. For example, you can initiate a connection to an email server on TCP port 25.

# 2.3 Given a scenario, troubleshoot common security issues

For this section, you will be presented with a scenario and you need to troubleshoot the problem or problems. You should be familiar with a good first troubleshooting step, as well as what to do if the first or second typical troubleshooting steps were already performed but didn't yield results.

### Unencrypted credentials/clear text

To troubleshoot insecure credentials, you should use a packet capture tool. You can capture at the source, at the destination or both. Most of the time, you should capture at the destination because you want to validate that credentials are being transmitted over the network insecurely. For example, if you suspect that an application that integrates with Active Directory is validating passwords insecurely, perform the following steps:

1. Configure the app to point to a single domain controller. Often, apps point at load balanced virtual names, so you should reconfigure the app to ensure all authentications are sent to a single domain controller so you can capture all the packets.
2. Install a packet capture tool on the domain controller or prepare the domain controller for packet capturing if you have a centralized packet capture tool.
3. Start capturing packets.
4. Perform logons to the application.
5. Analyze the packet captures to find out if credentials are being sent in clear text.

### Log and event anomalies

When unusual events or log entries are noticed, you should check to see whether the issue has already been logged by reviewing the logs and trying to correlate the entries with any known outages or degradations. If you have multiple servers running the same service, you should check the other servers to see if they are also getting the events or log entries. You can also use a search engine to search for event IDs or unique information logged in the event.

### Permissions issues

To troubleshoot permissions issues, you need to identify the permissions methods being used. For example, for a shared folder, there are both file system permissions and share permissions. When users are local on the server with the shared folder, only the file system permissions are applicable, but when users connect to the shared folder remotely, the file system permissions and the share permissions are both applicable. Other troubleshooting steps include turning on verbose logging, checking to see whether other users are experiencing the same issue, and trying the connection from a different device.

### Access violations

Access violations occur when a user accesses a resource or data that they are not authorized to access. The user might have accessed the resource or data by mistake or the action might have been malicious. To troubleshoot, you should track the user's activity for an hour before the access violation and try to answer key questions such as: When did the user initially sign in? Did the user sign in to multiple computers? What resources or data did the user access just before the access violation? What did the user do just after the access violation? Your goal is to figure out the intent of the user and to find out whether any other unauthorized activities occurred. For example, after accessing the unauthorized data, did the user connect to an unknown IP address on the internet?

### Certificate issues

There are a few common certificate issues you need to know:

- **Expired certificates**. Expired certificates can't be used. Expired certificate warnings are generally displayed, and communications often revert to insecure (such as from HTTPS to HTTP).
- **Untrusted certificates**. Operating systems usually have built-in certificate trust stores that provide built-in trust for certain certificate issuers. When you go to a website with a certificate from a trusted issuer, your browser permits the connection. If you go to a website with a certificate issued by an untrusted issuer, your browser will warn you about the danger and enable you to choose what to do next.
- **Mismatched certificates**. Suppose a user goes to https://www.google.com but the certificate used was issued for another domain name; that's a mismatched certificate. Most browsers will warn about mismatched certificates because it often is indicative of malware or a misconfiguration.

### Data exfiltration

When data is removed from a corporate device without authorization, it is known as data exfiltration. This is one of the key tasks that malicious users try to perform. First, find out which data was exfiltrated. Was it protected with digital rights management (DRM)? How much data was exfiltrated? Was other data exfiltrated previously? You should track the offending user account back several days to look for other unauthorized activities.

### Misconfigured devices

A misconfigured device is one that is in its default state or that otherwise has a configuration that puts the organization at risk.

- **Firewall**. If a firewall is misconfigured, it might allow malicious traffic into your network. You can review the most recent firewall configuration changes to see if a recent change is the cause. Otherwise, you can review the hit count on the firewall rules for anything out of the ordinary. Finally, you can compare the current configuration to a backup from a few days ago to look for changes.
- **Content filter**. If you use a content filter but it is misconfigured, it might not be filtering everything you want. It is helpful to compare the configuration against another device or against a backup.
- **Access points**. Many organizations have multiple access points. If you suspect one is misconfigured, you can compare the software version and configuration against an access point that has the right configuration.

### Weak security configurations

Weak security configurations put your organization at risk. Common examples of weak security configurations are default passwords, unencrypted management services (such as a web interface for administration using HTTP), insecure services (for example, Telnet), old versions of firmware or software, unpatched software, and lack of adherence to the principle of least privilege. You can troubleshoot these scenarios with a vulnerability scanner, a port scanner and a configuration management solution.

### Personnel issues

Personnel issues involve issues with people, typically employees or contractors.

- **Policy violation**. When a policy violation occurs, the person that violated the policy must be notified and the incident must be logged. Because policy violations can ultimately lead to termination, policy violations should be logged with specific details, such as the date, time and specific violation, and an action plan should be developed to ensure it doesn't happen again.
- **Insider threat**. An insider threat is a person inside your organization who has malicious intentions. Such threats can be hard to detect. Adhering to the principle of least privilege helps limit insider access, and having extensive auditing and logging in place can help you spot malicious activity.
- **Social engineering**. A key way to limit the effectiveness of social engineering is to routinely test employees with fake social engineering campaigns. For example, you might send a fake phishing email to employees and track who clicks on it, and have a third-party company attempt to gain access to your facility by having someone pose as an electrical utility worker. Education is the key. Employees must understand the threats and know what to do if they see one or are unsure.
- **Social media**. Social media can be a negative in a couple of ways: Employees might spend too much time there during working hours or confidential information might be accidentally shared there. Organizations often limit social media access or have specific use policies. You can use content filters and auditing and logging to track social media usage rates and look for anomalies.
- **Personal email**. Like social media, personal email can hurt employee productivity and be used to exfiltrate data. You can limit access to personal email services, use a proxy server to audit and log usage, and use a DLP solution to protect against data exfiltration.

### Unauthorized software

When employees install unauthorized software, it can put the organization at risk. The software could have malware embedded in it or be unstable and cause system issues. You can prevent employees from installing software on their computers. Additionally, you can use a configuration management solution to scan for unauthorized software on computers and automatically remove it.

**Baseline deviation**

A configuration management solution often has agents deployed to devices, which check configurations at set times. When deviations from your baseline are detected, they can be automatically remediated or logged and reported. To maximize security, you should automatically remediate baseline deviations.

**License compliance violation (availability/ integrity)**

Many organizations use third-party license management solutions to manage their licenses. Such solutions help you figure out if you need more licenses and if you comply with the licensing requirements. Without such a solution, you can use a configuration management solution to count the total number of licenses or installations and compare that against your license ownership counts.

**Asset management**

Asset management involves managing hardware (computers, phones, etc.) and software (such as licenses). You can use an asset management solution to track assets. It will have a database and likely use barcodes for all physical assets, which can be scanned in by a handheld scanner. Smaller organizations can use a spreadsheet to track all assets.

**Authentication issues**

To troubleshoot authentication issues, you can use a packet capture tool (to look at the connectivity and authentication methods, and check for encryption errors), event logs and log entries (to check for bad passwords or other authentication issues), and trial and error (for example, if a user can't authenticate to a web server, you can check if they can authenticate somewhere else to determine whether the username/password is valid).

## 2.4 Given a scenario, analyze and interpret output from security technologies

For this section of the exam, you will be presented with output and several descriptions of that output; you need to select the most appropriate description. Having hands-on experience for this section is helpful, especially if you don't work with this type of output on a regular basis.

**HIDS/HIPS**

Alerts coming from HIDS or HIPS will typically indicate a potential intrusion or attempted intrusion that was blocked. These are important alerts that must be acted upon quickly, typically by a security operations center.

**Antivirus**

Output from antivirus software usually indicates information about recent antivirus scans, detection of a virus or other malware, and alerts about other issues (such as the antivirus service being stopped or disabled). You can use this information to correct issues.

**File integrity check**

If a file integrity check fails, there will often be a message about a checksum mismatch or something similar. You should not trust files that fail integrity checks because they could be malicious.

**Host-based firewall**

A host-based firewall typically outputs three things: alerts, update notifications and logs. Alerts tell you that some type of communication has come in; you might have to act, or it might have been blocked automatically. Update notifications indicate that the firewall has updates to perform. Logs are the logs from the firewall. Typically, default logs track service startup and shutdown, update events, and other non-critical events. You can turn up the logging levels to capture additional details, such as every time a firewall rule is used or communication is blocked.

**Application whitelisting**

When you whitelist an application, you mark it as safe to run. Whitelisted applications typically do not go through a security check upon launch. In some cases, only whitelisted applications can run. Output from application whitelisting relates to apps that tried to run but aren't whitelisted or trouble with a whitelisted app (maybe it was updated and isn't working correctly with the whitelisting).

**Removable media control**

Removable media can be used to exfiltrate data or introduce malware. Many organizations prefer to restrict or disable the use of removable media. Some operating systems have built-in tools to help restrict or disable removable media. Third-party solutions offer enhanced options and reporting. You want to audit the use of removable media (to assess whether your controls are functioning) by reviewing log files and setting up alerts.

**Advanced malware tools**

Malware tools will report whether they find malware, as well as whether they were able to remove, block or quarantine the malware. This output is important because you might have to take manual action to remove malware.

**Patch management tools**

Output from patch management tools usually indicates whether patches were successfully installed. When they are not installed successfully, you need to analyze the detailed log entries to see the reason (for example, insufficient disk space or lack of permissions).

**UTM**

A unified threat management (UTM) solution combines some network features into a single device that provides network-based security (such as proxy, reverse proxy and firewall). You can turn on verbose logging, review log files and troubleshoot rules as part of your troubleshooting scenarios.

**DLP**

DLP systems provide alerting, which is configurable. You can have a DLP solution alert you if there is suspected data loss or any DLP rules were broken. DLP log files also capture such events and these should be sent to a SIEM solution.

**Data execution prevention**

Data execution prevention (DEP) is a technology that helps protect memory from malicious code. There is hardware-based DEP and software-based DEP. You can protect individual applications with DEP, or you can protect an entire computer. You can troubleshoot DEP by configuring it for a single application and then going through tests. You can also increase the logging level to get more information about a troubleshooting scenario.

**Web application firewall**

A web application firewall (WAF) helps protect applications from malicious attacks. A WAF can inspect app requests at the app layer to block advanced web-based attacks. WAFs have rules, like a firewall. You can check whether the rules are being used and capture traffic with a packet capture or built-in debug command.

## 2.5 Given a scenario, deploy mobile devices securely

The mobile computing world is growing: New functionality is routinely introduced and people are doing more on their mobile devices. Therefore, you need to understand how to secure the use of mobile devices. Like other exam sections, this one focuses on scenarios. Be sure you are comfortable recommending one or more technologies based on the requirements in a scenario.

**Connection methods**

Smartphones have a variety of ways to communicate. Some facilitate voice communications while others are targeted for data transfer or niche uses.

- **Cellular.** Smartphones connect to cellular networks over radio waves. A cellular network is split into cells, with cell towers providing the radio coverage for a designated geographic area. Some of the common cellular networks are GSM and CDMA.
- **WiFi.** WiFi is a wireless local area networking technology that uses radio technology to communicate. There are many WiFi standards, including 802.11n, 802.11ac and 802.11ay.

- **SATCOM**. Satellite Communications (SATCOM) is a technology that uses satellites to communicate. SATCOM can provide internet access and voice communications to devices, homes and businesses.

- **Bluetooth**. Bluetooth is a data communications standard using a wireless technology over 100 meters or less (often, much less). Bluetooth is used in a variety of devices including headphones, mice and keyboards. It doesn't provide the same level of performance and bandwidth that WiFi provides, but it is often enough for common peripheral uses.

- **NFC**. Near Field Communications (NFC) is a wireless communications technology that provides for communications up to 3 feet. It is mostly used for mobile payment systems or mobile-to-mobile small data transfers, such as sharing contacts. Performance is quite limited, with max speeds up to 424 kb/s.

- **ANT**. ANT is a proprietary wireless networking technology mostly used by smart wearables such as heart rate monitors, smart watches and sleep trackers. It is geared toward use with sensors and permits communications up to 30 meters.

- **Infrared**. Infrared communication is a wireless technology that relies on light that humans can't detect with their eyes. It is mostly used in consumer devices such as remote controls for televisions and other devices.

- **USB**. USB is a wired communication standard for transmitting data between devices that support USB. The latest version is 3.2 which provides maximum speeds up to 20 Gb/s. USB is mostly used to connect peripherals like keyboards, mice and printers to computers.

## Mobile device management concepts

There are many ways to manage mobile devices. For example, you can use a mobile device management (MDM) solution. Whichever method you use, there are certain concepts that are commonly used across all the management solutions. Be familiar enough with them that you could recommend them based on a scenario with requirements or a list of challenges to solve.

- **Application management**. When a device is under management, especially by an MDM solution, it can have its applications managed. For example, an organization might deploy 3 or 4 internal apps using the MDM solution. Or the MDM solution might be configured to block certain apps.

- **Content management**. Content management focuses on managing the data lifecycle on smartphones. Generally, this includes file storage (such as how files are stored on a device), file transfer (such as how files move from the smartphone to other repositories), and file sharing (such as being able to share a file with another user). From a security perspective, content management is important. If you can't provide a good user experience and enterprise-grade security, the solution might not be widely accepted or used.

- **Remote wipe**. Remote wipe is the capability to remotely delete the contents of a phone — apps, data and configuration. Remote wipe might include only business data or could include all data. Remote wipe is a key feature that can help minimize the chances of data loss if a phone is lost or stolen.

- **Geofencing**. Geofencing is a technology that enables actions based on a smartphone's location. For example, if a smartphone is taken outside of your organization's country, you can disable Bluetooth and send an alert to the phone notifying the user about Bluetooth being disabled. Geofencing can be used for productivity purposes (such as tracking a delivery driver) or for marketing (such as a mobile app sending a coupon as you enter a store).

- **Geolocation**. Most phones have GPS built in; this enables apps and the phone to track its geographic location. Geolocation can be used for access. For example, if your phone is outside of your home country, an app could be configured to deny you access.

- **Screen locks**. Screen locks are used to keep data on phones safe, especially in the event of a lost or stolen phone. Screen locks are often automatically deployed after a period of inactivity, such as 5 minutes. Screen locks are a key security option you should use across all phones.

- **Push notification services**. Push notifications are alerts that an app can send you based on a variety of environmental attributes, actions or locations. A simple example is a game that sends a push notification when it is your turn to play. Push notifications are also useful in business. For example, an emergency alert service might send a push notification to employees during a natural disaster. Many MDM solutions offer a push notification feature and enable management of push notification settings on smartphones.

- **Passwords and PINs**. Passwords and PINs are often used to unlock phones and apps, and are also used within apps for enhanced security. While passwords and PINs are older than biometrics, they are still considered more secure in certain scenarios. In some countries, people are not required to provide authorities with their passwords and PINs.

- **Biometrics**. On mobile devices, biometrics typically refers to fingerprints, face scans and retina scans. These biometric solutions are often used to unlock phones and apps, and are also used within apps for enhanced security.

- **Context-aware authentication**. Legacy authentication relies on passwords. Newer styles of authentication require multiple authentication factors (such as a mobile app or biometrics). Context-aware authentication uses information about the authentication transaction to decide whether to authenticate a user. For example, context-aware authentication might check the device being used to authenticate to see if it is a known device, if it has ever been used before, or if it is a company-owned device. A context-aware authentication might also look at the location of the authentication request — is it coming from a known network? Has the person ever authenticated from that location before? Many factors can come into play, based on your requirements. A context-aware application can ask for a second factor of authentication if a user's authentication request is considered higher risk (new device, new location or unusual time of day, for example).

- **Containerization**. Many MDM solutions take advantage of containerization. Containerization is the process of creating and using containers to isolate corporate apps and data from personal apps and data. For example, you might store all corporate data in a secure container while leaving all personal data in a default state. In this scenario, administrators can wipe a phone but impact only the corporate data (such when an employee is terminated).

- **Storage segmentation**. Storage segmentation is like containerization, but storage segmentation focuses strictly on segmenting storage, while containerization provides a bigger isolation environment for data, apps and services.

- **Full device encryption**. Full device encryption is the encryption of the entire disk. In such scenarios, you are required to unlock the encryption upon reboot, typically with a passcode or passphrase. The downside is that your phone's services (such as alarms or phone calls) are not available until you unlock the disk upon startup. Some smartphones are moving toward file-based encryption, which encrypts files on demand. File encryption can use different keys and methods for encryption, while full disk encryption is limited to a single key and method. Many organizations require encryption of user data, at a minimum. Such organizations usually enforce encryption through their MDM platform.

### Enforcement and monitoring for

- **Third-party app stores**. Many of the large vendors, such as Apple and Google, offer a dedicated app store for their devices. By default, employees can download and install any apps from the app store. Some of these could be malicious and some might be unsuitable for a work environment. Organizations can use mobile device management software to block the installation of certain apps or certain categories of apps. This can reduce the risk that employees will download malicious software without realizing it.

- **Rooting/jailbreaking**. Many mobile device management solutions have a built-in feature to detect rooted (relevant to Android) or jail broken (relevant to iOS) devices. Such devices have bypassed the mobile OS security and are at risk of vulnerabilities or malware because the user can install apps from any source, such as a source outside of the vendor's app store. Many organizations block rooted or jail broken devices from joining the network.

- **Sideloading**. Sideloading refers to the installation of apps outside the app store. While many app vendors prefer to work only within the vendor app stores, occasionally they offer an app outside the app stores. However, apps offered outside the app stores do not go through the rigorous vetting process that they would in a vendor app store. This poses additional risks for your organization. MDM solutions can block sideloading.

- **Custom firmware**. Some smartphones, especially those based on the Android platform, support custom firmware. In some cases, custom firmware opens features not available with the default Android software. However, custom firmware can present additional risks for an organization. Often, organizations block devices with custom firmware.

- **Carrier unlocking**. Many smartphones are locked into one or a couple of carriers. But you can often unlock a smartphone and switch carriers. For BYOD scenarios, this is not a concern for an organization. But with corporate-owned devices, this might not be a desired scenario.

- **Firmware OTA updates**. Many smartphone vendors provide firmware updates over the air (OTA). Generally, firmware updates are important because they often include security patches and updates. But organizations often like to test the firmware updates to ensure stability and compatibility before they officially support the firmware.

- **Camera use**. In high-security environments, organizations sometimes block access to the camera. This ensures that employees can't take pictures of documents or of sensitive or restricted areas.

- **SMS/MMS**. Text messaging over SMS/MMS is a common feature available on most smartphones. Some organizations need to restrict SMS/MMS use (such as to business use only) or disable SMS/MMS use (such as a high-security organization that requires only secure communication mechanisms).

- **External media**. Some devices accept external media. For example, you can plug in a storage device and copy data. Organizations sometimes block access to external media to reduce the chances of data loss.

- **USB OTG**. USB on-the-go (USB OTG) enables compatible devices to read data from USB drives without going through a computer. In most cases, you need a converter to convert the USB connection to a compatible connection type, such as micro-USB or USB-C.

- **Recording microphone**. Virtually all smartphones have built-in microphones that can be used to record audio. There have been reports of malware targeting microphones by turning them on and recording the audio. Some organizations prefer to block recording from the microphone to ensure that employees aren't secretly or illegally recording people or meetings.

- **GPS tagging**. In many smartphones, captured pictures are automatically tagged with GPS information. This enables somebody to look at the GPS coordinates of a picture and deduce where it was taken. In some environments, this might be a security risk. Organizations can opt to disable GPS tagging of photos in some MDM implementations.

- **WiFi direct/ad hoc**. WiFi direct is a technology that enables two wireless devices to connect to each other. Once connected, data can be shared. To minimize the chances of data loss, some organizations opt to block WiFi direct.

- **Tethering**. When one wireless device shares its internet connection with other devices, the other devices are tethered to the sharing device. Tethering is convenient because you can connect devices to the internet that don't have built-in internet access.

- **Payment methods**. Smartphone payments methods include payment solutions such as Apple Pay, Android Pay and Samsung Pay. These payment methods rely on NFC to seamlessly enable purchases at various venues, such as gas stations, vending machines and markets. For corporate-owned devices, some organizations disable mobile payment methods to prevent users from storing payment information on the devices.

## Deployment models

To efficiently deploy devices, you need to define the supported methods, put processes in place and document everything.

- **BYOD**. With bring your own device (BYOD), people access your network using devices they own and manage. Your organization installs device management software and ensures that the devices meet the organization's requirements. The advantage of BYOD is that everybody can get the supported device of their choice and they can upgrade as often as they want. Additionally, your organization doesn't have to procure devices or manage devices, which saves time and money for the organization. The downside is that organizations often must support a plethora of device types, which can become difficult. For example, the organization might want to deploy a new app, but if ithas device requirements, such as OS version requirements, it might not be able to because the organization can't force upgrades, updates or device changes on BYOD devices.

- **COPE**. Corporate-owned, personally enabled (COPE) is a model whereby organizations purchase devices and manage them. However, the organization allows users to use the devices for personal use, such as surfing the web, taking pictures, using social media and playing games. With COPE, device choices are typically more limited than BYOD. However, it is easier to support for the IT department and the IT department maintains more control.

- **CYOD**. With choose your own device (CYOD), organizations offer employees a choice of supported device types and the employee pays for the device and owns the device. Organizations deploy device management software. This model reduces hardware costs for the organization. CYOD sits somewhere between BYOD (think of this as a "wild west") and COPE (think of this as a more locked-down model).

- **Corporate-owned**. The corporate-owned model is a traditional model whereby the organization buys and maintains the hardware. Often, this model does not allow employees to use the devices for personal use. In such a scenario, employees routinely carry two devices — their corporate-owned device and their personal device. While some users enjoy this model, many do not because of the nuisance of carrying two devices. The downsides are relevant whether you're talking about smartphones or laptop computers.

- **VDI**. A virtual desktop infrastructure (VDI) is one that provides virtual desktops to users. This isn't a model valid for smartphone deployment but can be effective as a replacement for laptop deployment. Employees typically get a virtual desktop which they can connect to from their device (typically a laptop computer). The connection is often full screen, so it is like working on a corporate device. However, a smartphone isn't a good way to connect to a VDI for more than a quick task or two.

# 2.6 Given a scenario, implement secure protocols

For this section, you should be able to figure out which protocol or protocols you should use to meet the requirements of a given scenario. For example, you have an on-premises environment with servers and network devices, and you want to monitor them with a monitoring tool; which protocol should you use?

## Protocols

Many of the protocols in the following bullets are common protocols used routinely. However, if your experience is limited to one area (network or servers or desktop), you might not be familiar with all of them. Be sure you can differentiate between them for the exam.

- **DNSSEC**. Domain Name System Security Extensions (DNSSEC) is a specification for securing DNS information. DNSSEC calls for the signing of data to ensure that the data is valid. DNSSEC has not been widely adopted but is considered the standard for securing a DNS environment, especially from malicious attacks.

- **SSH**. Secure Shell (SSH) is a protocol used to secure network communications. It is widely used by server administrators to maintain Linux-based servers. SSH uses public-key cryptography. By default, it operates over port 22. You use SSH to sign into a secure shell on a remote server, but the protocol is also used elsewhere, such as with SFTP.

- **S/MIME**. Secure/Multipurpose Internet Mail Extensions (S/MIME) defines a standard by which you can securely communicate between two or more parties over email. S/MIME relies on public key cryptography, with parties exchanging their public certificate prior to secure communication. Most email clients support S/MIME, but it is not well-suited for web-based email.

- **SRTP**. Secure Real-Time Transport Protocol (SRTP) is a protocol to secure communications, typically over a telephony or communications-based network.

- **LDAPS**. Lightweight Directory Access Protocol Secure (LDAPS) is a protocol used to communicate securely with an LDAP server (a centralized directory that contains information about users, groups, computers and other network resources). It is an open standard and is implemented across a wide variety of products. For example, Microsoft's Active Directory Domain Services (AD DS and often just "Active Directory") provides LDAP and LDAPS functionality.

- **FTPS**. File Transfer Protocol (FTP) has a secure version, FTPS (File Transfer Protocol Secure). FTPS is FTP with extensions used to add TLS or SSL to the connection.

- **SFTP**. Secure FTP (SFTP) is different than FTPS: SFTP uses the SSH protocol to transfer files, whereas FTPS uses FTP. SFTP is more commonly used than FTPS.

- **SNMPv3**. Simple Network Management Protocol (SNMP) is a standards-based protocol for managing or monitoring devices over a network. It is commonly used in monitoring tools to obtain device information such as model number, firmware and software versions, and configuration information. Version 3 adds cryptographic capabilities, which is a big enhancement because SNMPv1 and SNMPv2 are considered insecure.

- **SSL/TLS**. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are protocols that provide secure communications over a network. SSL, now deprecated, was the initial implementation but was later superseded by TLS (although you can still find some use of SSL on the internet). TLS is newer and more secure, and offers additional features over SSL, such as forward secrecy.

- **HTTPS**. Hypertext Transport Protocol Secure (HTTPS) is an extension of HTTP that incorporates TLS (and sometimes the older SSL) to encrypt communications. HTTPS is the most widely used secure protocol on the internet.

- **Secure POP/IMAP**. Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are protocols used by email clients to communicate with email servers. Both offer a secure implementation using SSL or TLS. POP3, the third version of the protocol, is the most widely used, while IMAP is on version 4. POP3S is a secure version of POP3. IMAPS is a secure implementation of IMAP.

## Use cases

Beyond knowing the general meaning and functionality of the protocols, you need to know the scenarios in which you would deploy them. Below are some of the common use cases.

- **Voice and video**. Voice and video are two forms of communication. Voice translates to phone calls while video translates to video calls or video conferencing. For this use case, SRTP is appropriate. Additionally, there would likely be use of TLS for parts of the communication.

- **Time synchronization**. For time synchronization, the primary service is Network Time Protocol (NTP). NTP is a protocol to sync clocks between two devices over the network. It operates using UDP on port 123. There are other time services, either built on NTP or compatible with NTP, such as SNTP and Windows time service (W32Time).

- **Email and web**. For email , the primary protocols are SMTP (port 25, for email relay), POP/IMAP (for email retrieval using legacy email clients), S/MIME (for encrypted email), HTTPS (for administration and web-based email), and SSL/TLS (for securing various communications). For web, HTTP (port 80) and HTTPS (443) are the primary protocols.

- **File transfer**. For file transfer, you can opt to use FTP (quick, easy, lacking security), FTPS (like FTP but adds encryption), or SFTP (securely transfer files over SSH). Alternatively, you can use HTTPS for web-based file transfers.

- **Directory services**. For directory services, the most common protocol is LDAP and LDAPS. Active Directory and other standards-based directory services support LDAP and LDAPS.

- **Remote access**. For remote access to devices, HTTPS is the most common protocol. For remote access to servers, SSH (mostly for Linux-based computers) and RDP (Remote Desktop Protocol, mostly for Windows-based computers) are commonly used.

- **Domain name resolution**. For DNS, DNSSEC is the most common security protocol. Although not widely implemented, it is the standard for securing DNS when you have requirements for DNS security.

- **Routing and switching**. For routing and switching, there are several protocols. RIP, IGRP, OSPF and BGP are common examples. Routing Information Protocol (RIP) is a legacy protocol that uses distance-vector routing. Interior Gateway Routing Protocol (IGRP) is a legacy protocol by Cisco that also uses distance vector routing. Open Shortest Path First (OSPF) is an interior gateway protocol that provides more robustness than RIP. Border Gateway Protocol (BGP) is a complex routing protocol that provides the backbone functionality of the internet. For administration purposes, SSH and HTTPS are commonly used.

- **Network address allocation**. To efficiently and automatically distribute IP addresses to devices on a network, Dynamic Host Configuration Protocol (DHCP) is most commonly used. DHCP works via broadcast traffic initially.

- **Subscription services**. Network News Transfer Protocol (NNTP) is a legacy protocol used to communicate with Usenet, which hosts forums and file transfer. With NNTP, you subscribe to desired groups, whether for discussion or file transfer. Then, a client retrieves messages on demand or on a schedule basis. Traditionally, NNTP operated over port 119 (insecure) or port 563 (secure). Today, NNTP often operates over HTTPS.

# 3. Architecture and Design

This section is focused at a higher level than day-to-day operations. The expectation for this section is that you understand the implications of a technology or regulation, the pros and cons of certain technologies and design choices, and how technologies integrate with other technologies or in an environment for maximum security. There are 9 sections in Architecture and Design.

## 3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides

Sometimes, architects, engineers and administrators want to come up with their own designs, based on their own experience and knowledge. But this usually isn't the best path forward. Everybody has different experience and different levels of knowledge. Often, working in a big enterprise environment means a slower pace of technology integration and not being up to speed with the latest solutions and practices. It is a good practice to review and consider publicly available frameworks, best practices (especially from vendors) and secure configuration guides (whether from vendors or subject matter experts). Take your ideas and requirements and work with publicly available information to come up with the best available architecture and design.

### Industry-standard frameworks and reference architectures

Ensure that you are familiar with the most popular frameworks and understand the value or necessity of adhering to frameworks. Reference architectures aren't specifically covered below. Reference architectures are generally published by vendors with a goal of showcasing highly available, high-performance designs of their products. A key component of reference architectures is supportability — reference architectures are always a supported implementation, which is an important consideration when deciding on architecture and design.

- **Regulatory**. With regulatory frameworks, you are trying to meet a specific regulation in an industry, as part of working with a specific technology or as part of a government organization. One example is the Payment Card Industry Data Security Standard (PCI DSS), which governs organizations that store, transmit and process credit card and credit card holder data. The goal of PCI DSS is to ensure that organizations processing credit cards meet a minimum level of security with how they deal with credit card transactions. Organizations must be independently audited and certified.

- **Non-regulatory**. Non-regulatory frameworks are developed with similar goals to regulatory frameworks — improve security by providing information and guidelines to organizations. However, non-regulatory frameworks are not enforceable. Instead, they are voluntary; organizations can choose to adopt them or not. One example is the NIST Cybersecurity Framework (see https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

- **National vs. international**. Many countries have their own frameworks. Often, such frameworks apply only to government agencies or organizations working directly with government agencies. One example is the US FedRAMP program, which outlines a specific set of requirements for U.S. government agencies. See https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf for details. The International Organization for Standardization (ISO) provides frameworks across a wide variety of industries, including information technology. ISO/IEC 27000 has several frameworks published for international use.

- **Industry-specific frameworks**. Frameworks for industry are usually very specific to the industry. One widely known framework is the Healthcare Information Portability and Accountability Act (HIPAA), which has a goal of protecting the personally identifiable information and personal health information of patients. Healthcare providers must demonstrate compliance with HIPAA to avoid fines and even criminal penalties in some scenarios.

### Benchmarks/secure configuration guides

In addition to reference architectures, vendors often provide additional documentation covering performance benchmarks and secure configuration. These aren't necessarily step-by-step guides to use during an implementation, but high-level guidance that offers information to help you make choices based on your requirements. For the exam, you don't need to know about individual guides or memorize the information in them.

- **Platform/vendor-specific guides:**

  - **Web server**. Web servers are highly susceptible to attack, so many web server vendors provide guidelines to minimize the risk of compromise. For example, Apache publishes security tips at https://httpd.apache.org/docs/2.4/misc/security_tips.html.

  - **Operating system**. Many operating system vendors provide guides, guidelines or even scripts to help secure the operating system. For example, Microsoft publishes a security guide for Windows Server 2016 at https://download.microsoft.com/download/5/8/5/585DF9E9-D3D6-410A-8B51-81C7FC9A727C/Windows_Server_2016_Security_Guide_EN_US.pdf.

  - **Application server**. Application vendors also publish guides and best practices around hardening and configuration. One example is Oracle's Oracle Fusion Middleware Administrator's Guide, available at https://docs.oracle.com/cd/E21764_01/core.1111/e10105/toc.htm.

  - **Network infrastructure devices**. Many vendors provide guides for implementing their solutions. For example, NetApp publishes a security hardening guide for the ONTAP operating system that is used across their storage devices. See https://www.netapp.com/us/media/tr-4569.pdf for the NetApp Security Hardening Guide for NetApp ONTAP 9.

- **General-purpose guides**. There are many general-purpose guides out there, some from subject matter experts, some from IT pros based on their experience in the field, and some from other sources. One general-purpose guide is OWASP's OWASP Developer Guide, which can help developers build secure web applications. See https://www.owasp.org/index.php/OWASP_Guide_Project for details.

## Defense-in-depth/ layered security

Experts agree that the best approach to securing your environment is a layered defense. Instead of relying on a single security solution (such as an edge firewall), you build security in layers — at the edge, in the middle and on the client devices. A layered approach provides multiple levels of protection and makes it more difficult for attackers to gain access to your environment.

- **Vendor diversity**. Relying on a single vendor can put your organization at greater risk, especially when dealing with the cloud or a key infrastructure component. Some organizations opt to purposely mix vendors throughout their IT infrastructure to ensure that a single vendor's problem cannot disrupt their entire network. Vendor diversity also provides you more leverage when negotiating licensing and maintenance deals.

- **Control diversity**. To minimize risk, you should use IT controls from different areas. For example, you might combine physical controls (locked doors) with technical controls (resource-level permissions). You might opt to layer in other controls, too. Diversifying your controls is a good practice to ensure that you are not reliant on a single type and thus susceptible to issues if that one type of control fails or becomes degraded.

    - **Administrative**. Administrative controls are policies and procedures that your organization establishes to lower the overall risk in your environment. You might have an administrative control that ensures that employees don't follow each other into a locked building without swiping a badge or otherwise identifying themselves to the other person going in the door.

    - **Technical**. Technical controls are those that you use in your configuration. For example, you might use file system permissions to limit access or you might prevent certain types of users from logging onto specific computers.

## User training

As part of a multi-layered security strategy, you need to train users to understand their responsibility, understand where the risks are, and be able to identify threats such as phishing and social engineering. If you have state-of-the-art security systems but don't train your users, your organization is at risk.

# 3.2 Given a scenario, implement secure network architecture concepts

For this section, you should be familiar with all the technologies below, including when they should be deployed and the high-level details of a deployment, such as where things fit in a network and what purpose they serve.

## Zones/topologies

Be sure you know all these technologies and how they differ from each other:

- **DMZ**. A de-militarized zone (DMZ) typically sits at the edge of a network, straddling the internet and the LAN. It is commonly used for public-facing servers and appliances, such as web server for a public-facing website. It is common to also have reverse-proxy services and SMTP gateways in a DMZ. In many environments, resources in the DMZ are managed singularly and not with the same management tools that manage the LAN resources.

- **Extranet**. An extranet is like a DMZ because it is used to enable people outside your organization to gain access to resources. The primary difference is that an extranet is used for vendors, partners and suppliers.

- **Intranet**. An intranet is a private network used by employees or others working for an organization. It is usually available only while directly connected to the organization's network or through a VPN. An intranet is intended for internal use only. Note that people sometimes refer to an intranet as the internal company website instead of the overall internal network.

- **Wireless**. A wireless network is commonly deployed at an organization to facilitate access to the network from smartphones, personally-owned devices, and organizational devices that are not physically plugged into a network. To maximize security, consider the following options:

    - Use the latest security protocols. Wi-Fi Protected Access 2 (WPA2) is widely used and acceptable. It uses Advanced Encryption Standard (AES) encryption. Recently, WPA3 became available and will eventually replace WPA2.

    - Use EAP-TLS to secure authentication.

    - Implement multi-factor authentication for access to the network.

    - Implement a wireless intrusion detection system (WIDS) and a wireless intrusion prevention system (WIPS).

    - Separate wireless usage between employees and visitors/guests.

- **Guest**. A guest network is a separate network used for visitors, guests or other people not directly associated with your organization. It reduces the risk of having your organization's computers exposed to malware because unmanaged devices are not on the same network as guests.

- **Honeypots and honeynets**. A honeypot is a single computer system deployed and configured to attract attackers and keep them there so you can gain information about who they are, where they are, what they are attempting to gain access to and what techniques they are using. A honeypot is specifically configured to look attractive to an attacker (for example, it might appear to be running a vulnerable version of a popular web application). A honeynet can be considered a collection of honeypots but might contain only a single honeypot. A honeynet enables an organization to gain more data than a honeypot because all the network traffic on the honeynet (going in or going out) is considered illegitimate and can be captured for analysis. One benefit of honeynets and honeypots is that attackers become busy with them, taking their attention away from the real networks and resources.

- **NAT**. Network Address Translation (NAT) has two primary purposes — to conserve IP addresses and to mask the source IP addresses of computers. For example, an organization can set up NAT so that all users going to the internet appear to come from a single IP address. Without NAT, all users going to the internet would require their own public IP address, which isn't feasible because of the shortage of public IP addresses.

- **Ad hoc**. An ad hoc network is a temporary network, usually used to temporarily connect computers together. For example, you can connect an old computer to a new computer to facilitate the transfer of data.

### Segregation/ segmentation/ isolation

Be familiar with the pros and cons of the various segmentation types. If a scenario is presented that outlines specific security requirements, you should be able to identify the most appropriate segmentation for the scenario.

- **Physical**. When you physically separate networks, you use independent network hardware such as routers, switches and firewalls. This is considered more secure segmentation than logical or virtual segmentation. In high-security organizations, physical segmentation is often the best choice.

- **Logical (VLAN)**. Logical segmentation, usually by using VLANs, enables you to segment networks by using software logic. Devices are connected to the same switches and use the same routers and firewalls. However, broadcast traffic isn't allowed to pass between VLANs and you can isolate VLANs to mimic physical isolation. Implementing VLANs is easy and fast. VLANs are widely supported, which makes them attractive. They are widely used. Although VLANs are recognized as acceptable for virtually all segmentation requirements, for high-security environments where maximizing security is the most important outcome, you should look at physical segmentation.

- **Virtualization**. As virtualization has expanded, virtualization capabilities have also expanded. Modern virtualization technologies virtualize just about all aspects of the environment, including much of the networking. You can use logical segmentation (often through VLANs) without the use of additional network hardware. Virtualization-based isolation offers a similar security level as logical network segmentation.

- **Air gaps**. An air gapped computer is one that is not connected to the internet or connected to any other devices that are connected to the internet. Air gapped computers or networks offer maximum security for the most sensitive workloads. For example, government networks rely on air gaps for the most sensitive systems. There are downsides to air gaps: They are expensive to implement and maintain because you need to implement dedicated hardware and software to manage them, and simple operational tasks, like installing the latest security patches. become time-consuming tasks.

### Tunneling/VPN

A virtual private network is a secure tunnel connecting two private networks, two private computers or a private computer to a private network. Invented in 1996, VPNs are used by virtually all organizations with a private network to enable workers to work remotely or connect two offices together. As part of a VPN implementation, you should use the strongest authentication method possible, such as EAP-TLS. Additionally, you should use a VPN solution that supports the strongest encryption method available, such as IPsec or an SSL VPN. Avoid the use of Point-to-Point Tunneling Protocol (PPTP) because it is no longer considered secure.

- **Site-to-site.** A site-to-site VPN is one that connects two sites together. For example, you might connect a branch office with the corporate headquarters using a site-to-site VPN.

- **Remote access.** A remote access VPN is one that enables remote workers to connect to an organization's network from anywhere on the internet. Remote access VPNs are useful to enable workers to work from home, a coffee shop or any other place with an internet connection.

### Security device/ technology placement

Many network devices have multiple components, which communicate with the devices to provide features and improve performance.

- **Sensors.** Think of sensors as data gathering agents. They are often software-based but some are hardware-based. Sensors work with the raw data, often sending it to collectors or to the solution itself (such as a SIEM).

- **Collectors.** Collectors are agents that gather data from sensors or other inputs. They often talk to sensors or other input mechanisms. Typically, they do not communicate directly to devices; instead, they rely on sensors or other mechanisms to communicate with devices.

- **Correlation engines.** When you take in large amounts of data from many different sources, it can be tough to understand how the data relates to other data. Correlation engines are applications that try to form relationships between different data, often by using AI and machine learning.

- **Filters**. A filter is a mechanism that reduces the total amount of data you collect or view. A filter is an important component because it can reduce the overall amount of data you ingest or display, which can improve performance or speed up the time it takes you to find what you need. For example, if you captured 10 minutes of network traffic using a protocol analyzer, you could apply a display filter to view only the protocol you want, such as SNMP.

- **Proxies**. A traditional proxy is deployed to the LAN. It waits for web requests from clients and then proxies the requests on the clients' behalf to the internet. Proxies can cache content to enhance performance. A reverse proxy is often deployed to a DMZ. It listens for requests from the internet going to an internal system (such as a website to get your email) and proxies the request to the internal server on the client's behalf.

- **Firewalls**. Historically, when networks were simpler, firewalls were placed at the perimeter or edge of the network. However, in today's complex environments, firewalls are placed at the edge of the network, at the core of the network (to inspect and block some internal communications), and internally (to secure business-to-business connections).

- **VPN concentrators**. VPN concentrators are most commonly located at the perimeter of the network, sometimes directly connected to the internet. This makes sense, because they connect computers from the public internet to your LAN.

- **SSL accelerators**. Like a load balancer (and often the same device), SSL accelerators are typically placed in the LAN for internal servers or in the DMZ for public-facing servers.

- **Load balancers**. Load balancers are placed in front of services or servers. For example, you might have 10 web servers for a website; a load balancer ensures that requests for the website are evenly balanced between all the web servers. If a web server becomes unavailable, the load balancer can detect that through health checks and stop sending traffic to it. Load balancers are most often used in LANs and in DMZs, although generally not shared between a LAN and DMZ.

- **DDoS mitigator**. A DDoS mitigator is sometimes an appliance. It typically sits at the edge of the network, often in front of everything else. This enables you to mitigate DDoS attacks prior to malicious traffic entering your network.

- **Aggregation switches**. Aggregation switches are responsible for connecting other switches together (for example, edge switches). This is sometimes done to simplify network and cable management. Aggregation switches are often found in enterprise networks but rarely found in small networks.

- **Taps and port mirror**. You can use taps or port mirrors to capture network communications on your network. You can put a tap on a switch (for example, directly connected to a specific port on a specific device).

**SDN**

Software-defined networking (SDN) typically resides alongside or integrated with your virtualization infrastructure. It enables you to deploy and manage virtual switches, routers and firewalls virtually, through software.

## 3.3 Given a scenario, implement secure systems design

The section test whether you have the knowledge to implement a secure design of a system, such as a computer or computing device. You might be presented a list of requirements for an implementation and need to know which components and technologies will be needed to meet the requirements of the scenario.

**Hardware/firmware security**

For these topics, the focus is on the hardware layer. For example, you should be familiar with the hardware required to obtain specified outcomes.

- **FDE/SED.** Full disk encryption (FDE) is the act of encrypting an entire hard drive, instead of just the used space of a hard drive or individual files and folders. FDE is better than disk encryption that encrypts only used space or partial portions of the hard drive because it encrypts everything. Self-encrypting drives (SEDs) automatically encrypt and decrypt data. Often used with computers, SED enables you to use encryption seamlessly, without really realizing it. You provide a password upon startup, and the decryption enables you to use the hard drive. If the hard drive is stolen, it becomes worthless without the password to unlock the encryption.

- **TPM**. A trusted platform module (TPM) is a hardware chip, often built into the motherboard of a computer, that is responsible for helping establish a secure boot process, encrypt disk drives, protect passwords and occasionally other functions (such as for enforcing software licensing). TPM can be utilized by other components of the computer, such as the UEFI or operating systems. For example, Windows has BitLocker disk encryption, which can utilize a TPM to enhance the security of the disk encryption.

- **HSM**. A hardware security module (HSM) is a physical device used for cryptographic operations. Often, HSMs are used to sign encryption keys. Commonly, HSMs are used to secure an internal public key infrastructure (PKI). For example, you might generate your root CA certificate from your HSM.

- **UEFI/BIOS**. A UEFI and a BIOS have the same job — to be the middleman between the firmware and operating system during computer startup. The BIOS is a legacy technology because UEFI performs all the same tasks and doesn't have the same limitations. For example, when using a BIOS, you can't have a graphical user interface in the pre-boot environment. Virtually all modern computers use UEFI today.

- **Secure boot and attestation**. With secure boot, a computer has a list of trusted hardware and firmware. Upon boot, the hardware and firmware are checked, along with the digital signatures. If they are compliant, the computer boots. If not, it doesn't.

  **Supply chain**. In a supply chain attack, attackers attempt to secretly alter hardware or software and infiltrate organizations that buy the products. This can sometimes be easier than breaking into systems remotely. As part of your due diligence, it is important to vet suppliers and the entire supply chain. Attacks on the supply chain have been in the news recently. See https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies for details about a recent supply chain attack.

- **Hardware root of trust**. A root of trust is a component that executes first when a computer is turned on. For example, when a smartphone boots up, boot firmware is one of the first components to be engaged. It is a root of trust.

- **EMI/EMP**. Electro-magnetic interference (EMI) and electromagnetic pulse (EMP) weapons are weapons aimed at degrading, damaging or eliminating electrical systems and electronics. They do this by way of a short burst of electromagnetic energy that often overwhelms electronics.

## Operating systems

In this section, operating systems refers to general purpose computer operating systems (such as Windows and Linux) as well as purpose-built operating systems, such as those embedded in an appliance or smartphone.

- **Types.** Be prepared to distinguish between the different characteristics of the operating systems types for the exam.

  - **Network**. A network operating system is synonymous with a server-based operating system. The term is rarely used today because virtually all server operating systems are also network operating systems. A long time ago, a network operating system was a server-based system that provided services to clients on a LAN. Securing a network operating system is like a server operating system; see the next bullet for details.

  - **Server**. A server-based operating system is purpose-built to run services — small applications that provide a service to end users or other software. For example, a server built as an email server would have services to send outbound email, to receive inbound email and scan email for malware. Some server-based operating systems have a graphical user interface but others do not, for added security and

performance. A server is often secured via a centralized policy (such as a Group Policy Object in an Active Directory environment). Other common ways to secure a server include staying up to date on the latest patches, disabling unneeded services, adhering to the principle of least privilege, and monitoring and auditing all activities of the server.

- **Workstation**. A workstation operating system is a client-based operating system meant for people to use on a day-to-day basis at work or at home. A workstation operating system generally has a GUI and is designed to be user friendly and highly compatible with consumer hardware. You can secure workstations by using policies (especially those enforced from a central management point), disabling unnecessary software and functionality, running anti-malware software, and installing operating system updates regularly.

- **Appliance**. An appliance is a specialized hardware device, often running a specialized operating system purpose-built for the appliance. Such operating systems are smaller than a typical server-based operating system, run less services, and offer less features. Because of the reduced functionality, appliances can sometimes be more secure than server operating systems (although the opposite is sometimes true). Securing an appliance requires information from the vendor in additional to internal testing and experimentation.

- **Kiosk**. A kiosk is a purpose-built computer often used in a public space for customers, guests or workers. For example, many airports offer kiosks to enable fliers to check in for flights. Many of the major operating systems offer kiosk versions. Kiosk operating systems are much smaller than a typical computer operating system because the kiosks offer minimal functionality, such as checking in for your flight at the airport or withdrawing money at an ATM. Kiosk operating systems are sometimes embedded into the hardware and can be difficult to upgrade and maintain. Because of this, kiosks can be vulnerable to attack. It is a good practice to keep kiosk computers, especially those made available to the public, on their own segmented network with their own dedicated internet connection.

- **Mobile OS**. A mobile operating system is one built for smartphones; Android and iOS are the two major mobile operating systems today. As smartphones have gotten more powerful, mobile operating systems have too. In many ways, mobile operating systems are like workstation operating systems. As such, they are susceptible to attack, like workstations. It is a good practice to run the latest version of the mobile operating system, run anti-malware software, and uninstall all unnecessary software and services.

- **Patch management**. While we brought up patch management in the operating system section, it also applies across the board to all computing devices — smart phones, routers, switches, wireless access points, smart cameras, etc. Many security experts agree that the single most important security step organizations can take is to consistently install security updates as soon as they are released. As part of your patch management strategy, ensure that you test all updates in non-production environments to ensure they function and don't introduce problems.

- **Disabling unnecessary ports and services**. When we talk about unnecessary ports and services, we are talking about functionality built into an operating system or device but that you are not using and do not intend to use. For example, a server often comes with a file transfer service such as an FTP server (port 20 and 21). If you don't need it, you can disable it or remove it. Workstations often come with a remote desktop sharing service (for example, Remote Desktop Connection which uses port 3389) which you can disable if you don't plan to use it. Disabling unnecessary ports and services reduces the overall footprint of your computer or device, which improves security.

- **Least functionality**. A least functionality system is one that is designed to provide the least functionality required for the scenario. Earlier, we mentioned kiosks at airports — this is a least functionality implementation. With general purpose computers such as workstations, it is difficult to obtain true least functionality. However, aiming for it is a good way to start.

- **Secure configurations**. Secure configurations are configurations that have been deemed secure, either by your organization after testing, by vendors or by trusted third-party advisors. Organizations often standardize operating system installation based on a known secure configuration.

- **Trusted operating system**. A trusted operating system is one that offers enough security and auditing to meet common government requirements. The Common Criteria is an international standard used to classify operating systems as trusted operating systems. Most of the major operating systems today, such as Windows Server 2019 and MacOS 10.14, are considered trusted operating systems.

- **Application whitelisting/blacklisting**. Many operating systems offer application whitelisting (allowing apps to run) and blacklisting (disabling apps from running). It is a good practice to take advantage of these features. You have a couple of options: Disable all apps except those that are whitelisted (most secure but difficult to implement successfully), or enable all apps to run except those that are blacklisted (a common implementation that enables you to block specific apps).

- **Disable default accounts/passwords**. Many appliances and computing devices are built with default accounts and passwords. This enables buyers to quickly configure the devices and use them. However, many people never change the default passwords or default configurations, and some devices can be controlled remotely with the default credentials. A key step to securing devices is to change all default passwords during setup (especially before connecting the devices to the internet) and using special accounts to administer the devices. For example, create a user named Chris to perform administration functions and disable the built-in account if possible.

## Peripherals

An often-forgotten area of security are peripherals. In this section, we will walk through some of the considerations of the most popular peripherals.

- **Wireless keyboards**. Wireless keyboards are sometimes susceptible to radio frequency (RF) signal hijacking. Attackers use a simple tool to intercept communications with the intent of capturing passwords or injecting their own keystrokes, and eventually taking over the computer with malware. While wireless keyboard communication is sometimes encrypted, you should be aware of the attack potential. Bluetooth keyboards, which are more popular than wireless keyboards today, are not currently vulnerable. Note that wireless keyboard signals can travel a few hundred feet. To avoid this attack, use a wired keyboard.

- **Wireless mice**. Wireless mice are also susceptible to RF signal hijacking. Attackers can use automation to take over a computer with a vulnerable wireless mouse. To avoid this attack, use a wired mouse.

- **Displays**. Admins don't often think about displays when it comes to security. But shoulder surfing (the act of secret observing somebody while they go about their computing tasks) is a serious problem that can result in stolen credentials or other issues. To minimize the risk of shoulder surfing, use privacy screens. Privacy screens attach to the display and severely restrict the field of view; people standing off to the side or behind you cannot clearly see the display.

- **WiFi-enabled MicroSD cards**. Late model digital cameras often come with, or take advantage of, MicroSD cards that have WiFi built-in. This enables a photographer to take pictures and have them automatically transferred to another device or a cloud-based storage location. This is convenient because the photographer doesn't have to take out the MicroSD card, insert it into another device and manually copy the pictures. However, some of these cards are susceptible to attack. Known attacks can intercept the communication and gain access to the data. In high-security environments, such as photographing a crime scene, avoid the use of WiFi-enabled MicroSD cards.

- **Printers/MFDs**. Printers and multi-function devices (MFDs, which typically offer printing, scanning and faxing) are sometimes the target of attacks. Attackers attempt to get a copy of all documents printed, scanned or faxed. Because these devices often connect to a corporate network, and sometimes a corporate directory, they are often accessible from anywhere on a corporate network, and sometimes even on the internet. Additionally, these devices often offer a web interface, an FTP server or other connectivity methods. To maximize security, ensure that you keep the firmware up to date and disable unnecessary functionality.

- **External storage devices**. External storage devices are often used for temporary data transfer or for backups. Sometimes, these external storage devices are remotely accessible via a web interface or a file transfer protocol such as FTP. To maximize security, use full disk encryption and disable all remote connectivity to the devices. Rely on local connectivity, such as over USB.

- **Digital cameras**. Digital cameras connect to computing devices using USB or a similar cabled method. Sometimes, they can also connect to devices using WiFI or another cable-less method. Like storage devices, rely on cabled methods to maximize security. Keep your camera firmware up to date, too.

# 3.4 Explain the importance of secure staging deployment concepts

A company's production network must be available 24/7/365 to maximize overall performance, reduce costs and lessen risks. To align with the availability requirements of a production network, you need to use non-production networks to test configuration changes, software upgrades and other changes to the environment. After you validate a change in a non-production environment (or, even better, in multiple non-production environments), you can proceed with the change in your production environment.

## Sandboxing

Think of a sandbox like kids do — a place to play. When kids play in a sandbox, they aren't thinking about anything beyond exploring, experimenting and having fun. In an IT environment, a sandbox is considered the environment where you initially test things. For example, if you are thinking about deploying a major application upgrade to a key app, you might try that in a sandbox first. If you have a brand-new network tool that you are evaluating, you might try it in a sandbox. Sandboxes are nice to have, but when organizations do not have a sandbox, they usually use a development environment for sandboxing and development.

## Environment

Be familiar with the different environments outlined here. You should be able to pick the appropriate environment based on a given scenario. For example, if you wanted to perform a test in an environment that most closely resembled production, which environment would you use? Read on to see the answer.

- **Development**. A development environment is the first environment you use for code development or testing, after a sandbox. While a sandbox is an optional-use environment, a development environment is often a mandatory environment for organizations using a secure software development life cycle (SDLC).
- **Test**. A test environment is used after a development environment. It more closely resembles a production environment than a development environment, but not as close as a staging environment.
- **Staging**. A staging environment is the last environment for testing before a production environment. A staging environment is sometimes referred to as an acceptance test (AT) or universal acceptance test (UAT) environment. This environment most closely resembles production.
- **Production**. The production environment is the live environment. It is what companies rely on to keep the business running, keep customers happy and make money. The environment should never be used for testing or be changed before the changes are tested in non-production environments.

**Secure baseline**

A secure baseline is a template, a configuration, code or an image that the company considers secure. For example, a company might have a secure baseline for their Windows 10 devices. The baseline is used each time the company deploys a new Windows 10 device. The benefits of a secure baseline include having a consistent configuration (all devices start out the same), reducing human error (because a secure baseline is reused repeatedly), and time savings (not having to perform the initial configuration tasks every time a device is deployed). You can apply similar concepts to app configurations and other areas of your environment.

**Integrity measurement**

After a device has been deployed, it tends to drift away from the initial configuration (the secure baseline). The longer a device is active, the more it tends to drift. To ensure compliance with the secure baseline, organizations turn to configuration management solutions. Configuration management solutions can enforce the secure baseline settings. For example, every hour, the configuration management software can check the current configuration against the secure baseline and adjust any settings that don't align. Organizations often combine policies (whether server-based or centralized in Active Directory or a similar directory service) with configuration management. With policies, you can prevent changes to critical system settings.

## 3.5 Explain the security implications of embedded systems

Embedded systems are typically operating environments embedded into the hardware of a specialized device. In such cases, you have limited or no access to the hardware or components. In many cases, the hardware isn't user serviceable. Options tend to be more limited so choosing the right vendor and solution is important.

**SCADA/ICS**

Supervisory Control and Data Acquisition (SCADA) refers to geographically dispersed control systems, such as those that control the distribution of power or water. Industrial Control Systems (ICS) is a broader term referring to automated industrial control systems. ICS is everything related to industrial control systems while SCADA refers to the geographically dispersed control systems that are prevalent in utilities. Because SCADA and ICS are tied into large and critical infrastructure components, security is of the utmost importance. Attackers can take down power grids, cut off water or gas supplies, or otherwise disrupt key utilities.

### Smart devices/IoT

Smart devices and IoT devices are devices that are connected to the internet or a network and that use technology to enhance their functionality. For example, a smart watch can detect that you've been sitting down all day and coax you to stand up and move around. A smart refrigerator can send you an alert when you are low on milk or the water filter needs to be changed.

- **Wearable technology**. Wearable technology encompasses shirts, jackets, backpacks, watches, glasses and other wearables. Often these devices connect to other devices, such as smartphones (for example, via Bluetooth). At a minimum, security implications include the loss of personally identifiable information and health information (smart watches can track heart rate, activity level, sleeping patterns and other types of vitals).

- **Home automation**. The world of home automation is large and continues to grow. There are cameras, security systems, lighting system, audio systems, switches, blinds and entry systems. Virtually all the home automation devices connect to each other, connect to hubs or central control systems, or connect to the internet. In some cases, they connect to all those things! Security implications are varied. A common concern is unauthorized entry to your facility (home or office). For example, imagine connecting an Alexa-enabled device to a garage door or smart deadbolt. You say, "Alexa, open the garage" to open the garage door. Anybody can say that, even from outside your house. Vendors are starting to build in additional security to handle these types of tasks. For example, devices can ask for a PIN before executing a task. Because many of these devices control access or security cameras, there are other security risks, such as burglary or covering up unauthorized access by erasing security footage. Attackers can take over a home automation device and try to use that to take over your computing devices if they share the same network.

### HVAC

Like other devices, HVAC systems have started connecting to wireless networks and to the internet. This enables you to remotely turn on, turn off or otherwise control your HVAC system from anywhere. It's convenient, but it increases the risk that an attacker could maliciously access your HVAC system. While making your home or business too cold or too hot isn't a huge security concern, an attacker could heat up your server room or data center to cause a denial of service as servers shut down due to overheating.

### SoC

For this section, SoC refers to system on a chip, not security operations center. SoC devices are basically tiny computers on a chip, such as a Raspberry Pi (which has a SoC plus other hardware components). Because these are like computers, they are sometimes susceptible to attackers. Implications vary, depending on the use of the device. Common concerns are unauthorized remote access and securing physical access.

### RTOS

A real-time operating system (RTOS) is a system that processes requests in a specific amount of time. A standard operating system, such as Windows 10, processes requests in order and the turnaround time varies; there aren't any guarantees about the amount of processing time a task will take. RTOS systems are typically embedded and response times are important to the functionality of the implementation. Like any operating system, there are security implications — namely, unauthorized access, DoS and escalation of privilege.

### Printers/MFDs

The security implications of printers and multi-function devices are tied to data loss. Imagine everything that everybody printed at your company was secretly sent to a hacker, who then posted the material on the dark web. Or imagine that everything scanned by your employees was secretly sent to your competitor. Those are some of the implications for these devices.

### Camera systems

With camera systems being connected to networks or the internet, you need to think about the pictures and videos from the cameras. Who can access them? What would happen if all the pictures and videos became public? Other security implications are disabling of camera systems or reconfiguration of camera systems (for example, to point to a wall or to stop recording).

### Special purpose

Special purpose devices are those that have limited deployment for specialized use. Typically, you don't find these types of devices in a home or business.

- **Medical devices**. All the devices you see nurses and doctors using around a hospital or medical office qualify as medical devices. For the exam, we are focused on connected devices (wired or wireless). These devices store or transmit sensitive health information and patient information. Security implications are wide ranging, including failure to adhere to regulations such as HIPAA, becoming the target of a class-action lawsuit, being assessed fines and losing business.

- **Vehicles**. As of the last few years, many cars are now connected to the internet. Some cars have artificial intelligence and can drive themselves. Many have automated emergency braking systems. Attackers have displayed proof-of-concept attacks in which they remotely disabled a car or other vehicle or impaired its regular operation. Security implications are related to the safety of passengers and those around them. If an attacker can remotely control a car or disable a car on a high-speed freeway or road system, it is extremely dangerous.

- **Aircraft/UAV**. Severely limiting remote control is an important step for securing an aircraft. However, there are security implications from inside the aircraft, such as interfering with the electronics of the aircraft, which could cause a malfunction or lead to a crash. With unmanned aerial vehicles (UAVs), remote control is a key feature, so securing communications is important. For consumer-based systems, security implications of UAVs include invasion of privacy (for example, a UAV secretly taking pictures of you in your backyard) and loss of data (for example, copying or deleting all the data recorded by the UAV).

# 3.6 Summarize secure application development and deployment concepts

We've talked about the importance of a multi-layered security. Such an approach starts with application development. In the early days of software development, security wasn't a consideration. As the internet grew in popularity, it became clear that security is a key concept. Microsoft introduced Trustworthy Computing in 2002 to embrace security throughout the development lifecycle as well as outside of development.

## Development life-cycle models

- **Waterfall vs. agile**. The waterfall method in the traditional approach to software development: You gather requirements, create a design, develop the code, go through the rounds of testing, fix any issues, and then deliver a final product. The agile method is an iterative approach organized into phases called "sprints." For each sprint, a set of deliverables is defined. A sprint lasts a set period, such as 2 weeks, so progress is delivered regularly. Deliverables are defined by the value they bring to the customer, and high-value ones are delivered earlier in a project. Customers must be more involved in the project compared to the waterfall approach.

## Secure DevOps

While the popularity of DevOps and rapid delivery increased, organizations needed a way to incorporate their security teams into projects earlier. Instead of having a security review at the end of a project, organizations find value in including security team members from the beginning of a project. For security teams to blend seamless with DevOps teams, they need to use automation. With automation, security teams can move fast, like a DevOps team. Combining security with DevOps gets you Secure DevOps, sometimes referred to as DevSecOps.

- **Security automation**. Traditionally, security was a manual set of processes. With DevOps, especially DevSecOps, automation has become very important. Part of enabling automation is embracing a concept known as "infrastructure as code" or "security as code." When security teams can use code to deploy and enforce security, it speeds up the implementation time, enhances consistency and enables security to be built into project from the start.

- **Continuous integration**. Continuous integration is the practice of integrating code into a code repository one or multiple times a day. One of the primary goals of continuous integration is detecting problems quickly and as early in the development as possible.

- **Baselining**. Baselining is a method of comparing what you have to a previously established set of items. You can baseline project requirements, operating system configuration and even code. Baselines are useful for audits and troubleshooting.

- **Immutable systems**. In a traditional server environment, servers are deployed, and then administrators update them, upgrade them and change their configurations. With immutable systems, if changes are required after servers are deployed, new servers that

have those changes are deployed. If an upgrade is needed, new servers with the upgrade are deployed. With immutable systems, all servers or other components are the same. Immutable infrastructure provides consistency and predictability to your infrastructure.

- **Infrastructure as code**. Infrastructure as Code (IaC) is a method to manage your infrastructure (virtualization, servers, network technologies) using code and automation. IaC helps prevent configuration draft, provides consistency in the infrastructure and reduces human error.

## Version control and change management

Version control is a process by which you assign a version number to your application or code. For example, the initial application release might be version 1.0. After fixing the first set of bugs, you might release version 1.01. Minor updates to code are small increments to your version while major updates to code (such as the next release of an app) are large increments to your version (such as going from 1.9 to 2.0). Version control enables you to track changes to your code, along with when those changes were introduced. Change management is the process of managing changes in an environment. Changes in an environment could be related to an application release, a server upgrade or a network configuration change. Organizations use change management to ensure there is proper documentation for planned changes, that there is proper testing of changes ahead of time and that changes take place during known maintenance windows.

## Provisioning and deprovisioning

Provisioning is the process of deploying. Deprovisioning is the process of decommissioning. For example, if you are preparing to deploy a new application to the production environment, you might need to provision 16 web servers, 4 database servers and 4 app servers.

## Secure coding techniques

To maximize the security of your application, you should incorporate the following secure coding techniques:

- **Proper error handling**. One of the key purposes of error handling is to make sure your application stops safely without returning sensitive information, such as information that might lead the attacker to know more about your network, software versions or details of your configuration. It is a good practice to keep error messages generic for end users. For example, you could have an error message saying "Something went wrong. Please try again later."

- **Proper input validation**. Applications often ask for input from users. For example, a web-based application might ask you to provide your email address or to choose an option in a dropdown menu. To maximize security, all input should be validated to ensure it is legitimate. Validation should check for proper length (for example, if you ask for the last 4 digits of a phone number, the input should be 4 digits in length) and proper character type (for example, if you are asking for somebody's last name in English, then the input should only consist of letters in the English alphabet). Without proper input validation, you run the risk of unexpected application behavior that could lead to a security incident.

- **Normalization**. There are a couple of ways to think about normalization. One way is taking input or stored data and standardizing the way it is stored. For example, if you have a database of customer contact information, you might convert "California", "Calif.", "Cali", "S. CA" and "N. CA" to "CA". Similarly, you might convert the phone numbers "213.555.1212" and "213/555-1212" to "213-555-1212." Another way to think about normalization is from a database perspective. It involves a similar goal — standardize how data is stored. With databases, you can also reduce data redundancy.

- **Stored procedures**. Stored procedures are SQL statements (think "database script") used for a variety of purposes. For example, you can find out detailed information about your database, insert data into your database or even back up your database.

- **Code signing**. You can use a certificate to sign code. When you sign code with a digital signature, the author of the code is identified. Additionally, there is a hash of the code which enables others to see whether the code has changed since it was signed. Code signing is a good practice to ensure your code can be validated as legitimate.

- **Encryption**. There are many ways to use encryption with code. You can encrypt your code at rest, and you can use your code to encrypt input or output. To maximize security, you can use encryption to store all sensitive information, such as usernames, passwords, keys, file paths and internal server names. Instead of maintaining sensitive information in plain text inside your code, you can use encryption to store information outside your code and call it within the code.

- **Obfuscation/camouflage**. Code obfuscation, sometimes referred to as code camouflage, is the act of making code difficult to read or understand — for example, you might remove all comments and use random characters for your string names. It was sometimes used to discourage people from stealing or reusing your code. However, this is a form of "security through obscurity," which means that there isn't much value in this method because it doesn't make the code more secure, but instead only makes it take a little bit longer to interpret it. Worse, when other developers at your organization want to build on your code, it makes their job harder.

- **Code reuse/dead code**. Code reuse is a common practice. Code reuse involves reusing code that was already written either as is or as a starting point in a new application. For example, suppose you wrote an application to insert new information into a real estate database and now you are writing an application to add information to an online retailer database; you could reuse the code instead of starting from scratch. Code reuse can help reduce errors and bugs and reduce the total hours required for development. Dead code is code that isn't used. For example, suppose you have an application to upload, download and edit images, but later you opt to remove the option to edit. The editing code still exists but is now considered dead.

- **Server-side vs. client-side execution and validation**. Earlier in this section, we talked a little about input validation. You can perform validation at the client (for example, in a browser) or at the server (for example, back-end code to perform validation). Validating at

the client side has some benefits — for example, you don't send any malformed input to the server. However, one of the downsides is that the client validation could be bypassed; for example, an attacker can use a custom front end to communicate with your application. Validating at the server side also has some benefits — the validation code is at the server level and has additional power and additional infrastructure, especially compared to browser-based validation. Plus, server-side validation is difficult to bypass. It is a good practice to use both types of validation to maximize security.

- **Memory management**. Memory management is the process of optimizing the usage of memory, the allocation of memory to applications and services, and deallocation of memory. Without property memory management and input validation, your app could be susceptible to buffer overflow attacks or other vulnerabilities.

- **Use of third-party libraries and SDKs**. You can use third-party libraries and SDKs to save time and benefit from using code that's already been tested and reviewed. On the downside, your code will depend on the library or SDK, which might lead to lack of support, security issues, or significant updating as libraries or SDKs change.

- **Data exposure**. Data exposure happens when sensitive information is exposed outside of your app or even inside of your app. To reduce data exposure, you should use encryption for all sensitive information, whether the information is at rest (stored on disk) or in transit (such as being transmitted from your app to a database).

## Code quality and testing

As part of your software development lifecycle, you test and validate code. This has a direct impact on the overall code quality. Be familiar with the code quality technologies below.

- **Static code analyzers**. A static code analyzer is a tool to check your code for various issues, such as vulnerabilities. You run a static code analysis prior to releasing your application.

- **Dynamic analysis (e.g., fuzzing)**. Dynamic code analysis checks your code while it executes. You can check for behavioral issues (such as what happens when semi-random information is passed to your app) as well as performance issues.

- **Stress testing**. After you develop code but before you implement it in production, you should use stress testing to ensure that your code remains viable under heavy loads and with sudden ramp-ups in usage or activity.

- **Sandboxing**. Many developers are used to working in DEV, QA and production environments. Sandboxes are isolated non-production environments that are often used to perform isolated testing, especially testing that could be impactful or have unknown impacts. A sandbox is useful because you can't affect any other ongoing development work or the production environment.

- **Model verification**. After developing an application, you should use model verification to prove that the app does what the app's model claims it can do. For example, if your app automates the configuration of a web server, you should run the app to ensure that it configures a web server.

**Compiled vs. runtime code**

Compiled code runs through a compiler to become native code. Many languages are compiled languages, such as C++, C#, and Go. Compiled code is usually be faster than interpreted code. Runtime code is code that is compiled at runtime ("just in time").

## 3.7 Summarize cloud and virtualization concepts

For the exam, you need to be able to differentiate between key cloud concepts and technologies as well as core virtualization components. Specifically, be able to call out the type of deployment, hypervisor or location of a deployment based on a set of requirements.

**Hypervisor**

The hypervisor is a server or appliance that runs virtual machines (VMs). The hypervisor provides the hardware and software foundation for your virtual infrastructure.

- **Type** I. A type I hypervisor runs directly on the underlying hardware, providing virtual machines almost direct hardware access. It is the best performing type and provides for the most scalability. VMware ESXi and Microsoft Hyper-V are two of the leaders in this type of hypervisor.
- **Type II**. A type II hypervisor is a software-based virtualization that runs on top of an operating system, such as Windows or Linux. It doesn't offer as many of the advanced features of a type I hypervisor, doesn't provide as much performance, and doesn't scale. However, it is useful for development and testing scenarios. A type II hypervisor is best suited for individual use, such as by developers or system administrators.
- **Application cells/containers**. Containers are another way to virtualize your application. Instead of running individual virtual machines, you package your app/code and dependencies into a single container. Containers are portable and they share a back-end operating system. You can run multiple containers on a single server and they won't know about each other.

**VM sprawl avoidance**

VMs are easy to deploy, especially with automation. The ease of deployment combined with the speed can sometimes lead to VM sprawl — you have more VMs than you need or even realize you have, and you've lost track of what you have and which VMs are still required or in use.

### VM escape protection

When at attacker gains access to a VM, it is a big deal. But if the attacker can break out of the VM and gain control of the hypervisor, that's a much bigger deal — that's what VM escape is. It is difficult to do, but many have tried. There isn't a single configuration or setting that prevents VM escape. Instead, you need to rely on your multi-layered (defense in depth) security strategy.

### Cloud storage

Cloud storage is like local storage — a bunch of disk drives or SSDs, sometimes connected, that store data. However cloud storage is in the cloud, not on premises, and instead of deploying and managing the storage, you just consume it. Think of it as storage-as-a-service. Benefits include reduced administrative overhead and reduced costs. The downsides are that you lose control of the hardware and much of the configuration; often, you can't choose how the data is stored or how it is encrypted. You give up control.

### Cloud deployment models

When you deploy workloads to the cloud, you have your choice between several models. For some solutions, multiple cloud deployment models are feasible, and you choose based on specific requirements. Other times, only one cloud deployment model is feasible based on your goals. Many organizations, especially large enterprise organizations, use some of each deployment model. In other cases, especially with start-ups, only SaaS is used.

- **SaaS**. Software-as-a-service (SaaS) is a very popular cloud service model. It has been around a very long time, even before people were calling it SaaS and using the term "the cloud."
- **PaaS**. Platform-as-a-service (PaaS) is a complete environment for running your apps. A typical PaaS solution includes servers, storage, networking and other infrastructure and software that you need to have for your application. One common example of PaaS is database-as-a-service solutions, such as Microsoft's Azure SQL Database. They manage the infrastructure; you gain access to SQL.
- **IaaS**. Infrastructure-as-a-service (IaaS) provides the underlying components you need to run your data center in the public cloud. IaaS offers virtualization capabilities, virtual networking, storage and security services. If you only need to run VMs in the cloud, then you only need IaaS.
- **Private**. A private cloud is one that is deployed on premises and intended only for your organization. It often mimics a public cloud with virtualization and automation.
- **Public**. A public cloud is one that is deployed in a provider's environment and is intended to be a multi-customer environment. Resources are shared amongst customers, although customers are segmented from each other. Virtualization and automation provide the key backend foundational technologies in a public cloud.
- **Hybrid**. A hybrid cloud combines one or more private clouds with one or more public clouds. For example, an organization might have their own private cloud build in their environment, and also use some VMs based in a service provider's data center and SaaS solution in the public cloud. In such scenarios, it is common to use solutions that integrate

the clouds as closely as possible. For example, users might authenticate to apps the same way regardless of whether the app is in the company's own private cloud or in the public cloud. Similarly, all audit logs from all sources might be stored in the same location.

- **Community**. A community cloud, a relatively new cloud deployment model, is a cloud built for a specific community, such as the legal industry. The environment is shared amongst multiple customers. Often, community clouds are considered a hybrid form of private clouds built and operated specifically for a targeted group.

**On-premises vs. hosted vs. cloud**

On-premises refers to your own server room, data center or office. Hosted refers to third-party data centers that provide segmented space for customer computing equipment; for example, you can rent a rack to house your servers. A cloud is like a hosted environment, but instead of renting a rack to put your physical servers, you purchase virtualized solutions, such as a database service or an IaaS environment.

**VDI/VDE**

Virtual desktop infrastructure (VDI) refers to virtualized client computers that are hosted on hypervisors and made available to end users. With VDI, you have centralized management and can offer individual VMs to users. Virtual desktop environment (VDE) refers to a virtualized desktop running locally on your client computer. VDI is more scalable and offers remote connectivity to VMs, while VDE is a localized solution, typically for a very specific purpose (such as to use as a development or test environment).

**Cloud access security broker**

A cloud access security broker (CASB) is a security solution that typically is placed between your on-premises environment and your cloud provider's environment. A CASB enforces your organization's security policies in real time.

**Security as a service**

Many organizations deploy a multi-layered security strategy for their environment, deploying anti-malware, auditing, logging, monitoring, security incident response and other services. It requires a lot of time, money and manpower to deploy and maintain all of these services. Security as a service attempts to address the challenge of running your own security environment by offering security services on a subscription basis. A provider deploys, maintains and monitors the security stack while the customer consumes the data and urgent communications from the provider.

# 3.8 Explain how resiliency and automation

When it comes to reducing risk, there are two key strategies that you can use — resiliency and automation. Resiliency involves designing and deploying solutions without a single point of failure (whether it be a server, a firewall or even a data center). Automation is the act of automating tasks that would normally be performed by an administrator or developer. Automation greatly reduces human error because administrators and developers aren't manually making configuration changes.

## Automation/scripting

To automate, you need to use code, scripts, third-party applications or a mix of all three.

- **Automated courses of action**. Suppose that you have a server running a web service and the web service crashes; an administrator is notified by the monitoring system and manually restarts the service. Now imagine that scenario being automated. You have a service restart automatically if it stops or crashes, without human intervention. You can also automated a course of action based on a step-by-step set of tasks (such as deploying a new server) or based on specific events that occur (such as a service crashing).

- **Continuous monitoring**. Continuous monitoring is the act of monitoring your environment 24/7/365. While monitoring by itself normally refers to tools that help you figure out if a server is down or an app isn't working correctly, continuous monitoring is focused on ensuring your configurations adhere to your baselines or requirements — automated processes reset configurations if misconfigurations are detected.

- **Configuration validation**. Configuration validation is a process to look for configuration drift — when a server, service or app no longer matches the initial or desired configuration.

## Templates

Imagine that your organization must deploy 25 web servers a month to support you're a web application that uses a total of 500 web servers. Without a template, you might have to manually configure parts of the server, such as the web service. Using a template saves time and improves consistency, which often leads to better overall security. For example, if your web server uses a configuration file for the configuration, you can use a web server configuration template. Each time you deploy a new server, you configure the web service with the template.

## Master image

A master image is an image of an operating system that has been configured to meet your organization's policies and standards. For example, you might have a server image for web servers that has the latest security updates, the specific configuration needed and the prerequisites installed. A master image speeds up the time to deploy a new server and improves consistency.

### Non-persistence

If when you shut down your computer, all your data remains as-as on your hard drive, you have persistence. If when you shut down your computer, all the contents of your computer's memory are erased, that's non-persistence. With the growth of automation and public cloud, non-persistence has become more important. With non-persistence, you can more easily automate.

- **Snapshots**. A snapshot is a point-in-time backup. You can snapshot a disk. You can snapshot a VM. With many storage area network platforms, you can snapshot a volume, too. Like backups, snapshots can contain sensitive information. Encrypt your snapshots to improve security.
- **Revert to known state**. When you revert to a known state with a computer, you reset the computer configuration back to a specific date and time, such as the date and time of the snapshot or backup.
- **Rollback to known configuration**. When you roll back to a known configuration, you roll back an application to a version which you have documented to have a specific set of features or a configuration.
- **Live boot media**. Imagine you take a DVD and insert it into a computer. It boots up to a non-persistent operating system. You perform tasks. Then, you remove the DVD and restart the computer. That describes the use of live boot media. Live boot media provides a temporary (usually temporary) operating environment that's non-persistent.

### Elasticity

Elasticity is the process of provisioning new resources to meet additional demand, such as adding web servers to provide additional resources during the holidays. Elasticity also involves deprovisioning resources as they are not needed, such as removing the additional servers after the holidays when demand is reduced.

### Scalability

Scalability is like elasticity but deals only with increasing resources, not decreasing them.

### Distributive allocation

Within your environment, you distribute resources. Often this is based on your vendor standards (you might buy servers from a single vendor and you might use one type of operating system, for example). With distributive allocation, you distribute resources in a varied manner in order to reduce your dependency on a single vendor, a single site or a single type of technology. The goal with distribute allocation is to reduce risk — for example, the risk associated with having a single cloud provider whose network suffers a DDoS attack.

**Redundancy**

Redundancy is having multiple components to reduce the impact of a system failure. To ensure redundancy in a server, we would have 2 processors, multiple memory sticks, multiple hard drives working together, at least two power supplies, and at least two NICs. For redundancy to be most effective, it must extend to all the dependent components and systems. For example, imagine that your server has two power supplies but you plug the power cords into the same power strip. Your power redundancy has suffered, although you still have some redundancy in case one of the power supplies fails. Note that you can have redundancy in your components, but it doesn't mean that you have high availability (which is described below). For example, you might have 2 power supplies but only 1 is plugged in.

**Fault tolerance**

Fault tolerance enables a system to continue to function even if a failure occurs in a component. For example, imagine you have 3 hard drives in a RAID 5. One hard drive fails, but the data continues to be accessible. The RAID is in a degraded state but it works. That's fault tolerance. Fault tolerance is typically focused on hardware, not software.

**High availability**

High availability describes an environment where systems continue to be available regardless of what fails or how it fails. High availability is like fault tolerance but focuses on both hardware and software. High availability isn't always instantaneous availability but typically strives to be as close to that as possible.

**RAID**

RAID is the process of taking multiple hard drives and physically or virtually combining them together to improve performance or availability. RAID is classified by types. For example, RAID 1 is a mirror where a minimum of 2 hard drives have identical data, while RAID 5 is a stripe set with a minimum of 3 hard drives, with 1 hard drive used for parity.

## 3.9 Explain the importance of physical security controls

Beyond the importance of hardware, software and configuration security, you should also be familiar with physical security controls. Physical security controls deal with security of your offices, data centers, employees and physical assets.

**Lighting**

Imagine an office building at night. It is dark. Employees have gone home. Without proper lighting, a burglar could sneak around the facility and maybe even break in without anybody (people driving by, security cameras or even security guards) being able to see anything. Lighting is an important security deterrent — burglars generally don't like to be seen and lighting is their enemy. At a minimum, you should use lighting to illuminate entrances, exits and walking paths. For additional security, consider using motion-activated lighting, which lights up brightly when movement is detected nearby.

**Signs**

Signs are useful for securing your facilities. For example, posting "No trespassing" signs on the perimeter of your facility tells people that your facility isn't a place for unauthorized visitors. Posting "Facilities are monitored by security cameras" signs is effective because it warns people that they might be on camera and thus more susceptible to arrest and conviction if they commit a crime.

**Fencing/gate/cage**

While you can walk up to many office buildings, fencing is important for restricted facilities such as a data center. Inside of restricted areas such as a data center or server room, it is a good practice to use additional physical security such as gates (to perform an identity check prior to final entrance) and cages (to segment IT systems). In an environment shared among customers, cages are often used to segment customer equipment.

**Security guards**

Security guards are effective at safeguarding your facility. They can see and hear things that security cameras can't always see or hear (outside the camera's view, for example). They can evaluate a situation based on their experience and take quick action (for example, see a person in a ski mask and call the police). They can also serve as a deterrent. If your building has a security guard but the building down the street doesn't, a burglar might choose the latter building.

**Alarms**

Upon unauthorized entry, an alarm can automatically contact the police, turn on a loud siren or both. An alarm is an effective physical security control because seeing it often scares off burglars from even attempting to break into your facility. If they decide to break in, the alarm siren would likely scare them off and can even alert police, who can catch the burglar.

**Safe**

A safe is a locked and armored vault, typically small enough to carry but sometimes large enough to walk into. Safes are used to store the most valuable or irreplaceable objects. For example, you might store money or a master key in a safe. Safes are often effective against fires, floods and burglars.

**Secure cabinets/ enclosures**

Sometimes, you need to lightly secure items. For example, you might want to lock up some project documents at night. Secure cabinets or enclosures are useful for lightly securing items. Generally, they keep out casual observers or curious neighbors. However, they are not very secure because they can be pried open with common tools. Therefore, they should be used only with items that are not critically important or sensitive.

**Protected distribution/ Protected cabling**

Sometimes, you need to lightly secure items. For example, you might want to lock up some project documents at night. Secure cabinets or enclosures are useful for lightly securing items. Generally, they keep out casual observers or curious neighbors. However, they are not very secure because they can be pried open with common tools. Therefore, they should be used only with items that are not critically important or sensitive.

**Airgap**

An airgap is a physical segmentation of a computer or network from the internet or another insecure network. For example, you might have a sensitive server connected to a LAN and the LAN is not connected to any device or network that has access to the internet. Thus, the computer cannot be connected to from the internet. An airgap greatly increases the security of a computer or a network. However, as seen in the news recently, compromises are still possible using USB sticks or other offline methods.

**Mantrap**

Mantraps are physical contraptions that minimize or prevent tailgating. For example, you might see a secure turnstile at a stadium or other event; it allows only a single person to enter at a time.

**Faraday cage**

A Faraday cage is an enclosure that blocks electromagnetic fields. For example, your smartphone cannot be contacted when it is stored in a Faraday cage. Faraday cages are often used to protect delicate electronic equipment, such as equipment seized as evidence in a criminal case.

**Lock types**

There are many types of locks, each with strengths and weaknesses. For example, most people are familiar with deadbolts or knob locks, both of which are in most homes, often on the front door. Other types of locks are mortise locks, often found in commercial buildings, and cam locks, often found in cabinets. Some organizations opt to use cable locks for physically locking computers to desks, which makes them harder to steal.

**Biometrics**

Biometrics is a type of identification system that relies on measuring a person's physical characteristics, such as their retinas, face and voice. Biometrics are sometimes used for primary authentication, such as unlocking your computer or smartphone. Other times, biometrics are used for a second authentication factor — for instance, when you go to a restricted facility, you might have to swipe a badge to enter the property and then use a hand scan to gain access into other areas of the facility. Biometrics enhance security, especially compared to passwords.

**Barricades/bollards**

Barricades are walls used to block access. Sometimes, they are short, such as to block access to cars. Other times, they are tall, such as to block access to people. Barricades are often used temporarily, such as during an environmental disaster or a riot. Bollards are poles that are installed into the ground and stick up out of the ground enough to provide a barricade. Often, they are installed to surround important infrastructure, such as a backup generator. Other times, they are used for safety, such as to keep cars away from pedestrian walkways.

**Tokens/cards**

Tokens and cards are often small (wallet-sized or smaller) cards that employees use to gain access to buildings, parking garages and other facilities. Token and card readers are often placed at entry points (such as doors) to electronically read cards, validate the cards with a back-end computer and unlock doors when a valid card is presented.

**Environmental controls**

Environment controls provide temperature control and environmental protection for your facilities.

- **HVAC**. Heating, ventilation and air conditioning (HVAC) control the temperature of your facilities. While keeping people comfortable in an office is important, HVAC is critical for data center operations because computer equipment often becomes unstable or unable to run when temperatures get too hot.
- **Hot and cold aisles**. In a data center, maintaining the proper temperature is critical to ensure equipment keeps running. One common technique is to designate hot and cold rows. In such a scenario, servers and equipment face each (for example, servers in row 1 face servers in the row straight across). Hot air comes out of the back of each row but does not go into the intake of other equipment. Based on this setup, every other row is a cold (intake) row and every other row is a hot (exhaust) row.
- **Fire suppression**. Fire suppression refers to technologies that reduce the spread of a fire (such as fire doors) or help put out a fire (such as fire extinguishers). There are many types of fire suppression, such as sprinkler systems (often used in office environments but not ideal for data centers) and carbon dioxide fire suppression (or other clean agent fire suppression, which are ideal for data centers).

**Cable locks**

Cable locks are locks used to secure individual assets, such as computers, bikes, cameras or other small equipment. These locks often prevent casual thieves but are not usually secure enough to discourage professional thieves.

**Screen filters**

A screen filter is a monitor/screen overlay that drastically reduces the field of view of the monitor or screen. When you put a screen filter on a computer monitor, it makes it difficult for people walking by or casually looking over your shoulder to see the screen. A person has to stand directly behind you at the right angle to see the screen, and that makes it difficult for anybody to do that without notice. Screen filters are often used by executives or other people who routinely work with sensitive data, such as salary spreadsheets or employee performance reports.

**Cameras**

When you use cameras to capture activity around your facility, you gain the benefit of being able to replay the activities later, potentially helping to track down responsible people in an incident. Additionally, you ward off potential intruders — the sight of the cameras is often enough to persuade the bad guys to move onto a less secure facility. Cameras are an important part of your multi-layered physical security strategy.

**Motion detection**

Motion detection has historically been tied to alarm systems such as burglar alarms. You set the alarm when you leave the facility and any motion detected thereafter is considered malicious and an alarm goes off. Motion detection has expanded to other uses too, including the use in security cameras that start recording when motion is detected, lights that turn on when motion is detected, and automation that closes a door or gate 5 seconds after the last motion is detected.

**Logs**

With physical security, logs are tied to all your physical security solutions, such as badge readers, biometrics readers and visitor logs used to manually sign into a facility. Logs are important because they can help you investigate an incident. For example, you can find out which parking garage an employee used, which door they entered, the time they entered and all the doors they opened thereafter. You can correlate that information from information from cameras to form a complete picture.

**Infrared detection**

Late-model cameras can record in almost complete darkness using infrared detection technology. Using infrared radiation, detection is possible through heat signatures. In low lighting conditions, infrared cameras are important. Otherwise, you can invest in proper lighting to minimize the need for infrared detection.

**Key management**

With physical security, key management is the process of managing keys. Often, we're talking about physical keys, such as building keys or master keys. But key management also extends to digital keys. To maximize security, you should have a formal process for managing keys, especially sensitive keys such as a master key that can open all the doors at your facility. Like digital security, you should adhere to the principle of least privilege with keys. An air conditioning repairman assigned to repair the HVAC system in Building 2 should get only a key to Building 2. Master keys should be stored somewhere safe, such as a safe or safety deposit box.

# 4. Identity and Access Management

This section is focused on the concepts related to granting and revoking privileges for the purpose of data access or to perform actions on systems. There are 4 sections in Identity and Access Management.

## 4.1 Compare and contrast identity and access management concepts

Controlling access to assets is one of the paramount themes of security. You will discover a variety of different security controls work together to provide access control. An asset can be information, systems, devices, facilities or personnel.

### Identification, authentication, authorization and accounting (AAA)

- **Identification**. Identification is the process of someone claiming to be a particular identity. The subject must provide an identity to a system to begin the authentication, authorization and accounting processes. For example, the subject might type a username, swipe a smartcard or provide a device token. A core principle is that all subjects must have unique identities.

- **Authentication**. Authentication verifies the identity of the subject by comparing one or more factors against a database of valid identities (e.g., user accounts). Another core principle is that the information used to verify the identity is private information and shouldbe protected. For example, instead of storing passwords in clear text, authentication systems store hashes of passwords in the authentication database.

  Identification and authentication always occur together as a single two-step process — providing an identity is the first step, and verifying the identity (authentication) is the second step. Without completing both steps, a subject cannot gain access to an asset.

- **Authorization**. Authorization indicates who is trusted to perform specific operations — subjects are granted access to objects based on proven identities. For example, administrators grant a user access to files based on the user's proven identity. If the action is allowed, the subject is authorized; if it is not allowed, the subject is not authorized.

  Identification and authentication are "all-or-nothing" aspects of access management; either a user's credentials prove a claimed identity, or they do not. In contrast, authorization includes a wide range of variations. For example, a user may be able to read a file but not delete the file, or a user may be able to create a new document but not alter other users' documents.

- **Accounting**. Accounting includes auditing, logging, and monitoring, which provide accountability by ensuring that subjects can be held accountable for their actions. For example, when auditing is enabled, it can record when a subject reads, modifies or deletes a file.

  While accounting relies on effective identification and authentication, it does not require effective authorization. In other words, once subjects are identified and authenticated, accounting mechanisms can track their activity even when they try to access resources that they aren't authorized for.

## Multifactor authentication

The basic methods of authentication are also as factors. Multifactor authentication includes two or more of the following factors:

- **Something you are**. This includes a physical characteristic of an individual with different types of biometrics. Examples include fingerprints, voice prints, retina patterns, iris patterns, face shapes, palm topology and hand geometry.
- **Something you have**. This includes the physical devices that a user possesses. Examples include a smartcard, hardware token, memory card or USB drive.
- **Something you know**. This could be a password, personal identification number (PIN) or passphrase, for instance.
- **Somewhere you are**. This includes an individual's location based on a specific computer, a geographic location (based on an IP address) or a phone number (based on caller ID).
- **Something you do**. This includes an actionable characteristic of an individual. Examples are signature and keystroke dynamics.

## Federation

A federation is composed of distinct networks from different organizations. In a federation, the intention is for these organizations to share resources and/or data while still using their existing credentials. For example, imagine Company1 wants to closely collaborate with Company2 by sharing calendar information. Company1 can federate with Company2. Users in Company1 can view the calendar information of users in Company2 using their Company1 credentials. Users in Company2 can view calendar information in Company1 using their Company2 credentials. Federations make for seamless sharing as well as connecting organizations to public cloud services.

**Single sign-on**

Single sign-on (SSO) uses federated identities to provide a more seamless experience for users when accessing resources. However, instead of a user attribute, the hosted provider would match the user's internal login ID with a federated identity. For example, suppose employees log on within the organization using their corporate login ID. When a user accesses the online services, the federated identity management system uses their login ID to retrieve the matching federated identity.

**Transitive trust**

Transitive trust is the concept that if A trusts B and B trusts C, then A inherits the trust of C. Transitive trust is a serious security concern because it might enable bypassing of restrictions or limitations between A and C, especially if A and C both trust B. An example of this would be when a user (A) requests data from B and then B requests the data from C, the data that users receive is essentially from C — a transitive trust exploitation.

## 4.2 Given a scenario, install and configure identity and access services

In this section, you will be given an opportunity to choose an appropriate identity and access service and how it should be configured based on a list of requirements.

**LDAP**

Many organizations use a centralized directory stored in a database that stores information about users and other objects and is typically used as an access control system. One example of this is based on the Lightweight Directory Access Protocol (LDAP). For example, Microsoft Active Directory Domain Services (AD DS) is LDAP-based.

The LDAP directory is similar to a telephone directory for network services and assets. Users, clients and processes can search the directory service to find a desired system or resource. Users must authenticate to the directory service before performing queries and lookup activities.

**Kerberos**

Kerberos uses a ticket system for authentication. It offers a single sign-on solution for users and provides protection for logon credentials. Kerberos provides confidentiality and integrity for authentication traffic using end-to-end security and helps protect against eavesdropping and replay attacks. The current version, Kerberos 5, relies on symmetric-key cryptography (also known as secret-key cryptography) using the Advanced Encryption Standard (AES) symmetric encryption protocol.

**TACACS+**

Terminal Access Controller Access-Control System (TACACS) was introduced as an alternative to RADIUS (described below). TACACS Plus (TACACS+) was later created as an open, publicly documented protocol. TACACS+ provides several improvements over RADIUS by separating authentication, authorization and accounting into separate processes. In addition, TACACS+ encrypts all of the authentication information, not just the password as RADIUS does.

**CHAP**

This is one of the authentication protocols used over Point-to-Point Protocol (PPP) links. Challenge Handshake Authentication Protocol (CHAP) encrypts usernames and passwords and performs authentication using a challenge-response dialogue that cannot be replayed. CHAP also periodically re-authenticates the remote system throughout an established communication session to verify a persistent identity of the remote client. This activity is transparent to the user.

**PAP**

This is another standardized authentication protocol for PPP. Password Authentication Protocol (PAP) transmits usernames and passwords in clear text. It offers no form of encryption, but simply provides a method to transport the logon credentials from the client to the authentication server.

**MS-CHAP**

MS-CHAP is the Microsoft version of the CHAP protocol and exists in two versions, MS-CHAPv1 and MS-CHAPv2. Some of the differences between CHAP and MS-CHAP are that MS-CHAP provides an authenticator-controlled password change mechanism and an authenticator-controlled authentication retry mechanism. In addition, MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet. There are known weaknesses with MS-CHAP, including the use of DES to encrypt the NTLM password hash, which opens the door for custom hardware attacks utilizing brute-force attacks.

**RADIUS**

Remote Authentication Dial-in User Service (RADIUS) centralizes authentication for remote connections. It is typically used when an organization has more than one remote access server. A user can connect to any network access server, which then passes the user's credentials on to the RADIUS server for authentication, authorization and accounting. While RADIUS encrypts the exchange of the password, it doesn't encrypt the entire session. Additional protocols can be used to encrypt the data session.

**SAML**

Security Assertion Markup Language (SAML) is an XML-based language that is commonly used to exchange authentication and authorization information between federated organizations. It is commonly used to provide SSO for users accessing internet resources.

**OpenID Connect**

OpenID Connect is an authentication layer that uses the OAuth 2.0 framework. It provides decentralized authentication, allowing users to log in to multiple unrelated websites with one set of credentials maintained by a third-party service, which is referred to as the OpenID provider.

**OAuth**

OAuth (which implies open authentication) is an open standard used for access delegation. The latest version of this framework is OAuth 2.0; it is supported by many online service providers.

**Shibboleth**

Shibboleth is a free and open standard software package that is used for SSO and federation between and within organizations. The software is owned and managed by the international Shibboleth Consortium.

**Secure token**

A security token is a physical device used for authentication, either in addition to or in place of a password. Examples of a secure token include a wireless keycard or USB device. Some tokens store cryptographic keys (such as a digital signature), biometric data (such as fingerprint details) or passwords.

**NTLM**

NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity and confidentiality to users. The NTLM protocol suite is implemented in a Security Support Provider, which combines the LAN Manager Authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols into a single package.

## 4.3 Given a scenario, implement identity and access management controls

After authentication, the next step is authorization. The method of authorizing users to access resources depends on the access control method.

**Access control models**

Access control models define how users gain access to resources. There are several models, each with its own methods of providing access. Here are the five most popular access control models:

- **MAC**. The Mandatory Access Control (MAC) model uses labels that are applied to both users and objects. For example, a user who has the label "top secret" can be granted access to a document that has the label "top secret". In this example, the subject and the object have matching labels.

- **DAC**. The Discretionary Access Control (DAC) model uses an access control list (ACL) that is applied to objects. The ACL defines the owner for the object, and the owner can grant or deny access to any other users. The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model.

- **ABAC**. The Attribute Based Access Control (ABAC) model uses rules that can include multiple attributes about users and objects. This allows the model to be flexible, as it applies the rules to all users and objects equally. The rules within a policy can use plain language statements such as "Allow shop floor workers to access the WAN using a corporate mobile device."

- **Role-based access control**. The role-based access control (RBAC) model uses roles or groups, which are typically identified by job functions. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. If a user account is in a role, the user has all the privileges assigned to that role.

- **Rule-based access control**. The rule-based access control model applies global rules that apply to all subjects. For example, a firewall uses rules that allow or block traffic to all users equally. Rules within the rule-based access control model are sometimes referred to as restrictions or filters.

### Physical access control

Physical controls are considered something you have; they are the first line of defense when providing adequate security.

- **Proximity cards**. Proximity cards are worn or held by an authorized bearer. When they pass a proximity reader, the reader is able to determine who the bearer is and whether they have authorized access.

- **Smart cards**. Smart cards are credit-card-sized IDs, badges or security passes with an embedded magnetic strip, bar code or integrated circuit chip. They contain information about the authorized bearer that can be used for identification and/or authentication purposes. Some smartcards can even process information or store reasonable amounts of data in a memory chip.

## Biometric factors

Another common authentication and identification technique is the use of biometrics, which are methods for the something you are authentication factor.

- **Fingerprint scanner**. Fingerprints are the visible patterns on the fingers and thumbs of people. They are unique to an individual and have been used for decades in physical security for identification. Fingerprint scanners are now commonly used on laptop computers and USB flash drives for identification and authentication.

- **Retinal scanner**. Retinal scanners focus on the pattern of blood vessels at the back of people's eye. They are the most accurate form of biometric authentication and can differentiate between identical twins. Retinal scanners typically require users to be as close as three inches from the scanner.

- **Iris scanner**. Iris scanners focus on the colored area around the pupil and are the second most accurate form of biometric authentication. Like the retina, the iris remains relatively unchanged throughout a person's life. Iris scans are considered more acceptable by general users than retina scans typically because scans can occur from farther away — 20 to 40 feet.

- **Voice recognition**. This type of biometric authentication relies on the characteristics of a person's speaking voice, known as a voiceprint. The user speaks a specific phrase, which is recorded by the authentication system. To authenticate, they repeat the same phrase, which is compared to the original recording. Voice pattern recognition is sometimes used as an additional authentication mechanism but is rarely used by itself.

- **Facial recognition**. Facial recognition scanners use the geometric patterns of people's faces for detection and recognition. For example, the authentication system might use a one or more pictures of you combined with your name. Face scans are also used to identify and authenticate people before they are permitted to access secure spaces, such as a secure vault.

## False acceptance rate

A false acceptance occurs when an invalid user is authenticated; it is –also known as a false positive authentication. For example, the authentication system successfully authenticates an intruder using an invalid account or a fingerprint that is not registered. The ratio of false positives to valid authentications is the false acceptance rate (FAR).

## False rejection rate

A false rejection occurs when a valid user is not authenticated. For example, an authentication system might incorrectly reject the fingerprint of a valid user with a registered fingerprint. This is sometimes called a false negative authentication. The ratio of false rejections to valid authentications is the false rejection rate (FRR).

### Crossover error rate

You can use the crossover error rate (CER), also known as the equal error rate (ERR), to compare the overall quality of biometric devices. The point where the FRR and FAR percentages are equal is the CER, and the CER is used as a standard assessment value to compare the accuracy of different biometric devices. Devices with lower CERs are more accurate than devices with higher CERs.

### Tokens

A token is a password-generating device that display a number for authentication. At any point in time, the authentication server and the token will have the same number for each user. Tokens are typically combined with another authentication mechanism. For example, users might enter a username and password and then enter the number displayed on the token — this is an example of multifactor authentication.

- **Hardware**. Hardware token devices use dynamic one-time passwords, making them more secure than static passwords, which remain the same over a long period of time. A dynamic password is frequently changed. A dynamic onetime password is used only once and is no longer valid after it has been used.

- **Software**. Some organizations use a PIN displayed from a software application running on the user's device. For example, an authentication server might periodically send a new six-digit PIN to a mobile app.

- **HOTP/TOTP**. A trend that many online organizations are using is two-step authentication. For example, when you log on to a bank website, the authentication system sends a code via a text message to your mobile phone. You successfully authenticate after entering the code on the bank website. This process typically uses one of the following standards, and many online organizations use a combination of both:

  - **HOTP**. The hash message authentication code (HMAC) includes a hash function used by the HMAC-based One-Time Password (HOTP) standard to create one-time passwords. It typically creates six- to eight-digit numbers. The HOTP value remains valid until used.

  - **TOTP**. The Time-based One-Time Password standard is similar to HOTP but it uses a timestamp and remains valid only for a specific timeframe. The TOTP password expires if the user doesn't use the code within the timeframe.

### Certificate-based authentication

For certificate-based authentication, certificates are issued to the user or device and presented when accessing resources.

- **CAC/PIV**. Common Access Cards (CACs) or Personal Identity Verification (PIV) cards are smart cards that include pictures and other identifying information about the bearer. Users often wear them as badges for physical security and insert them in to smart card readers to access digital resources.

- **Smart card**. Smart cards contain information about a user for the purposes of identification and/or authentication. However, they aren't effective identification methods by themselves because they can be easily lost or stolen. Most organizations require users to authenticate using another method, such as a PIN or a username and password. Most current smart cards include a microprocessor and one or more certificates. The certificates can be used for asymmetric cryptography, such as encrypting data or digitally signing email.

- **IEEE 802.1x**. IEEE 802.1x provides a framework for authentication and key management in wired and wireless networks. In this scenario, software on the client communicates with the authentication server. After successful authentication, the network switch or the wireless access point allows the client to access the network.

### File system security

The methods for securing data on data storage systems depend on the file system and the type of media. Using the principle of least privilege, administrators can restrict access to data in supported file systems to minimize both accidental and intentional data loss or corruption. For example, Windows operating systems use the NTFS file system to restrict users' access to data using permissions like read, change, etc., while Linux operating systems use other file systems that provide similar functionality. To secure data on storage devices that lack a file system that supports restricting access, administrators can deploy encryption. For example, Windows operating systems can use BitLocker to Go to secure data from unauthorized access.

### Database security

Database security can use a wide range of security controls to protect databases against compromises of confidentiality, integrity and availability. These controls can be used to protect the data, the database applications or stored functions, the database systems, the database servers and the associated network links. The controls can include technical, administrative and physical controls. For example, technical controls might be a database firewall, database encryption, and auditing or monitoring of database permissions.

## 4.4 Given a scenario, differentiate common account management practices

While there are various methods for managing accounts, it's critical for an organization to understand and implement the appropriate user account and account security management practices.

## Account types

- **User account.** A user account, also referred to as a named account, is an account associated with one individual for the purposes of accessing resources. Frequently, the account will have limited access to the resources (for example, the user can read only certain files and delete only some of them).

- **Shared and generic accounts/credentials**. A shared, or generic, account is an account that is typically shared by more than one individual for the purposes of accessing resources. While the account has limited access to resources, it is challenging for organizations to know who used the account on a given occasion.

- **Guest account**. A guest account is similar to a shared account but it is typically enabled on demand for occasional or one time use. Frequently, guest accounts have blank passwords and provide users with anonymous access. Since this can be a security risk, it is a best practice to leave guest accounts disabled until they are required.

- **Service account**. A service account is an account that is specifically used by a service instead of an individual (e.g., software that needs access to resources). Since service accounts typically have a higher level of privileges than user accounts, they are often configured with strong, complex passwords. However, it is common to configure service accounts to not require password expiration.

- **Privileged account**. A privileged account is an account that has a higher level of privileges than user accounts to resources. Granting a user administrative privileges requires approval by appropriate personnel within the organization.

## General Concepts

- **Least privilege**. The principle of least privilege ensures that users are granted only the privileges they need to perform their role within the organization.

- **Onboarding**. Onboarding is the process of adding new users to the identity management system of an organization. The onboarding process is also used when a user's job role or position changes or when the individual is granted additional levels of privilege or access.

- **Offboarding**. Offboarding is the removal of a user's identity from the identity management system once the individual has left the organization. This can include disabling and/or deleting the user account, revoking certificates, and terminating other specifically granted privileges. It can also include informing physical access management personnel to not allow the individual to enter the building in the future.

- **Permissions auditing and review**. Permissions auditing and review is the process of ensuring that only eligible users have access to the resources within an organization. As part of the process, the organization will determine whether each user's privileges to resources align with the user's role within the organization. During the audit, the organization will assess the effectiveness of its access controls and ensure that accounts are managed appropriately.

- **Usage auditing and review**. Usage auditing and review is the process of recording the actions users perform on resources within an organization. As part of the process, the organization will determine whether each user's actions align with the user's privileges and roles within the organization.

- **Time-of-day restrictions**. Organizations might choose to restrict a user's access to resources to specific times in a day as well as days of the week. For example, to minimize security vulnerabilities, an organization could implement a policy that restricts a user's access to resources to business hours only. As a result, the user will not have access to resources during non-business hours.

- **Recertification**. Recertification is the process of renewing a certification and accreditation after changes are made to the original certification process or after a specific time period. An organization's security policy should specify the conditions that require recertification.

- **Standard naming convention**. A standard naming convention is an agreed-upon convention for naming resources. The convention might be based on location, purpose or relationship and should ensure the name is unique within an organization.

- **Account maintenance**. Most organizations need a method for maintaining accounts, for example, to reset passwords, enable/disable accounts or update specific attributes. This function is typically provided by a front-line support (or help desk) team that users can contact for assistance. Although an organization might dedicate a team for account maintenance, a different team or process would typically be used for account provisioning and deprovisioning.

- **Group-based access control**. Organizations might choose to grant access to resources based on user's membership in a group. This method simplifies administrative overhead but can weaken security if user permissions are not audited and reviewed periodically.

- **Location-based policies**. Organizations might choose to restrict user's access to resources based on the physical location or region of the user. For example, to minimize security vulnerabilities, an organization in a specific region might implement a policy that restricts a user's access to resources unless the user is in the same region. As a result, users outside of the region will not have access to resources.

## Account policy enforcement

- **Credential management.** In systems that use a hashing algorithm such as Secure Hash Algorithm 3 (SHA-3), passwords are typically stored as a hash; they are rarely stored as plain text. In fact, these systems do not store the password — when a user authenticates, the system hashes the provided password, compares it to the stored password hash and authenticating the user only if the hashes match.

- **Group policy**. Organizations might implement multiple password policies for users. The policies might apply to different groups of users or apply overlapping policies to various groups of users within the organization.

- **Password complexity**. The complexity of a password refers to how many character types are included in the password. An organization can even implement a password policy that requires a minimum number of each character type (uppercase characters, lowercase characters, numbers and special characters or symbols).

- **Expiration**. Password expiration is the maximum time a user's password remains valid. An organization can implement a password policy for password expiration by defining the maximum password age. For example, an organization might require users to change their password after 90 days. As a result, each user will be required to reset their password before they can access resources on the 91st day.

- **Recovery**. Organizations might provide a process by which users can regain access to an account to which they no longer have access. For example, a self-service password reset process enables users to recover access to their account by answering one or more security questions. Only the authorized user would know with the correct answers, which they provided when the account was provisioned.

- **Disablement**. You can disable an account completely, which renders it unusable, even with the correct password. Disablement is often used when an employee leaves a company. After a specific amount of time, disabled user accounts are deleted. On some systems, user accounts are also disabled after a specific number of invalid password entries or authentication attempts.

- **Lockout**. An organization can implement a password policy to lock out an account after an incorrect password is entered a predefined number of times. Typically, this number is set high enough to allow for some user errors.

- **Password history**. The password history is the list of a user's previous passwords. Typically, authentication systems will remember many of the passwords each user has used.

- **Password reuse**. An organization can implement a password policy that prevents users from reusing passwords on their password history list. To prevent users from getting around the policy by changing their password repeatedly until a previously used password is bumped off the password history and therefore can be used again, an organization can combine a password reuse restriction with a minimum password age setting. For example, an organization might choose to set the minimum password age to one day so that users can reset their passwords only once a day.

- **Password length**. The password length is the number of characters in a user's password. Longer passwords are harder to crack than shorter passwords. Many organizations require the passwords for privileged accounts to be longer than those for user accounts.

# 5. Risk Management

Risk management is how an organization manages the likelihood of an event and the impact of the event on the organization. Because every organization will assume some level or risk, this typically involves organizations developing and implementing processes, policies and procedures.

## 5.1 Explain the importance of policies, plans and procedures related to organizational security

This topic is a high-level design/architecture topic. You should be comfortable explaining the concepts and knowing how they can help an organization's security.

### Standard operating procedure

A standard operating procedure (SOP) is the specific actions required to implement a specific security mechanism, control, or solution within an organization. SOPs should be documented in detail. In most scenarios, the procedures are system- and software-specific, so they must be updated as the hardware and software evolve. Procedures help ensure standardization of security across all systems; if they are followed correctly, then all activities should be in compliance with policies, standards and guidelines.

### Agreement types

An agreement is an arrangement between two parties. For example, an agreement constitutes an arrangement between two organizations or between IT and other departments.

- **BPA**. A business partnership agreement (BPA) is a document used by business partnerships to define all the terms and conditions of the business relationship. Typically, this agreement includes the goals and duration of the partnership, contribution amounts, accounting obligations, distribution of profits, process for adding or removing partners, and the terms and conditions of termination of the partnership.

- **SLA**. A service-level agreement (SLA) is a detailed document that describesdescribe the vendor, consultant and contractor controls that are used to define the expected levels of performance, compensation and consequences. Some of the common components in SLAs include system uptime, maximum downtime, peak load, average load, responsibility for diagnostics and failover time, as well as the financial and other contractual remedies if the agreement is violated.

- **MOU/MOA**. A memorandum of understanding (MOU), or memorandum of agreement (MOA), is a general document that defines the intention of two entities to collaboratively work together toward a common goal. An MOU is the first step of mutual understanding between two parties and will include general points, while an MOA is the next step when two parties define more details for beginning an agreement.

- **ISA**. An interconnection security agreement (ISA) is similar to a MOU/MOA except it is more formal and includes monetary penalties if one of the parties does not meet its obligations. For example, if two parties plan to transmit sensitive data, they can use an ISA to specify the technical requirements of the connection, such as how the two parties establish, maintain and disconnect the connection. It might also specify the minimum encryption methods used to secure the data.

## Personnel management

The act of managing your employees and contractors is referred to as "personnel management". Personnel management often deals with the process of hiring new people, terminating existing workers and maintaining good relations with current employees.

- **Mandatory vacations**. Some organizations have a policy that requires employees in sensitive positions to take mandatory vacations of five or ten consecutive business days. Common in the finance industry, these policies help deter fraud because of the knowledge that another person will be performing an employee's duties and examining their work. In addition, some complex embezzlement and fraud schemes require the employee to take steps daily to cover up the crimes. It is common for organizations to also schedule audits to coincide with mandatory vacations to increase the likelihood of discovering fraud and other crimes.

- **Job rotation**. Job rotation is a policy that compels employees to rotate into different jobs, or at least rotate some of their duties. This practice can deter fraud (such as sabotage) and prevent information misuse as well. Like mandatory vacations, job rotation makes it more difficult for an employee to cover their tracks, since someone else will be performing their duties. In addition, job rotation can also discover innocent mistakes as another employee transitions into the role.

- **Separation of duties**. Separation of duties separates the tasks and associated privileges for specific security processes among multiple individuals within the company. This process is commonly used in financial accounting systems, whereby there are separate roles for receiving checks, depositing cash and reconciling bank statements, and approving write-offs. The same benefits exist in information security, whereby there are separate roles for management access to firewalls, servers, accounts, etc. It is imperative that an organization implement a security policy so that no individual acting alone can compromise security controls.

- **Clean desk**. Some organizations require a desk to be free of paperwork or other material that might contain sensitive or internal information. A clean desk policy ensures that employees are cognizant of items being left out on their desk. This prevents malicious individuals from walking around the office and stumbling across sensitive information.

- **Background checks**. Background checks are used to identify an individual's previous activities. Most background checks are conducted prior to employment and can include an individual's criminal, financial or driving records. While there are exceptions to the rule, past behavior is a fairly reliable indicator of how people might perform today.

- **Exit interviews**. Exit interviews are conducted when an employee retires, resigns or is dismissed from the company. Not only does this interview allow the company to retrieve assets, it enables management to learn about any issues, problems or grievances that could affect future loss. It is also beneficial for management to remind employees leaving the company about the details of any nondisclosure agreements that weresigned when the employee was hired.

- **Role-based awareness training**. Training is a key way to ensure that employees understand important company policies and procedures. Role-based awareness training is training customized for roles. For example, the training you give to somebody working as a network administrator is different than training you give to a salesperson. While some training is applicable across all roles, much of it isn't.

- **Data owner**. The data owner is responsible for ensuring the organization has adequate security controls based on the data classifications defined in the security policy. The data owner could be liable for negligence if they fail to establish and enforce security policies to protect sensitive data. For example, the data owner could be the chief operating officer (COO), the president or a department head.

- **Systems administrator**. The systems administrator is responsible for granting appropriate access to users. They might or might not have complete administrator rights, but they will have the ability to assign permissions. Administrators typically assign permissions based on the principle of least privilege, whereby they grant users access to only the data needed to perform their tasks.

- **System owner**. The system owner is the individual who owns an asset or system that processesdata, including sensitive data. The system owner develops and maintains the system security plan and ensures that the system is deployed according to the security requirements. While the system owner is typically the same individual as the data owner, it can be a different role in an organization (e.g., department head).

- **User**. A user is an individual who accesses data using a computing system to accomplish work tasks. Typically, users have access to only the data they need to perform their work tasks.

- **Privileged user**. A privileged user is an individual who requires a higher level of privileges to resources than other user accounts. Granting administrative privileges requires approval by appropriate personnel within the organization.

- **Executive user**. An executive user is an individual who is at or near the top of management in an organization. While an executive user might not be a privileged user, the account might require special controls. For example, only certain privileged users might be able to manage an executive user's account.

- **NDA**. A non-disclosure agreement (NDA) is a legal contract between two or more parties that details confidential information the parties will share with one another and should restrict access to the information from any third parties. NDAs can require that both parties are restricted in their use of the information, or they can restrict the use of information by a single party. For example, some employment agreements will include a clause restricting employees' use and dissemination of company-owned confidential information.

- **Onboarding**. Onboarding occurs when an employee is hired by an organization. The person is given employment information, and their user account is provisioned with the appropriate access to system resources. Many organizations will automate this process to ensure consistency and adhere to security practices.

- **Continuing education**. Since cybersecurity threats are constantly evolving, it is important for an organization to empower security personnel with the tools and knowledge to understand potential threats and how to avoid them. At a minimum, cybersecurity training should include the most common attack methods, the tools and techniques used to safeguard against attacks, and the appropriate methodology for responding to cybersecurity incidents.

- **Acceptable use policy/rules of behavior**. An acceptable use policy (AUP) is a set of rules defined by the organization that detail the type of behavior that is permitted when using company assets. An AUP should contain explicit language defining procedural requirements and the responsibilities of users. The purpose of the AUP is to help limit the risks posed to an organization by safeguarding the business and its property, both physical and intellectual.

- **Adverse action**s. While it is difficult to identify all inappropriate behavior, an organization should inform employees that adverse actions that affect business operations might cause a suspension of services. This should be described in the AUP or the security policy.

### General security policies

General security policies should identify the rules and procedures for all individuals accessing an organization's assets and resources. The security policies should also define how a company plans to protect the physical and IT assets and resources.

- **Social media networks/applications**. An organization should develop a social media security policy that governs the use of social media by employees. While using social media for business purposes can be beneficial to the organization, have clearly defined rules and procedures for using social media from company resources can significantly reduce risk.
- **Personal email**. The security policy should clearly define the use of business and personal email. For example, the policy might state that personal use of business email is strictly prohibited, or the policy could include guidelines on the personal use of business email. Some organizations allow employees to access personal email from business assets (e.g., computers, mobile devices, etc.). Because access to these uncontrolled email addresses presents a risk to the organization, the security policy should define how and when employees may access their personal email.

## 5.2 Summarize business impact analysis concepts

This section is focused on business impact analysis concepts but stays at a high level, similar to what you might expect from a manager or director.

### RPO

A recovery point objective (RPO) is a specific point in time a resource can be recovered to. Typically the resource or application owners decide on the RPO and management approves it. IT staff will configure the required frequency of replication and/or backups to meet the RPO. For example, critical resources should be backed up more frequently than less critical resources.

### RTO

A recovery time objective (RTO) defines how long the organization can operate without the resource or application. Again, the resource or application owners decide on the RTO and management approves it. IT staff will configure the systems and/or environment to meet the RTO. For example, the recovery time for critical apps often very short.

**MTTF/MTTR**

For managing the hardware lifecycle within an organization, hardware should be scheduled for replacement and/or repair. The schedule should be based on the mean time to failure (MTTF) and mean time to repair (MTTR) established for each asset. Typically, MTTF is the expected functional lifetime of the asset based on a specific operating environment. MTTR is the average length of time required to perform a repair on the device.

**MTBF**

The mean time between failures (MTBF) is the average the time between one failure and a subsequent failure. Manufacturers often list only the MTTF if the MTTF and MTBF values are the same.

**Mission-essential functions**

Mission-essential functions are a defined set of functions in an organization that must be continued throughout, or resumed rapidly after, a disruption of normal operations. Some organizations will implement tiers of mission-essential functions.

**Identification of critical systems**

After defining the mission-essential functions in an organization, it is important to identify the critical systems that support these functions. A critical system is defined as a system that must be highly available and/or reliable. Most critical systems are related to safety, mission, business or security.

**Single point of failure**

A single point of failure is a part of a system that will cause a failure of the entire system if it fails. A single point of failure is not desirable for organizations with a goal of high availability.

**Impact**

Impact is an estimate of the potential losses for an organization associated with a specific risk. During risk analysis, organizations will develop an estimate of probability and impact. The common types of impact include:

- **Life**. Organizations might estimate risk assessments based on the impact to life, or quality of life, factors. For example, an organization might consider the impact of providing health club benefits to employees.
- **Property**. Organizations might estimate risk assessments based on the impact to property. For example, an organization might consider the impact of leasing equipment as opposed to purchasing it.
- **Safety**. Organizations might estimate risk assessments based on safety or health risks. These might be related to a location, lifestyle, occupation or activity. For example, an organization might consider the risk of purchasing a building where tornados or earthquakes are common occurrences.

- **Financial**. Organizations might estimate risk assessments based on financial impacts such as lost revenue, costs and expenses.
- **Reputation**. Organizations might estimate risk assessments based on the impact of social factors such as reputation. For example, an organization might assess the risk of advocating for political parties for fear of alienating part of the customer base.

**Privacy impact assessment**

A privacy impact assessment is a process that assists organizations in identifying and minimizing the privacy risks of new projects or policies. The organization audits its own processes and identifies how these processes might affect or compromise the privacy of the individuals whose data it holds, collects or processes.

**Privacy threshold assessment**

A privacy threshold assessment helps an organization determine if a system contains private information. It is an effective tool that helps organizations analyze and record the privacy documentation requirements of corporate activities and determine whether a privacy impact assessment is required.

## 5.3 Explain risk management processes and concepts

As with the previous section, you need to be comfortable with the concepts here, especially as a manager might be familiar with them. There is less focus on technicalities and more focus on the business aspects.

**Threat assessment**

A threat assessment is used by an organization to determine the credibility and seriousness of a potential threat, as well as the probability that the threat will become a reality. Typically, a threat assessment includes identification, initial assessment, case management and a follow-up assessment. This information obtained from a threat assessment is used in a risk assessment. Types of threats include:

- **Environmental.** Environmental, or 'Mother Nature,' threats are tornados, earthquakes, floods, droughts, etc.
- **Manmade.** Manmade threats can be intentional or accidental, and can include loss of data, hacking, etc.
- **Internal vs. external.** All threats that organizations consider during a threat assessment will fall into one of two categories: internal or external. Internal threats are threats an organization can control. For example, an organization might assess the risk of implementing a data loss prevention system to ensure that corporate data is not exposed to unauthorized personnel. On the other hand, external threats are threats an organization is unable to control. For example, an organization can't control weather, protestors, or external hackers.

## Risk assessment

During risk management, an organization determines the likelihood of an event and the impact of the event to the organization. The process can be very detailed, complex and lengthy and involve multiple steps. Here are the key terms to understand:

- **SLE**. The single-loss expectancy (SLE) is the expected monetary value of an asset due to the occurrence of a risk.
- **ALE**. The annualized loss expectancy (ALE) is the expected monetary loss of an asset due to the occurrence of a risk over a one-year period.
- **ARO**. The annualized rate of occurrence (ARO) is the frequency at which a risk is expected to occur over a one year period. The ARO value can range from zero, indicating that the risk is expected to never occur, to a very large number, indicating that the risk occurs frequently.
- **Asset value**. As part of a risk assessment, an organization will appraise the value of assets. The value assigned to an asset is specific and encompasses tangible costs (e.g., purchase cost) as well as intangible costs (e.g., value to competitor).
- **Risk register**. A risk register, also called a risk log, is a master document that is maintained by an organization during a risk assessment to track issues and address problems as they arise.
- **Likelihood of occurrence**. The likelihood of occurrence is the probability that a specific risk will occur. The value can be expressed as a fraction between 0 and 1 or as a percentage.
- **Supply chain assessment**. As part of a risk assessment, an organization might perform a supply chain assessment for the purposes of reducing vulnerability and ensuring business continuity. Using the risk management process tools, organizations assess the risks and uncertainties caused by logistics-related activities or resources from partners in the supply chain.
- **Impact**. The impact of a risk is the consequences if it occurs (i.e., the cost of a risk).

- **Quantitative**. One of the two risk assessment methodologies, quantitative risk assessment assigns actual costs to the loss of an asset. Both methods are important for a complete risk assessment, as most organizations use a hybrid of both methodologies in order to gain a balanced view.

- **Qualitative**. One of the two risk assessment methodologies, qualitative risk assessment assigns subjective and intangible costs to the loss of an asset. Both methods are important for a complete risk assessment, as most organizations use a hybrid of both methodologies in order to gain a balanced view.

- **Testing**. An organization might choose to use risk-based testing to evaluate system quality and reduce the likelihood of system defects. When organizations lack sufficient time to test all system functionality, risk-based testing might include validating the system functionality that has the highest impact and probability of failure.

- **Penetration testing authorization**. Before a cybersecurity team can perform simulated attacks of an organization's network and systems, they must obtain permission from the organization. The authorization might include scope of the testing, liability and/or physical access.

- **Vulnerability testing authorization**. Before a cybersecurity team can scan the systems and network of an organization to identify security vulnerabilities, they must obtain permission from the organization. The authorization might

- **Risk response techniques**. After an organization completes a risk assessment, they must address each specific risk using one of the following options:

    - **Accept**. An organization might accept the risk (based on their risk tolerance) after a cost/benefit analysis determines that the cost of countermeasures would outweigh the cost of asset loss due to a risk. Typically, accepting risk requires a written statement that indicates why a safeguard was not implemented and who is responsible, as well as the consequences if the risk is realized.

    - **Transfer**. An organization might transfer, or assign, the risk by placing the cost of loss onto another entity internal or external to the organization. For example, an organization might purchase insurance or outsource some responsibilities.

    - **Avoid**. An organization might avoid the risk by selecting alternate options that have less associated risk than the default option. For example, an organization might require employees to fly to destinations rather than allowing them to drive.

    - **Mitigate**. An organization might reduce risk (also called risk mitigation) by implementing safeguards or countermeasures to eliminate vulnerabilities or block threats. On a side note, countermeasure selection is a post-risk assessment activity.

- **Deter**. An organization might deter risk by implementing deterrents to violators of security and policy. For example, an organization might implement auditing, security cameras or strong authentication.

- **Ignore**. An organization might ignore, or reject, the risk, denying that a risk exists. In this scenario, the organization hopes that the risk will never be realized. This should be considered an unacceptable risk response technique.

### Change management

Change management is used by organizations to ensure that no change leads to reduced or compromised security. While change management helps organizations prevent unwanted reductions in security, the primary goal of change management is to ensure that all changes in the organization include detailed documentation and auditing and can be reviewed and scrutinized.

## 5.4 Given a scenario, follow incident response procedures

In this section, order is important. Be sure to understand the order that a response takes and the people involved in the various tasks.

### Incident response plan

An incident response plan is a document to help IT respond to an incident. It includes details about how to detect, how to respond and how to recover.

- **Documented incident types/category definitions**. To create the incident response plan, an organization will define the common events that they classify as security incidents, such as an attempted network intrusion, an attempted denial-of-service attack, detection of malicious software, unauthorized access of data or a violation of security policies.

- **Computer incident response team**. A computer incident response team, or cyber-incident response team (CIRT), is a carefully selected group of well-trained people whose purpose is to respond to a computer, or cybersecurity, incident. This team will manage the incident so that it can be quickly contained and investigated, and the organization can recover. The team is typically comprised of employees who can drop their current responsibilities and have the authority to make critical decisions.

- **Roles and responsibilities**. Who is included in a CIRT and their roles will largely depend on the needs and resources of the organization. While the team can include outside personnel (e.g., law enforcement, vendors or technical specialists), here is a list of the common roles:

  - **Management.** Management's role during an incident, apart from giving the team the authority to operate, is to make the big decisions based on input from other members of the team.

  - **Information Security**. Information Security's role includes assessing the extent of the damage, containment, basic forensics and recovery. The members of the Information Security team are trained in handling electronic incidents.

  - **IT/MIS**. The IT/MIS role is to ease the effects to users and to assist the Information Security team with technical matters as required. In the event of an incident, the IT team will need to know where the data can be accessed and what areas of the network are off limits.

  - **IT Auditor**. The IT Auditor's role is to observe and learn how an incident started, ensure procedures are followed, and work with IT and Security to avoid problems in the future. IT Auditors might be present during an incident (such as if they work for the organization), but not take a great deal of action at that time.

  - **Security**. The Security role can include assessment of any physical damage, investigation of physical evidence, and guarding evidence during a forensics investigation to maintain a chain of evidence. If an incident involves direct contact with an asset, the security team should have the appropriate training to assist.

  - **Attorney**. The Attorney's role is to ensure the usability of any evidence collected during an investigation in the event that the company chooses to take legal action. The attorney can also provide advice regarding liability issues in the event that an incident affects customers, venders or the general public.

  - **Human Resources**. Human Resource's role is to provide advice on how to manage situations involving employees. HR will typically not be used until after an investigation has begun, and only if an employee is involved.

  - **Public Relations**. Public Relations' role is to communicate with team leaders to ensure there is an accurate understanding of the issue and the company's status, and to communicate with the press or to inform the stockholders of the current situation. A company's image is an asset that is of considerable vale, especially if the company is publicly traded.

  - **Financial Auditor**. The Financial Auditor will attempt to assign a monetary number to the damage that occurred as a result of an incident. This monetary value is frequently required for insurance companies and required if the organization takes legal actions. However, it is considered one of the more challenging aspects of an incident assessment.

- **Reporting requirements/escalation**. Event reporting and escalation procedures should be documented in the incident response plan. This process will ensure information security events and weaknesses associated with systems are communicated in a timely manner so the appropriate corrective action can be taken.

- **Cyber-incident response teams**. A cyber-incident response team is responsible for working through the cyber-incident response plan. The team is a technical team and begins responding immediately after learning of an incident. The ultimate goal is to eradicate the components from the incident (such as malware) and get the organization running normally again.

- **Exercise**. The purpose of an exercise is to demonstrate the effectiveness of the incident response planning. A simulated cyber attack will test the incident response plan's ability to manage and respond to a real-world cyber attack.

## Incident response process

An effective incident response process is handled in several steps or phases.

- **Preparation**. During the preparation phase, an organization will establish an incident response capability so that the organization is ready to respond to incidents. In addition, the organization will plan to prevent incidents by ensuring that systems, networks and applications are secure.

- **Identification**. One of the most challenging parts of the incident response process is to accurately determining whether an incident has occurred and, if so, the extent and magnitude of the problem. During this phase, an organization will determine whether an incident occurred in the past, is occurring now or could occur in the future.

- **Containment**. Most incidents require containment so it is important for an organization to develop a custom remediation strategy. As part of the containment phase, an organization documents actions and procedures for each type of incident (e.g., shut down a system, disconnect it from a network, etc.).

- **Eradication**. After an incident has been contained, an organization might need to eradicate, or eliminate, components of the incident. For example, during this phase, an organization might need to delete malware or disable breached user accounts, as well as mitigate vulnerabilities that were exploited. During the eradication phase, it is important to identify all affected hosts within the organization so they can be remediated.

- **Recovery**. During the recovery phase, an organization will restore any affected systems to normal operation and confirm that the systems are functioning normally. In addition, the organization might need to remediate identified vulnerabilities to prevent similar incidents. For example, during this phase an organization might restore systems from backups, rebuild systems, install patches/updates, change passwords or configure firewalls.

- **Lessons learned.** After recovery, it is important for an organization to conduct a meeting with all involved parties and identify any improvements that can be made to the process. Conducting a "lessons learned" meeting can be extremely helpful in improving security measures and the incident handling process. This meeting allows the organization to achieve closure about an incident by reviewing what occurred and the effectiveness of the incident response steps. Ideally, this meeting should be held within several days after the incident to ensure higher accuracy when recalling events and actions.

## 5.5 Summarize basic concepts of forensics

Note that this section focuses on basic concepts. There isn't an expectation that you have performed forensics in your job. However, because forensics is a specialized area of practice, spend extra time to study the material here.

### Order of volatility

The order of volatility is the order in which an organization should collect forensic evidence. Since highly volatile data can be easily lost, the most volatile data should be collected first and the least volatile data should be collected last. For example, an organization might choose the following order: physical memory, virtual memory, disk drives, backups and printouts.

### Chain of custody

In scenarios where evidence might be used in civil or criminal litigation, it is important for an organization to establish a chain of custody, also known as a chain of evidence, which documents the location of the evidence from the moment it is collected to the moment it appears in court. This can include the police who collect it, the evidence technicians who process it and the lawyers who use it in court.

### Legal hold

A legal hold is a process that an organization might use to preserve all relevant information when litigation is anticipated. The legal hold process is typically initiated by a communication from legal counsel to an organization to suspend the normal disposal of records, such as the recycling of tape backups or the archiving or deletion of data.

### Data acquisition

Based on the type of media, there are various methods an organization can use to retrieve data for the purposes of forensic analysis.

- **Capture system image**. When capturing a system image, an organization will create an exact sector-level duplicate of the media. Typically, the duplicate is created using a hard-drive duplicator or software imaging tool that mirrors the data at the block level.

- **Network traffic and logs**. As part of network forensics, an organization might monitor and analyze computer traffic for the purposes of intrusion detection and information gathering, or as part of evidence in litigation. An organization might also use network sniffing, recording, acquisition, and analysis of the network traffic and event logs in order to investigate a network security incident.

- **Capture video**. When capturing video and/or audio for the purposes of forensic analysis, it is important for an organization to understand how the system records the data (e.g., digital or analog) and the options available to retrieve the data (e.g., CD/DVD writing, USB, etc.).

- **Record time offset**. During the playback of a system image, media or data, it is important for an organization to understand the time offset of when the information was recorded (e.g., time zone). The time offset is typically logged when capturing the data to ensure that investigators account for the difference when reviewing the information later.

- **Take hashes**. After an image is captured, it is typically verified at critical points throughout the analysis to ensure that the evidence is still in its original state. This verification typically includes using the SHA-1 or MD5 hash functions. The process of verifying the image with a hash function is called hashing.

- **Screenshots**. In some scenarios, it can be necessary to capture information for forensic analysis using screenshots. Typically, these are still image captures of information on a computer monitor. This is commonly used in less-critical forensic analysis or in scenarios when the capture of a system image, media or data is not available.

- **Witness interviews**. Many times during forensic analysis, it is important to interview, or depose, individuals who might have direct knowledge related to the incident. This can include individuals who are responsible for the systems or network devices that were compromised or individuals who might have information about the attack.

### Preservation

After data is captured, it has to be preserved as evidence. While there are various laws that cover the seizure and preservation of data, in criminal cases this will often be performed by law enforcement personnel, as mandated by a warrant. However, in civil litigation it will typically be an officer within the organization. The assumption is that a company is able to investigate their own equipment without a warrant.

### Recovery

Many times during a forensic analysis, it can be necessary to recover information that has been intentionally or mistakenly deleted. It is the responsibility of an investigator to recover as much evidence as possible using various tools or methodologies. The type of data recovered varies depending on the investigation, but examples include chat logs, emails, documents, images or internet history. This data might be recovered from accessible disk space, deleted (or unallocated) space or the operating system's cache files.

### Strategic intelligence/ counterintelligence gathering

Strategic intelligence is the collection, processing, analysis, and dissemination of intelligence information for formulating policy and military plans at the international and national policy levels. In the commercial world, this information is used to build qualities that enable leaders to be effective strategists. The intelligence information gathered in counterintelligence is for protecting an organization's intelligence program against an attacker or the opposition's intelligence service. The information gathered can be used for forensic analysis, counter espionage or sabotage.

- **Active logging**. During counterintelligence gathering, it might be necessary for an organization to maintain active logs of the activity of the opposition or attacker.

### Track man-hours

When calculating cost values in a quantitative risk assessment, it is important for an organization to track the man-hours and expenses incurred by the incident response team. This is because assessments use specific monetary amounts, such as cost and asset values.

## 5.6 Explain disaster recovery and continuity of operations concepts

This section is focused on business continuity and disaster recovery. Many IT professionals have exposure to various aspects of these topics in their day-to-day job, so you might already be comfortable with much of the information here.

### Recovery sites

Based on business requirements, it might be necessary to have a location where an organization can relocate following a disaster recovery. This location is known as a recovery, or backup, site.

- **Hot site.** A hot backup site is a duplicate of the organization's current data center. All systems are configured with near-complete backups of user data. Typically, real-time synchronization is used between sites to ensure the data is current. While a hot site is the most expensive option, it enables the organization to restore normal operations in the shortest time with minimal losses after a disaster.

- **Warm site**. A warm site contains all the required hardware and connectivity to restore services; it is a reasonable duplicate of the organization's current data center. However, data has to be restored after a disaster. For example, the last backups from the off-site storage facility must be delivered and bare metal restoration must be completed.

- **Cold site**. A cold site is simply empty operational space with basic facilities. Everything required to restore service must be procured and delivered to the site before recovery can begin. While a cold site is the least expensive, the delay of becoming fully operational can be substantial.

## Order of restoration

Since staff and resources are limited during recovery, when w planning for disaster recovery, it is important for an organization to determine the order in which systems should be brought online — from the critical systems that should be restored first to the least critical systems that should be restored last. The organization should periodically review the order of restoration list as new systems are brought online and legacy systems are decommissioned.

## Backup concepts

When planning for a data restore after a disaster, an organization should choose the appropriate backup type that meets its business requirements.

- **Full**. A full backup is a complete copy of the data. A full backup provides the simplest method for recovery, since the entire data can be easily restored using a single recovery set. However, many organizations use them on a periodic basis only because they are time-consuming to make and they require a large amount of backup storage.

- **Incremental**. An incremental backup copies only the data that has changed since the previous backup, regardless of whether the backup was full or incremental. An incremental backup provides the fastest backup time and requires the smallest amount of backup storage. However, an incremental backup has a slower recovery time, since all incremental backups must be restored.

- **Differential**. A differential backup copies only the data that has changed since the previous full backup; it is considered a cumulative incremental backup. A differential backup provides a faster restore time and requires less backup storage than an incremental backup. However, a differential backup requires more time to create than an incremental backup.

- **Snapshots**. A snapshot is a copy of an application, disk or system. Typically, an organization will use a snapshot to restore a system or disk to a specific time. However, a snapshot is not commonly used as a periodic backup strategy because of the amount of backup time and backup storage required.

## Geographic considerations

It is imperative for an organization to include geographic diversity when planning for business continuity and disaster recovery.

- **Off-site backups**. While implementing backups ensures redundancy of data, hosting the backups in an off-site location ensures the redundant data does not have a single geographic point of failure.
- **Distance**. An organization should include enough distance between a primary and secondary site to minimize the potential for a disaster that affects both sites simultaneously (e.g., power outage, fire, tornado, hurricane, etc.). While there are varying opinions on the minimum distance between a primary and secondary site, the most appropriate distance depends on the business requirements.
- **Location selection**. When choosing the location of a primary or secondary site, it is important to assess the environmental risks, such as whether the location is susceptible to specific natural disasters (e.g., flood plain, fault line, frequency of tornados or hurricanes, etc.). In addition, the organization should consider the availability of technical resources at each location. This can include staffing requirements, access to replacement parts, access to alternate power sources, etc.
- **Legal implications**. Based on an organization's industry, there might be laws that impact business continuity planning. For example, businesses in the healthcare industry are required to have a disaster recovery plan with established guidelines for electronic records and signatures. There are a diverse range of laws that govern the healthcare, government, finance and utilities industries.
- **Data sovereignty**. When planning for geographic diversity, an organization might need to consider sovereignty laws governing data. For example, there might be national, state, or local laws that require hosting the data in specific locations.

## Continuity of operations planning

Continuity of operations planning helps ensure trouble-free operations through an unanticipated disruption.

- **Tabletop exercises**. The purpose of business continuity planning tabletop exercises is to demonstrate the ability of one or more critical business processes to continue functionality after a disruption — usually within a specific timeframe. Some of these exercises might be related to a cyberattack, data corruption or loss, natural disaster, or multiple disruptions.
- **After-action report**. The after-action report is a detailed document summarizing the results of the tabletop exercises. It can include the purpose and scope, objectives, exercise type and methodology, scenario, participants, and results (e.g., successes, failures, workarounds, etc.).

- **Failover**. After a disruption to business operations, an organization might need to consider failover of all information systems to an alternate site. Similarly, business operations planning needs to account for which services will be available during the disruption and how they will accommodate employees' access to those services.

- **Alternate processing site**. The alternate processing site is a site that allows all mission-critical or business-essential functions to be restored if there is a disruption to the primary processing site. The alternate processing site should sustain the continuity through restoration of services to the primary processing site.

- **Alternate business practices**. It might be necessary for an organization to implement an alternate set of business practices after a disruption. For example, non-mission critical personnel might be required to work from home, and employees might have to use alternate (or manual) processes for conducting day-to-day business until services are restored.

## 5.7 Compare and contrast various types of controls

For this section, you need to be prepared to choose a type of control based on a given scenario, and to choose from a list of controls based on a set of requirements.

**Deterrent**

Deterrent controls are warnings to discourage inappropriate or illegal behavior. For example, this includes warning messages about unauthorized access to an asset or a strict security policy stating severe consequences for employees who violate the policy.

**Preventive**

Preventative controls are barriers that are designed to stop an attacker from gaining unauthorized access to an asset. For example, this could be may include antivirus/antimalware software, firewall, or intrusion prevention systems (IPS).

**Detective**

Detective controls detect abnormalities and send alerts during an unauthorized access to an asset. For eexample, this include intrusion detection systems (IDSs) and security information and event management systems (SIEMs). Some controls, such as antivirus/antimalware software and intrusion prevention systems, are considered both preventive and detective.

**Corrective**

Corrective controls mitigate the damage after a disruption or attack. Examples include vulnerability patching and restores from a backup.

**Compensating**

Compensating controls (also known as alternative controls) are used when all the other controls cannot mitigate a risk. This might be due to business or security requirements. For example, this includes disabling internet access for highly classified data or segregation of duties.

**Technical**

Technical controls are security safeguards or countermeasures that are implemented using hardware, software or firmware components of an information system. Examples include antivirus/antimalware software, firewalls and logical access control systems.

**Administrative**

Administrative security controls (also called procedural controls) are primarily procedures and policies that define and guide employee actions in dealing with the organization's sensitive information.

**Physical**

Physical controls are used to deter or deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm. Examples include fences, doors, locks and fire extinguishers.

## 5.8 Given a scenario, carry out data security and privacy practices

This section is more of a hands-on section — you are expected to understand the operational tasks involved in administering the data security and privacy of your organization.

**Data destruction and media sanitization**

When an organization no longer needs sensitive data, the data should be destroyed by authorized personnel. Proper destruction, or sanitization, ensures the data cannot be subject to unauthorized disclosure. An organization's security policy should define the acceptable methods of destroying the data based on the data's classification.

- **Burning**. For information on paper resources, an organization might consider burning, using an incinerator, to ensure the data is not retrievable. While this method is effective, it is not considered the most environmentally-friendly option.

- **Shredding**. Shredding involves cutting paper into thin vertical strips (straight-cut shredding) or vertical and horizontal confetti-like pieces (cross-cut shredding). While most records can be shredded using the straight-cut method, cross-cut shredding is more appropriate for sensitive and confidential records.

- **Pulping**. Paper can also be destroyed by pulping. This process involves reducing the paper to fibers (called pulp) by mixing the paper with water and chemicals. Typically, the pulp can be recycled into other paper products.

- **Pulverizing**. An organization might pulverize paper resources. This process involves crushing or grinding the paper to reduce it to fine particles (such as powder or dust).

- **Wiping**. For electronic media, an organization might consider wiping (also called clearing or overwriting) the data. The process involves writing characters, or random bits, over all addressable locations on the media. This method ensures the cleared data cannot be recovered using traditional recovery methods and allows the media to be reused. However, it is possible to retrieve some of the original data from the media using sophisticated forensics techniques. In addition, some types of data storage devices do not support wiping (e.g., spare or bad sectors on hard drives and many modern SSDs).

- **Degaussing**. An organization might also consider degaussing the data using a degausser. The process involves using a strong magnetic field that erases data on some media (e.g., magnetic tapes, etc.). This allows the media to be reused. Unfortunately, this process is not recommended on hard disks since it will destroy only the electronics used to access the data and not where the data is stored (i.e., the platters inside the hard disks). In addition, the degaussing method is not supported on optical CDs, DVDs or SSDs.

- **Purging**. In less secure environments, an organization might consider purging the data to prepare media for reuse. The process is considered a more intense form of wiping in that it repeats the clearing process multiple times. In addition, it might also use another method, such as degaussing, to completely remove the data. While this method provides a higher level of assurance that the original data is not recoverable, it is not trusted by all business sectors (e.g., the U.S. government).

## Data sensitivity labeling and handling

As one of the first steps in asset security, an organization should identify and classify its information and assets. The organization labels assets appropriately based on the security policy requirements. In this context, assets include the data, the hardware used to process it and the media used to store it.

- **Confidential**. The confidential, or proprietary, label refers to any information that helps an organization maintain a competitive edge. In other words, disclosure of the information would cause exceptionally grave damage to the primary mission of an organization. This can include trade secrets, intellectual property, sales and marketing plans, financial data, etc.

- **Private**. The private label is for information that should stay private within the organization but that does not meet the definition of confidential data. In other words, disclosure of the information would cause serious damage to the primary mission of an organization. Many organizations label PII and PHI, as well as internal employee data and some financial (e.g., payroll) data, as private.

- **Sensitive**. The sensitive label is applied to information that should stay private within the organization but that does not meet the definition of confidential or private data. In other words, disclosure of the information would cause damage to the primary mission of the organization. This might include data about the internal network, such as its layout, devices, operating systems and software, which could be used to gain unauthorized access.

- **Public**. The public (or unclassified) label is for information that is available to any individuals outside the organization, such as websites and brochures. Although an organization does not protect the confidentiality of public data, it can protect the integrity of the data. For example, the organization might prevent individuals outside the organization from modifying content on its public websites.

- **Proprietary**. When a company has data specific to their operations or intellectual property, it is considered proprietary. For example, a chain of cookie shops might have several recipes that are proprietary data.

- **PII**. Personally identifiable information (PII) is any information that can identify an individual, such as name, Social Security number, date and place of birth, etc. “Individuals” includes employees as well as customers.

- **PHI**. Protected health information (PHI) is any health-related information that can be related to a specific individual, such as health information, healthcare provider, health plan, life insurer, etc. Any organization that store PHI information( including doctors, hospitals and employers) is required to protect it.

## Data roles

While one individual or multiple individuals might manage data protection within an organization, there are distinct roles that are required to ensure the organization complies with the security policy.

- **Owner.** The data owner is responsible for ensuring the organization has adequate security controls based on the classification defined in the security policy. In fact, the owner might be liable for negligence if they fail to establish and enforce security policies to protect sensitive data. The owner might be the chief operating officer (COO), president or a department head.

- **Steward/custodian.** The data steward or custodian is operationally responsible for the physical and electronic security and integrity of the information. Many times, the data owner will delegate day-to-day tasks to the steward. For example, the steward might be senior administrators who are responsible for ensuring that the data is backed up or for granting access and ensuring appropriate use of the information.

- **Privacy officer.** The privacy officer is responsible for ensuring that an organization protects data in accordance with laws and regulations. Many times, the privacy officer will have a legal background and assist in developing the security policy. This role will ensure the organization's practices comply with laws specific to the sensitivity of the data (e.g., PII, PHI, etc.).

### Data retention

Data retention is retaining data a specific length of time as dictated by an organization's security policy. Typically, a minimum threshold is defined in the security policy, but a maximum threshold can be defined as well. For example, many organizations require the retention of all audit logs for a specific amount of time. This data can then be used to reconstruct events during a security incident.

### Legal and compliance

It is the responsibility of an organization to ensure that the data security and privacy practices in its security policy conform to any applicable laws or regulations (e.g., laws regulating PII, PHI, etc.). In the absence of any applicable laws or regulations, the organization should show due diligence by including recommended standards for data security based on other businesses' practices in a similar industry.

# 6. Cryptography and PKI

Cryptography enables an organization to protect sensitive data stored on its systems and ensure that communications with business partners outside the organization are confidential.

## 6.1 Compare and contrast basic concepts of cryptography

Cryptography is a complex field. This section focuses on the basic concepts. But for those without experience, even the basic concepts will seem complex at first.

### Modes of operation

Most cipher modes encrypt data one block of information at a time. There are methods or modes of operation for how the cipher modes perform the encryption. The purpose of cipher modes of operation is to mask patterns that exist in encrypted data.

### Symmetric algorithms

Symmetric key algorithms, also called private key cryptography, rely on a shared secret encryption key. All of the parties participating in a communication possess a copy of the shared key and use it to encrypt and decrypt messages — the sender encrypts the message with the shared key and the receiver decrypts the message with the shared key. Symmetric encryption is very difficult to break when large-sized keys are used. It is primarily used to perform bulk encryption.

### Asymmetric algorithms

Asymmetric key algorithms, also known as public key algorithms, rely on a public key and a private key. All of the parties participating in a communication possess a copy of the public key but only one party possesses the private key. This provides a solution to the weaknesses of symmetric key encryption because the keys must be used in tandem to encrypt and decrypt. For example, if the public key encrypts a message, then only the corresponding private key can decrypt the message, and vice versa.

### Hashing

A hashing algorithm is a mathematical algorithm that maps data of arbitrary size to a hash of a fixed size. The purpose is to be a one-way function, infeasible to invert. In fact, the public key used in asymmetric encryption is based on a hash value — the value is computed from a base input number using a hashing algorithm.

| | |
|---|---|
| **Salt** | A salt is random data that is used as an additional input to a one-way function that hashes data. The random characters are concatenated to the front of a password before processing. This is commonly meant to safeguard passwords or passphrases in storage and helps protect against dictionary and other pre-computation attacks. |
| **Nonce** | A nonce is bits of data or a random number that are used just once as additional input to cryptographic communication. It is commonly used in authentication protocols to ensure that old communications cannot be reused in replay attacks. |
| **IV** | An initialization vector (IV) is similar to a nonce except that the random number must be selected in a nonpredictable way. In other words, the IV must be truly random and not sequential. Randomization is crucial for encryption schemes to achieve semantic security. |
| **Elliptic curve** | An elliptic-curve algorithm (ECC) reliesrely on the algebraic structure of elliptic curves over finite fields. As a result, ECC requires smaller keys than other cryptography to provide equivalent security. For example, a 1,024-bit RSA key is cryptographically equivalent to a 160-bit elliptic curve cryptosystem key. |
| **Weak/deprecated algorithms** | Cryptography algorithms are based on mathematical formulas. As computers become smarter and faster, the algorithms become weaker, resulting in less secure environments. Therefore, the algorithms are deprecated and replaced with more sophisticated algorithms. |
| **Key exchange** | For environments using symmetric cryptosystems, the previously unrelated parties face substantial challenges when attempting exchange the private key to secure communication. On the other hand, the key exchange for asymmetric (or public key) cryptography supports worldwide secure communication between parties that may not know each other prior to the communication. In fact, asymmetric algorithms provide convenient key exchange mechanisms and are easily scalable. |
| **Digital signatures** | After choosing a cryptographic hashing algorithm, an organization can implement a digital signature system that uses digital signature algorithms to provide proof that a message originated from a particular sender and to ensure that the message was not modified while in transit between the sender and the recipient. Digital signature algorithms rely on a combination of public key cryptography and hashing functions. |

**Diffusion**

One of the two operations that cryptographic algorithms rely on to obscure plaintext messages is diffusion (the other is confusion). Diffusion occurs when a change in the plaintext results in multiple changes spread throughout the cipher text. For example, if a single bit of the plaintext is changed, then half of the bits in the cipher text should change, and vice versa. Since a bit can have only two states, when the bits change from one random position to another, half of the bits will have changed state.

**Confusion**

The other operationAnother cryptographic algorithms rely on to obscure plaintext messages is confusion. Confusion occurs when each binary digit (bit) of the cipher text depends on several parts of the key, obscuring the connections between the two. This relationship between the plaintext and the key is so complicated that an attacker cannot determine the key merely by altering the plaintext and analyzing the cipher text results.

**Collision**

A collision occurs if two separate inputs produce the same hash value. Collisions are rare, but because hash functions have infinite input length and a predefined output length, inevitably two different inputs will eventually produce the same hash output.

**Steganography**

Steganography is the art of using cryptographic techniques to embed secret messages within another message. Steganographic algorithms rely on making alterations to the least significant bits of image files. In fact, the changes are so minor that there is minimal effect on the viewed image. For example, an organization can use steganography to add digital watermarks to documents to protect intellectual property.

**Obfuscation**

Obfuscation attempts to hide data in plain text or without the use of encryption. For example, you might use a letter substitution method where each letter of the alphabet is assigned to a different letter or each letter is assigned a number, or you might write sentences backwards or words the wrong way. There are simple variations and complex variations. Obfuscation is not considered a valid or secure method of protecting data but can be useful in very specific scenarios when the data is not sensitive and the use case requires only making it a little bit more difficult to obtain the data.

**Stream cipher**

A stream cipher is an algorithm that encrypts one bit, or character, of a plaintext message at a time. Although the stream cipher uses an infinite stream of pseudo-random bits as the key, the randomization should be unpredictable and the key should never be reused.

**Block cipher**

A block cipher is an algorithm that encrypts a fixed size of data (block) in a plaintext message; typically, each block is 64 bits, 128 bits or 256 bits. Padding is used in scenarios where bits of plaintext are shorter than the block size. Most of the symmetric ciphers used today are block ciphers.

| | |
|---|---|
| **Key strength** | The key length (or key size) is the number of bits in a key used by a cryptographic algorithm. Most symmetric-key algorithms are designed to have security equal to their key length. This is because the key length defines the upper bound on an algorithm's security — a measure of the fastest known attack against an algorithm based on the key length. |
| **Session keys** | A session key is a single-use symmetric key that is randomly generated to encrypt and decrypt a secure communications session. |
| **Ephemeral key** | In contrast to a static key, an ephemeral key is a short-lived cryptographic key used in the key establishment process. Usually they are not directly trusted as they are generated on the fly. |
| **Secretalgorithm** | A secret key algorithm (or symmetric key algorithm) is a cryptographic algorithm that uses the same cryptographic key to encrypt plaintext and decrypt cipher text. |
| **Data in transit** | Data in transit, or data in motion, refers to data actively moving from one location to another. This includes data transmitted over a private network or the internet. |
| **Data at rest** | Data at rest refers to data stored on media such as hard drives, external USB drives, backup tapes, etc. |
| **Data in use** | Data in use refers to data that is being processed (generated, updated, appended or erased) by an application. For instance, this may be data in system memory or temporary storage buffers. |
| **Random/pseudo-random number generation** | Random number generation is possible with hardware random number generators, but they are very slow. On the other hand, pseudo-random number generation uses an algorithm and an initial value to generate a sequence of random numbers at a much faster speed. |
| **Key stretching** | Key stretching is a technique that is used to make a weak key (e.g., a key with a small key size) more secure against a brute-force attack. Key stretching does this by using a key generation function to create a stretched, or enhanced, key based on the weak key. For example, salting a key appends a long, secret string to the weak key. |
| **Implementation vs. algorithm selection** | Implementation is the act of implementing cryptography, whereas algorithm selection is the process of choosing the right algorithm for your implementation. |

- **Cryptographic service provider.** A cryptographic service provider (CSP) is a software library that provides software or hardware-based encryption and decryption services. For example, an application might use a CSP to implement strong user authentication.

- **Cryptographic module.** A cryptographic module is hardware or software that performs cryptographic operations within a physical or logical boundary. The module might perform functions such as encryption, decryption, digital signatures, authentication techniques and random number generation.

### Perfect forward secrecy

Perfect forward secrecy is a protocol that uses a unique, short-term, private key for each secure session. This functionality ensures that even if a private session key is compromised, the exposed content will be limited to the session only.

### Security through obscurity

Security through obscurity is the act of hiding something that isn't secure, instead of securing it. For example, imagine that you have a management console to configure a database. Instead of forcing administrators to authenticate to it, you give it a long URL that is difficult to remember. While security through obscurity can prevent inexperienced malicious users from finding something you don't want them to find, it is considered ineffective and is typically not used in high-security environments.

### Common use cases

- **Low-power devices**. Low-power, or low-energy, devices have significantly lower energy use and storage capabilities than many other standard devices. Consequently, organizations are constrained to using lightweight cryptography to secure these devices.

- **Low latency**. The processing time required by a cryptographic algorithm can be significant. While low-latency encryption is an important property for standard devices, it is significantly more important for low-power devices.

- **Supporting confidentiality**. Considered one of the chief goals of cryptosystems, confidentiality ensures information or communications are kept private. It does this in three different scenarios: when data is at rest, when data is in transit and when data is in use.

- **Supporting integrity**. Integrity in cryptography ensures that data is not altered without authorization. For example, integrity ensures that stored data was not altered between the time it was created and the time it was accessed. Similarly, the recipient of a message can be certain that the message received is identical to the message that was sent from the sender.

- **Supporting obfuscation**. Obfuscation is valid only in low security environments where the threats are small and impacts are low. For example, teachers might store hall passes in a folder labeled "Blank paper" to keep kids from easily finding them.

- **Supporting authentication**. Considered a major function of cryptosystems, authentication verifies the claimed identity of system users.

- **Supporting non-repudiation**. Provided only by public key (or asymmetric) cryptosystems, non-repudiation provides assurance to the recipient that the message was originated by the sender. It prevents the sender from claiming they did not send the message (also known as repudiating the message).

- **Resource vs. security constraints**. A resource constraint is when you lack enough hardware or software to perform a task in a specific amount of time. It could also relate to human resources, such as not having enough people to manage your servers. Security constraints are different because they might be technical limitations of a solution or a standard or constraint built into your company policies and procedures.

- **High resiliency**. When you design a solution that ensures continuous operations even if some components fail, you design a highly resilient solution. High resiliency is often obtained by having extra hardware, additional software and security checks.

## 6.2 Explain cryptography algorithms and their basic characteristics

The exam blueprint calls out specific algorithms — study these and don't focus on algorithms not listed. While it can't hurt to be familiar with others, stay focused on the algorithms and cipher modes in this section.

### Symmetric algorithms

- **DES**. The Data Encryption Standard (DES) is a standard block cipher algorithm designed at IBM that is used by many other algorithms. Because of the relatively small key size (56 bits), DES is now considered insecure.

- **AES**. Advanced Encryption Standard (AES) is one of the most popular symmetric encryption algorithms. NIST selected it as a standard replacement for DES in 2001. AES is based on the Rijndael cipher and has been implemented into many other algorithms and protocols. For example, Microsoft's BitLocker and the Microsoft Encrypting File System (EFS) use AES. In addition, most CPU manufacturers include hardware AES support and the U.S. government has approved its use to protect classified data. AES supports key sizes of 128 bits, 192 bits and 256 bits.

- **3DES**. The triple DES (3DES) was created as a possible replacement for DES. Triple DES applies the DES algorithm thrice and has better practical security than DES. While the first design used 56 bit keys, newer implementations use 112 bit or 168 bit keys. Triple DES is used in many smart payment cards.

- **RC4**. The Rivest Cipher 4 or Ron's Code 4 (RC4) algorithm is a stream cipher that performs well because of its speed and simplicity. While RC4 is good if the key is never reused, it is considered insecure by many security experts.

- **Blowfish**. The Blowfish algorithm is a block cipher that was also developed as an alternative to DES. Because Blowfish can use variable key sizes that range from 32 bits to 448 bits, it is considered a strong encryption protocol. In fact, the bcrypt application in Linux systems uses Blowfish to encrypt passwords to protect against rainbow table attacks (see more on bcrypt later in this chapter). Rainbow tables are precomputed tables that match cryptographic hashes to a plaintext string. They are often used for cracking passwords efficiently.

- **Twofish**. Similar to Blowfish, the Twofish algorithm is a block cipher developed as an alternative to AES. Twofish uses a key size of 128 bits, 192 bits or 256 bits. It was designed to be more flexible than Blowfish by supporting additional hardware and uses two techniques not found in other algorithms: pre-whitening and post-whitening.

### Cipher modes

- **CBC**. Cipher block chaining (CBC) is a block cipher mode of operation that encrypts data as an entire block. During encryption, CBC will chain each block of plaintext with the previous cipher text block. Consequently, the decryption of a block of cipher text depends on all the preceding cipher text blocks. A single bit error in a cipher text block affects the decryption of all subsequent blocks. Attempts to rearrange the order of the cipher text blocks cause corruption during decryption.

- **GCM**. Galois/Counter Mode (GCM) is a block cipher mode of operation that uses hashing over a binary Galois field to provide both data authenticity (integrity) and confidentiality. GCM has been widely adopted because of its efficiency and performance in hardware and software implementations.

- **ECB**. Electronic Codebook (ECB) is a block cipher mode of operation that divides messages into blocks and encrypts each block separately. The simplest of the encryption modes, a key characteristic of ECB is that each possible block of plaintext has a defined corresponding cipher text value and vice versa. In other words, the ECB encrypts identical plaintext blocks into identical cipher text blocks and does not hide data patterns well. Because of this lack of diffusion, security experts do not recommend using ECB in cryptographic protocols.

- **CTR**. Counter (CTR) is a mode of operation that allows the block cipher to function like a stream cipher. The CTR generates keystream bits regardless of the encrypting data block's content. It does this by encrypting successive values of a counter, which produce a sequence that should never repeat.

- **Stream vs. block**. While both stream and block ciphers are symmetric ciphers, stream ciphers are based on generating an infinite cryptographic keystream by encrypting one bit at a time. On the other hand, block ciphers encrypt one block at a time, combining blocks for additional security. Block ciphers typically require more memory because they encrypt larger chunks of data and will even use data from previous blocks; stream ciphers have less memory requirements because they encrypt a minimal number of bits and will typically be much faster than block ciphers. Although stream ciphers are more challenging to implement, block ciphers are more susceptible to noise in transmission — a mistake in one part of the data will cause the rest of the data to be unrecoverable. Finally, stream ciphers do not provide integrity protection or authentication, whereas some block ciphers provide integrity and confidentiality protection. Typically, the best use cases for stream ciphers are scenarios where the amount of data is either unknown, or continuous (e.g., network streams). Alternatively, block ciphers are more useful when the amount of data is known beforehand (e.g., a file or data fields).

## Asymmetric algorithms

- **RSA.** The RSA (Rivest–Shamir–Adleman) algorithm is one of the first public-key cryptosystems. Based on an asymmetric algorithm, RSA publishes a public key that relies on two large prime numbers. While anyone can use the public key to encrypt a message, only someone with knowledge of the prime numbers can decrypt the message. Since RSA is a relatively slow algorithm, it is less commonly used to directly encrypt user data. On the other hand, RSA is commonly used for secure data transmission by encrypting a shared, symmetric key that is then used to perform bulk encryption/decryption at a much faster speed.

- **DSA.** The Digital Signature Algorithm (DSA) is considered a standard for digital signatures. The digital signature provides message authentication, integrity and non-repudiation. DSA creates the digital signature by using unique mathematical functions involving two 160-bit numbers. These numbers originate from the message digests (strings of digits created by a one-way hashing formula) and the private key. While messages are signed by the signer's private key, the digital signature is verified by the signer's corresponding public key. DSA uses the public key only for authentication, not for encrypting or decrypting messages.

- **Diffie-Hellman.** The Diffie–Hellman (DH) key exchange was one of the first public-key protocols in the field of cryptography. While most encrypted communication requires that the parties exchange keys using a secure channel, DH provides a method of securely exchanging cryptographic keys over a non-secure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

- **Groups.** Groups are sometimes used in cryptography to form primitives. Primitives are low-level algorithms often used for specific functions, such as one-way hashing functions.

- **DHE.** Diffie–Hellman ephemeral (DHE or EDH, depending on which cipher suite is used) is similar to DH but also provides forward secrecy by using ephemeral keys — the DH private key is transient and not saved by the server. DHE is commonly used to encrypt transport sessions (e.g., TLS).

- **ECDH.** Elliptic-curve Diffie–Hellman (ECDH) is a variant of the DH protocol that uses elliptic-curve cryptography for the anonymous key agreement. As a result, each party of the key exchange will have an elliptic-curve public–private key pair.

- **Elliptic Curve (ECDHE).** Elliptic-curve Diffie–Hellman ephemeral (ECDHE) is a variant of the DHE protocol that uses elliptic-curve cryptography to generate ephemeral keys. As a result, ECDHE also provides forward secrecy.

- **PGP.** Pretty Good Privacy (PGP) is an encryption program that provides cryptographic authentication and privacy. It does this by using a combination of encryption methodologies such as hashing, data compression, symmetric-key cryptography and public-key cryptography. PGP can be used to sign, encrypt/decrypt text files, emails, files, directories and disk partitions. PGP is owned and maintained by Symantec Corp.

- **GPG.** GNU Privacy Guard (GnuPG, GnuPGP or simply GPG) is the non-proprietary, free version of PGP. GPG is based on the OpenPGP standards established by the IETF. In addition, GPG provides for integrating it into email and operating systems such as Linux.

### Hashing algorithms

There are various cryptographic hashing algorithms that can be used to produce a checksum value. A checksum value is a small piece of data derived from the data being protected. The primary purpose of the checksum is to validate the authenticity of data (for example, that it hasn't changed).

- **MD5**. The Message-Digest algorithm 5 (MD5) is one of the two most widely used hashing algorithms. The function takes an input of arbitrary length and produces a message digest that is 128 bits long (i.e., a 128-bit hash value), typically rendered as a 32-digit hexadecimal number. MD5 has been known to cause collisions (i.e., two distinct messages that hash to the same value). However, it can still be used as a checksum to verify data integrity, such as verifying unintentional corruption or determining the partition for a particular key in a partitioned database.

- **SHA**. The other one of the two most widely used hashing algorithms, the Secure Hash Algorithm (SHA) is the common standard used for creating digital signatures. SHA was developed by the NSA. SHA-1 takes an input and produces a 160 bit hash value, typically rendered as a 40 digit hexadecimal number. SHA-2 can product hash values that are 224, 256, 384 or 512 bits.

- **HMAC**. Hash-based message authentication code (HMAC) is a type of message authentication code (MAC) that verifies both the data integrity and the authentication of a message. Because HMAC uses two passes of hash computation, the algorithm provides better immunity against length extension attacks.

- **RIPEMD**. RACE Integrity Primitives Evaluation Message Digest (RIPEMD) was developed by European researchers; the design is based on the MD5 hashing algorithm. One of the most recent versions, RIPEMD-160, is an improved version of RIPEMD. The performance of the algorithm is similar to SHA. RIPEMD is available in 128, 256 and 320 bit versions.

- **Key stretching algorithms**. Key stretching algorithms increase the strength of stored passwords by using salts. Here are two common key stretching techniques:

  - **Bcrypt**. Bcrypt is a password hashing function that is based on the Blowfish block cipher. Bcrypt incorporates a salt to protect against rainbow table attacks. In addition, bcrypt adapts over time by increasing the iterative counter that allows it to resist brute-force attacks. Bcrypt is the default password hash algorithm on many Unix and Linux systems to protect the passwords stored in the shadow password file.

  - **PBKDF2**. Password-Based Key Derivation Function 2 (PBKDF2) helps reduce the vulnerability of encrypted keys to brute-force attacks. PBKDF2 applies an HMAC function to a password and salt value multiple times to product a derived key. Using the key as a cryptographic key in subsequent operations makes password cracking much more difficult. Many algorithms and systems, such as WPA2, Apple iOS and Cisco operating systems, use PBKDF2 to increase the security of passwords.

## Obfuscation

Obfuscation is the act of hiding or obscuring something.

- **XOR.** XOR is an additive cipher that is commonly used in many algorithms. A cipher text can be created by applying the XOR operator to every character using a predefined key. Decrypting the cipher text simply involves applying the XOR operator with the key.

- **ROT13.** The rotate by 13 places (ROT3) cipher is a letter substitution cipher in which the letters of the alphabet are offset 13 places (all instances of the letter 'A' are replaced with the letter 'N', all instances of 'B' are replaced with 'O', etc.). The ROT13 cipher is the Caesar cipher (one of the earliest and simplest ciphers, such as replacing A with B, B with C, and so on) with a shift of 13. Because there are 26 letters in the basic Latin alphabet, to decode ROT13 the same algorithm is applied. Unfortunately, the cipher can be broken very easily so it provides virtually no security.

- **Substitution ciphers.** Substitution ciphers are the most common type of cipher and rely on replacing each letter of the plaintext, including punctuation marks and spaces, with another letter or random symbol. In contrast with a ROT13 or other Caesar cipher, the alphabet in a substitution cipher is completely jumbled and not simply the alphabet shifted. There are various forms of substitution ciphers that replace single letters, groups of letters, the entire message, or various substitutions at different positions in the message.

# 6.3 Given a scenario, install and configure wireless security settings

This is another hands-on section. You are expected to be familiar with the detailed installation and configuration of wireless security settings. As part of your exam preparation, spend some time reviewing your wireless routers in additional to reviewing this information.

## Cryptographic protocols

Cryptographic protocols, or encryption protocols, perform security functions using cryptographic algorithms.

- **WPA.** The Wi-Fi Protected Access (WPA) protocol protects wireless network traffic in transit by implementing much of the IEEE 802.11i standard. WPA uses the Temporal Key Integrity Protocol (TKIP) to verify the integrity of the packets. WPA uses the message integrity check algorithm TKIP to prevent an attacker from altering and resending data packets. However, security experts do not recommend using WPA because of major security flaws.

- **WPA2**. The Wi-Fi Alliance developed WPA2 as a replacement for WPA. WPA2 provides mandatory support for CCMP, which is an AES-based encryption protocol.

- **WPA3**. The Wi-Fi Alliance developed WPA3 as a replacement to WPA2. This new standard uses 128-bit and 192-bit encryption with forward secrecy and will mitigate security issues posed by weak passwords.

- **TKIP**. Temporal Key Integrity Protocol (TKIP) is a wireless encryption protocol that uses the standards as defined in the IEEE 802.11 standard. TKIP was designed to replace Wirelss Equivalent Privacy (WEP) without requiring the replacement of legacy hardware. TKIP uses a 128-bit key that it dynamically generates for each packet, which prevents the types of attacks that compromised WEP. Although TKIP is much stronger than a cyclic redundancy check (CRC), it is not as strong as the algorithm used in WPA2. In fact, TKIP is no longer considered secure; it was deprecated in the 2012 revision of the 802.11 standard.

- **CCMP**. Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is a wireless encryption protocol that uses the standards defined in the IEEE 802.11i amendment to the original IEEE 802.11 standard. Designed to address the vulnerabilities in WEP, CCMP is an enhanced data cryptographic encapsulation mechanism used for data confidentiality, integrity and authentication. CCMP is based on the AES standard and uses 128-bit keys and a 48-bit initialization vector algorithm, which minimizes vulnerability to replay attacks.

## Authentication protocols

Authentication protocols provide for the transfer of authentication data between two parties (e.g., client and server).

- **EAP**. The Extensible Authentication Protocol (EAP) is an authentication protocol that is frequently used in wireless networks and point-to-point connections; EAP is not used for wired networks. EAP provides formats for other protocols to encapsulate EAP messages (e.g., WPA, WPA2, etc.). Also, EAP supports multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords and public key encryption authentication.

- **PEAP**. The Protected Extensible Authentication Protocol (PEAP) is a version of EAP designed to provide more secure authentication for 802.11 wireless networks that support 802.1X port access control. It does this by encapsulating the EAP traffic within an encrypted and authenticated TLS tunnel. This ensures the client authentication information in the tunnel is protected and safe from eavesdropping.

- **EAP-FAST**. EAP Flexible Authentication via Secure Tunneling (EAP-FAST) is a protocol that is used in wireless networks for session authentication. EAP-FAST was designed to address the weaknesses in the Lightweight Extensible Authentication Protocol (LEAP) by performing authentication over a TLS tunnel. EAP-FAST uses Protected Access Credentials (PAC) to establish the TLS tunnel for authentication. The process has three phases: and has three phases

  - **Phase 0**. The PAC (shared secret) is provisioned and provided to the parties of the connection.

  - **Phase 1**. The TLS tunnel is established using the PAC.

  - **Phase 2**. The parties of the connection exchange credentials.

- **EAP-TLS**. EAP Transport Layer Security (EAP-TLS) is an EAP authentication protocol that is used to secure communications over a wireless network. EAP-TLS requires client-side X.509 certificates to authenticate with the server, but it is considered one of the most secure EAP standards available.

- **EAP-TTLS**. EAP Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS support by not requiring a client-side certificate to authenticate with the server. This simplifies the setup procedure, since the server can then use the established secure connection to authenticate the client.

- **IEEE 802.1x**. IEEE 802.1x is an IEEE standard for port-based network access control (PNAC). The IEEE 802.1x standard defines the encapsulation of the EAP protocol. The IEEE 802.1x standard provides a framework for devices on wireless or wired networks.

- **RADIUS Federation**. Remote Authentication Dial-In User Service (RADIUS) is a networking protocol frequently used for 802.1x authentication. RADIUS provides centralized authentication, authorization and accounting management for users who connect to a network service. RADIUS is frequently used by ISPs and enterprises to manage access to the internet or internal networks, wireless networks, and other services. For example, network access servers usually include a RADIUS component that communicates with the RADIUS server to allow clients to connect to the network.

## Methods

WPA provides various methods for authenticating users. These vary based on the method of key distribution and the encryption protocol.

- **PSK.** The WPA-PSK, or pre-shared key, method is designed for home or small office networks. While this method does not require an authentication server, each wireless network device encrypts the network traffic using a 128-bit encryption key, which is created from a 256-bit shared key. The client is required to enter the shared key as a passphrase of 8 to 63 ASCII characters or a string of 64 hexadecimal digits.

- **Enterprise.** The WPA-Enterprise method uses IEEE 802.1x and is designed for enterprise networks. This method requires a RADIUS authentication server. Although WPA-Enterprise requires enterprise-grade authentication, the method provides additional security, such as protection against dictionary attacks on short passwords, snooping and VLANs assigned automatically, and it supports Network Access Protection (NAP).

- **Open.** Open networks, or open access points, do not require authentication for clients to connect. While this method might use encryption, it is easily exploited. For this reason, security experts do not recommend implementing open networks unless needed for business requirements. For example, this method is commonly used in airports, coffee shops, hotels, business centers and other public areas.

- **WPS.** Wi-Fi Protected Setup (WPS) is an authentication key distribution method that is intended to simplify and strengthen network security. WPS was created by the Wi-Fi Alliance to allow home users to set up Wi-Fi Protected Access using one of four methods: PIN, push button, near-field communication (NFC) or USB. In addition, the method allows users to add new devices to an existing network without entering long passphrases. However, a major security flaw was discovered with the WPS PIN method that allowed attackers remote access.

- **Captive portal.** Commonly used in open wireless networks, a captive portal is a web page that shows users a welcome message informing them of the conditions of access (e.g., allowed ports, liability, etc.) and might require authentication or payment. Captive portals are commonly implemented at commercially provided Wi-Fi hotspots, such as airports, coffee shops, apartment houses, hotel rooms and business centers.

# 6.4 Given a scenario, implement public key infrastructure

This section focuses on implementation details. Be prepared to be given a scenario, potentially with requirements and existing infrastructure information, and have to explain how to move forward with a public key infrastructure (PKI) based on the requirements.

## Components

A PKI is made up of several components. Some components are required, such as a CA. Others are optional, such as an OCSP. To prepare for the exam, you should be able to distinguish between the components and understand how they are used.

- **CA.** A Certificate Authority (CA) is a trusted entity that issues digital certificates based on the X.509 standard. Similar to notarization services for digital certificates, the CA acts as a trusted third party between the owner of the certificate and the party relying on the certificate. For example, the CA issues certificates used in securing web pages (i.e., HTTPS) and electronically signing documents.

- **Intermediate CA**. An intermediate, or subordinate, CA is a variation of the CA in that it performs the day-to-day work of signing certificates and updates revocation information of certificates. A root CA will frequently have one or more intermediate CAs that is trusted by the root CA.

- **CRL**. One of the two techniques used to verify the authenticity of certificates and identify revoked certificates, a certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing CA and should no longer be trusted. This will typically occur prior to the certificate's scheduled expiration date. Similar to a blacklist, the CRL is used by various clients (e.g., web browsers) to check whether a certificate is valid. One of the disadvantages of using a CRL is that clients must frequently download updates to maintain a current list.

- **OCSP**. The other of the two techniques used to verify the authenticity of certificates and identify revoked certificates, the Online Certificate Status Protocol (OCSP) provides a request/response mechanism for clients to obtain the revocation status of a digital certificate. This advantage eliminates the latency inherent in maintaining a CRL by providing real-time certificate verification.

- **CSR**. A certificate signing request (CSR) is a specially formatted message sent from an applicant to a CA for the purpose of requesting a digital certificate. Along with the CSR, the applicant will send the public key for which the certificate should be issued. Included in the CSR are the identifying information (e.g., domain name, common name, friendly name, etc.) and the integrity protection (e.g., digital signature, etc.).

- **Certificate**. An X.509 certificate is a digital certificate used to verify that a public key belongs to a particular entity (e.g., a user, computer or service). Based on the X.509 public key infrastructure (PKI) standard, the certificate contains the version, serial number, issuing CA, validity period and other information about the entity. While the public key in a web server's certificate is used to encrypt traffic to the site, the certificate identifies who owns the site.

- **Public key**. One of the two components of an asymmetric key pair, a public key is used by a sender to encrypt a message using the recipient's public key. In digital signatures, the public key is used by the recipient to verify messages signed with the sender's private key.

- **Private key**. The other component of an asymmetric key pair, a private key is used by a recipient to decrypt a message that was encrypted using the public key. In digital signatures, the private key is used by the message sender to sign messages. This proves to the message recipient that the message has not been altered. Both of the keys in the key pair — the private key and the public key — have to be created before the CSR.

- **Object identifiers (OID)**. Object identifiers (OID) is an identifier mechanism endorsed by the International Telecommunications Union (ITU), ISO/IEC and IETF for the standardized naming any object, concept or thing by using an unambiguous, persistent name expressed as a group of characters. OID is used to name almost every object type in X.509 certificates (e.g., components of Distinguished Names, CPSs, etc.).

## Concepts

- **Online vs. offline CA**. Most CAs are online — they actively process CSRs and provide data for CRL downloads or responses to OSCP requests. Because the consequences of a compromised root CA are so great, security experts recommend safeguarding them from unauthorized access. For this reason, the root CA is isolated from network access and is frequently kept in a powered-down state — an offline CA. An offline CA should have no impact on any PKI operations if the root CA has delegated operations (e.g., issuing, distributing and revoking digital certificates) to one or more intermediate CAs. The root CA is brought online only when required for infrequent tasks, such as the issuance or re-issuance of certificates authorizing intermediate CAs.

- **Stapling**. OCSP stapling is a standard for checking the revocation status of X.509 digital certificates. Although OCSP responses are much faster than a CRL download, there can be a minor delay during the start of the TLS connection (the handshake). OCSP stapling removes the need for a browser to request the OCSP response directly from a CA by appending a time-stamped OCSP response signed by the CA to the initial handshake. This eliminates the need for clients to contact the CA, because the web server caches, or staples, the OCSP response to the initial TLS handshake. As a result, OCSP stapling reduces the workload by 30% and improves security.

- **Pinning**. Public key pinning is a security mechanism that helps websites prevent impersonation by attackers using fraudulent digital certificates. A website's certificate is typically validated by verifying the signature hierarchy, but this chain of trust can be compromised. To combat this risk, the web server provides the client with a list of pinned public key hashes for a given period of time. Upon subsequent connections to the web server, the client expects the server to use only these public keys in its certificate chain.

- **Trust model**. PKI relies on a hierarchical trust model that assigns to a third party the responsibility of establishing a trust relationship between two parties. At the top is a commonly recognized source (root CA) that all the parties using the PKI trust. Typically, under the source are subordinate authorities (intermediate CA) that rely on the source authority.

- **Key escrow**. Key escrow is a key exchange process in which a key used to decrypt data is held in escrow, or stored, by a third party. Only an authorized party may access the key. If the key is lost or compromised, only an authorized party may access the key to decrypt the data.

- **Certificate chaining**. Digital certificates are verified using certificate chaining, which is an ordered list of certificates in a hierarchy. The chain begins at the bottom with the digital certificate, and each certificate in the chain is signed by the entity identified by the next certificate in the chain. Any certificate between the digital certificate and the root certificate is called a chain or intermediate certificate. The chain ends with a root CA certificate, which is always signed by the CA itself. The signatures of all certificates in the chain are verified up to the root CA certificate.

## Types of certificates

- **Wildcard**. A wildcard certificate is a digital certificate that is used with a domain and all the corresponding subdomains. The notation for a wildcard certificate consists of an asterisk and a period before the domain name.

- **SAN**. A Subject Alternative Name (SAN) allows additional subject names to be associated with a digital certificate. The additional names might or might not be similar to the primary subject name of the certificate. In fact, a SAN can include email addresses, IP addresses, URIs, directory names or DNS names.

- **Code signing**. A code signing certificate is a digital certificate used to confirm the software author and ensure that the code has not been altered. Code signing certificates are commonly used by software developers to digitally sign apps, drivers, and software programs.

- **Self-signed**. A self-signed certificate is a digital certificate that is signed using its own private key. For example, a root CA certificate is considered a self-signed certificate. However, self-signed certificates are typically not used for multi-party communications unless the certificates are added to a whitelist of trusted certificates (e.g., root CA certificates).

- **Machine/computer**. While some digital certificates are assigned to a user, other digital certificates are assigned to a machine or computer. In this latter scenario, certificates can be used allow clients to verify the authenticity of servers as well as mutual authentication, or two-way, authentication. Mutual authentication refers to two parties authenticating with each other simultaneously.

- **Email**. Securing email using a digital certificate ensures the confidentiality and integrity of messages between parties. Multiple options for the sender to secure email are available, including signing, encryption or both. One of the primary protocols used is the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol, which has emerged as a standard for encrypted email. S/MIME uses the RSA encryption algorithm and is recommended by security experts.

- **User**. A certificate assigned to a user is required to allow users to sign or encrypt email.

- **Root**. A root certificate is the top-most certificate assigned to the root CA. It is also the most important certificate in a PKI. If something happens to the certificate (such as it is revoked or it expires), it impacts all of the certificates issued by the PKI.

- **Domain validated**. A domain validated (DV) certificate is a digital certificate in which the domain name of the applicant has been validated by proving ownership of a DNS domain. A DV certificate is typically used for Transport Layer Security (TLS). Domain ownership is typically proven using domain registrar information, DNS records, email or the web hosting account of a domain.

- **Extended validation**. An extended validation (EV) certificate is similar to a domain validated certificate but with more stringent verification of the requesting entity's identity by a CA. Although a DV certificate provides a basic level of verification, the EV certificate provides additional trust for consumers who want confidence that a website operator is a legal, established organization with a verifiable identity. The additional vetting that is required of applicants include manual checks of all the domain names requested by the applicant, checks against independent information sources, checks against official government sources and phone calls to the company to confirm the position of the applicant. If the certificate is accepted, the government-registered serial number of the business and its physical address are stored in the EV certificate.

## Certificate formats

There are several file name extensions for X.509 certificates. Some of these extensions are also used for other data, such as private keys.

- **DER.** A Distinguished Encoding Rule (DER) certificate is a binary encoded certificate. All types of certificates and private keys can be encoded using the DER format. DER formatted certificates commonly use the .cer and .der file name extensions.

- **PEM.** A Privacy-enhanced Electronic Mail (PEM) certificate is a variation of the DER certificate. The PEM certificates are Base64 encoded ASCII files, which are enclosed between the strings "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----". PEM certificates are the most common format; they use the .cer, .crt, .pem and .key file name extensions.

- **CER.** CER is a file extension for certificate files. Certificates are usually in binary DER form, but Base64-encoded certificates are common too (see .pem above). The Windows operating system natively handles the .CER file extension for operations such as viewing and importing certificates.

- **P7B.** P7B files, also called Public-Key Cryptography Standards (PKCS) #7 certificates, contain only certificates or certificate chain certificates but not the private key. P7B certificates commonly use the .p7b and .p7c file name extensions.

- **PFX.** A personal information exchange (PFX) certificate is binary encoded. The PFX certificate stores the server certificate, intermediate certificates and the private key in an encrypted file. PFX certificates commonly use the .pfx file name extension.

- **P12.** A P12 file, also called Public-Key Cryptography Standards (PKCS) #12 certificate, typically contains certificate and password-protected private keys. The P12 certificate is a successor of the PFX certificate and commonly uses the .p12 file name extension.

netwrix

# Study Guide Questions for the CompTIA Security+ Certification Exam

The questions presented here are meant to be used after you read the Study Guide for the CompTIA Security+ Certification Exam. If you are unable to answer at least 70% of the questions, go back to the study guide and review the material for the questions that you missed.

## Domain 1 Threats, Attacks and Vulnerabilities

1 You are investigating malware on a laptop computer. The malware is exhibiting the following characteristics:

- It is blocking access to some user data.
- It has encrypted some user data.
- A stranger is demanding compensation to give you access to the data.

Which type of malware is on the laptop computer?

**a**. Worm
**b**. Spyware
**c**. Trojan
**d**. Crypto-malware

**Correct answer:** D

**Explanation:** Based on demand for payment, you can be certain that this is some type of ransomware. Because it has encrypted some of the data, the malware is called crypto-malware.

2 An executive assistant reports a suspicious phone call to you. You ask him to describe the calls in more detail and he provides the following information:

- The caller claims to be a member of the IT department.
- The caller claims that the executive assistant's computer has a virus.
- The caller requests access to the executive assistant's computer to remove the virus.
- The caller asks for immediate access due to the vicious nature of the virus.

The executive assistant thought the call was suspicious because it came from outside of the company and he had never heard of the person before. Which type of attack occurred and which technique did the attacker use to try to gain access to the computer?

**a**. Watering hole attack using intimidation
**b**. Impersonation attack using scarcity
**c**. Vishing attack with urgency
**d**. Whaling attack with authority

**Correct answer:** C

**Explanation:** When a phishing attack occurs by telephone, it is called a vishing attack. When an attacker tries to persuade the victim with urgency, the goal is to alarm the victim or scare the victim into quick action (such as giving the person access to the computer). In this scenario, the attacker made the virus sound vicious in hopes that the executive assistant would quickly grant access to his machine.

3 One of your customers recently reported that their corporate website was attacked. As part of the attack, the website was defaced and a message supporting a political party was added. Which of the following threat actors is likely responsible?

**a**. Script kiddie
**b**. Hacktivist
**c**. Insider
**d**. Competitor

**Correct answer:** B

**Explanation:** Because the website was defaced with a political message, a hacktivist is likely responsible for the attack.

4 Your company plans to have a third-party company perform penetration testing on their IT environment. The company has established the following guidelines for the testing:

- The third-party company will not be given any information about the IT environment.
- The third-party company will not be given access to the IT environment.

Which type of penetration testing should you request?

**a**. White box
**b**. Black box
**c**. Pivot
**d**. Persistence
**e**. Gray box

**Correct answer:** B

**Explanation:** With black box testing, the third-party company has to rely on public sources of information and public-facing resources to get started.

5 A customer has requested that you test their user password strength. The customer provides you a secure, air-gapped computer and the password hashes. You need to try to crack the passwords using the hashes. Speed is the most important factor because the customer is contemplating an enterprise-wide password reset. Which of the following technologies should you use in your attack?

**a**. Rainbow tables
**b**. Dictionary
**c**. Brute force
**d**. Collision

**Correct answer:** A

**Explanation:** Of the available choices, rainbow tables provide the fastest effective attack method for password hashes. Because the tables are pre-computed, they provide excellent performance, especially for password hash attacks.

## Domain 2 Technologies and Tools

1 You are preparing to implement two web servers, both of which will serve the same website and content. The website has a single page, which simply displays the air temperature inside the company's datacenter. You opt to deploy a load balancer so that both servers are active. You need to implement the simplest load balancing scheduling algorithm for this scenario. Which scheduling algorithm should you implement?

**a**. Affinity
**b**. Round-robin
**c**. Active-passive
**d**. Active-active

**Correct answer:** B

**Explanation:** In this scenario, only affinity and round-robin are valid choices for the scheduling algorithm. For simple load balancing scenarios, you should use round-robin — it is simple to deploy and maintain. Affinity is useful when you need users to communicate with a single web server (such as during an online purchase).

2 You are troubleshooting communication between a client and a server. The server has a web application running on port 80. The client is unable to connect to the web application. You validate that the client has network connectivity to the server by successfully pinging the server from the client. You check the server and notice that the web server service is running. Now, you need to validate the port that the web application is listening on. Which of the following tools should you use?

**a**. Tracert
**b**. Arp
**c**. Netstat
**d**. Tcpdump

**Correct answer:** C

**Explanation:** In this scenario, you need to look at the listening ports on the server. You should use the Netstat tool to list all the listening ports. Optionally, you can look at the web server configuration to look for the configured port, but this is not one of the answers listed.

3 A customer is preparing to deploy a new web application that will primarily be used by the public over the internet. The web application will use HTTPS to secure the user connections. You are called to review the configuration of the environment. You discover the following items:

- The customer's internal PKI issued the certificate for the web application.
- The certificate used for the web application is a wildcard certificate.

Based on your findings, which of the following outcomes is most likely to occur for public users?

**a**. The certificate will be reported as untrusted.
**b**. The certificate will be reported as expired.
**c**. The certificate will be reported as mismatched.
**d**. The certificate will be reported as revoked.

**Correct answer:** A

**Explanation:** The certificate will be reported as untrusted because the internal PKI issued the certificate, but the web application is used by the public over the internet and the public doesn't trust your internal PKI. While there are scenarios in which an internal PKI is trusted for public use, that isn't specified in this scenario. The wildcard certificate, while not recommended for this scenario, will not cause any of the issues listed.

4 You are configuring a mobile device management solution to be used for your company's mobile devices. The management team has a single immediate requirement: prevent users from bypassing the Apple or Android app store to install apps. What should you do?

**a**. Configure MDM to prevent carrier unlocking.
**b**. Configure MDM to prevent sideloading.
**c**. Configure MDM for content management.
**d**. Configure MDM for containerization.

**Correct answer:** A

**Explanation:** Sideloading is the act of installing apps outside of the app stores. Many organizations prefer to block sideloading because of the high risk of malware in apps outside of an official app store.

5 You are implementing a secure file sharing solution at your organization. The solution will enable users to share files with other users. The management team issues a key requirement — the file sharing must occur over SSH. Which protocol should you implement?

**a**. S/MIME
**b**. FTPS
**c**. SRTP
**d.** SFTP

**Correct answer:** D

**Explanation:** SFTP uses SSH for file transfer. FTPS is a file-transfer protocol but it uses FTP rather than SSH. The other two protocols are not designed for file sharing: S/MIME is used for email communication, and SRTP is used to secure communications over a telephony or communications-based network.

## Domain 3 Architecture and Design

1 You are implementing a software distribution server farm. The server farm has one primary purpose — to deliver your company's installer files to customers or potential customers via trial installers. The software distribution will be available over the internet to anyone. The company has established the following requirements:

- The software distribution implementation must not provide access to the company's internal resources.
- The software distribution implementation must maximize security.

You need to implement the server farm using a technology or zone to meet the requirements. What should you do?

**a**. Implement the server farm in the DMZ.
**b**. Implement the server farm in an extranet.
**c**. Implement the server farm in the intranet and use port forwarding.
**d.** Implement the server farm in an air-gapped network.

**Correct answer:** A

**Explanation:** In this scenario, you need any internet user to be able to get to your software distribution system. The DMZ provides for this. The second requirement is to maximize security. As a segmented network at the edge of your network, the DMZ satisfies this requirement as well. While an air-gapped computer or network would also maximize security, users would not be able to get to the software distribution system. An extranet is like a DMZ, but it used for vendors, partners and suppliers, not the general population.

2 You are deploying a forward proxy. The proxy will cache intranet and internet content to speed up web requests from users. You want to maintain a simple configuration and maximize security. You need to decide which network zone to use for the proxy servers. Which zone should you choose?

**a**. Intranet with a private IP address
**b**. Extranet
**c**. DMZ
**d.** Intranet with a public IP address

**Correct answer:** A

**Explanation:** The proxy will cache content on the intranet and on the internet. If it is deployed in the intranet, it will have easy access to both. If it were deployed outside of the intranet, then permitting communication to the intranet from the DMZ (or elsewhere) might open attack vectors and result in a complex configuration.

3 You are ordering servers for a customer that needs high security. You plan to use encrypted hard drives and a secure boot process with all the servers. You opt to use a hardware chip on the motherboard to facilitate the use of encrypted hard drives and the secure boot process. Which of the following components should you order for each server?

**a**. Hardware security module (HSM)
**b**. Trusted platform module (TPM)
**c**. Hardware root of trust
**d.** UEFI BIOS

**Correct answer:** B

**Explanation:** A TPM is a hardware chip on a motherboard that enables cryptographic operations for tasks such as secure boot and disk encryption. An HSM provides encryption keys to other services, such as a PKI or a web-based service.

4 You were recently hired by a small company that is beginning to develop software internally and wants to ensure that its IT environments supports a secure development lifecycle. The company asks you to propose a list of the environments required to support their development efforts, along with the order in which they should use the environments for software releases. Which of the following options should you recommend?

**a**. Staging, Development, Test and Production environments
**b**. Test, Development, Staging and Production environments
**c**. Staging, Test, Development and Production environments
**d.** Development, Test, Staging and Production environments

**Correct answer:** D

**Explanation:** A development environment is the place to develop code. Then, you deploy the code to a test environment that resembles your production environment. Next, you deploy it to a staging environment that resembles your production environment as closely as possible. Last, you deploy it to your production environment.

5 You have a new web application that collects data from users — users fill out a form and submit it. You store the data in a database. After a few months, you review the data and discover that some information is not stored in a consistent manner. For example, some phone numbers are stored with dashes (213-555-4321), some are stored with periods (213.555.4321), and some are stored with other methods, such as (213)555-4321. Other data, such as the name of the city, is inconsistent. For example, some users used “San Francisco”, some used “San Fran”, some used “SF”, and others used “SFO”. You need to figure out a way to ensure consistent data. Which two of the following methods can you use? (Choose two answers.)

**a**. Error handling
**b**. Input validation
**c**. Normalization
**d.** Obfuscation
**e.** Model verification

**Correct answer:** B, C

**Explanation:** You can use input validation to ensure that data is entered in a specific format. For example, you could require users to choose a city name from a drop-down menu and enter phone numbers without dashes. Alternatively, you can use normalization to fix the data after you obtain it. For example, you can use normalization to change “San Fran”, “SF” and “SFO” to “San Francisco” and to strip non-numeric characters from phone numbers.

## Domain 4 Identity and Access Management

1 You are integrating your on-premises identify provider (IdP) with a cloud-based service. The cloud-based service offers federated authentication. Which two of the following protocols could you use for the integration? (Choose two.)

**a**. LDAP
**b**. SAML
**c**. Kerberos
**d.** OpenID Connect

**Correct answer:** B, D

**Explanation:** SAML is one option for federating with a cloud-based service; it has been around for a long time and is widely supported. OpenID Connect is another option; it is newer than SAML and gaining momentum in the industry. LDAP and Kerberos are protocols used for on-premises authentication and directory integration; they are not suitable for internet-based authentication.

2 You are troubleshooting a user authentication issue. The user reports that they are trying to connect to a cloud-based portal. The portal prompts them for a second factor of authentication. The company uses TOTPs for multi-factor authentication. However, the user reports that when they enter their TOTP, it isn't accepted. Which of the following reasons could be the cause?

**a**. The hash expired.
**b**. The one-time password expired.
**c**. The initial authentication via SSO is failing.
**d.** The user's password expired.

**Correct answer:** B

**Explanation:** In this scenario, the one-time password is expired. The user might not be entering it fast enough or is entering it too late. Because the user is getting prompted for the multi-factor authentication, the initial authentication (via SSO or manual auth) is functional.

3 You are updating the user account configuration for your company. You need to ensure that a user will be prevented from logging on if 10 bad password attempts are tried on their user account, even if the 11th attempt is the valid password. Which of the following technologies should you implement?

**a**. Account lockout
**b**. Password expiration
**c**. Password history
**d.** Account disablement

**Correct answer:** A

**Explanation:** Account lockout prevents the use of an account after a specified number of bad password attempts. An account must be unlocked before it can be used again. Some organizations automatic unlock the account after a specific period of time.

4 An app team is integrating their app with your on-premises directory service. The app requires a user account that will be used to look up objects in the directory and run automated tasks. A company security policy requires the use of the principle of least privilege. Which type of account should you choose?

**a**. Shared account
**b**. Guest account
**c**. Service account
**d.** Privileged account

**Correct answer:** C

**Explanation:** A service account is an account that runs as a service (often in the background), runs jobs (such as scheduled tasks) and performs other non-human functions, so it meets the needs for the app team. A shared account is shared amongst multiple users. A guest account is a temporary account which often has limited or no access. A privileged account is used by IT administrators but often provides too much access to use as a service account (because it wouldn't follow the principle of least privilege).

5 Your company is planning to switch to certificate-based authentication for its client computers. The client computers are company-owned and run Windows 10. You need to implement a technology for certificate-based authentication that is suitable for this scenario. Which technology should you implement?

**a**. Hardware security module (HSM)
**b**. Smart card
**c**. Proximity card
**d.** Trusted platform module (TPM)

**Correct answer:** B

**Explanation:** Of the answer choices listed, only one is a certificate-based authentication solution suitable for client computers and general-purpose computing. Smart cards are compatible with client computers and user authentication and meet the requirements of this scenario.

## Domain 5 Risk Management

1 Your company is reviewing backups of key data. It finds that some data has not been backed up. However, an existing company policy requires that all data be backed up. You need to have the data backed up. Which of the following people should handle the backup?

**a**. Data owner
**b**. Privacy officer
**c**. Data custodian
**d.** Data creator

**Correct answer:** C

**Explanation:** The data custodian is responsible for the day-to-day operations of managing data, including backups. In this scenario, the data custodian should back up the data, while the data owner should dictate requirements for the data.

2 Your company has a control in place for shared user accounts: Such accounts can only be used to log onto training computers. However, your directory service has a limitation that only 32 computers can be added to the control. Recently, the training lab received additional computers and now has 100 computers. You need to use a different type of control for the shared user accounts. Which type of control should you use?

**a**. Administrative
**b**. Deterrent
**c**. Preventative
**d.** Compensating

**Correct answer:** D

**Explanation:** A compensating control is an alternative control that you use when a primary control isn't feasible (such as when prohibitively expensive or technically impossible). In this scenario, the primary control is no longer viable, and a compensating control is needed.

3 You are preparing to perform a risk assessment for a customer. The customer has issued the following requirements for the assessment:

- The assessment must be objective.
- The assessment must report on the financial costs and/or implications of each risk.

Which risk assessment approach should you use?

**a**. SLE
**b**. ALE
**c**. Qualitative
**d.** Quantitative

**Correct answer:** D

**Explanation:** In this scenario, you need an objective (instead of a subjective) analysis. The quantitative approach is objective, looking at numbers and costs. A qualitative approach is subjective, less precise, and open to judgment. SLE and ALE are not risk assessment approaches.

4 You are helping your organization with its business continuity and disaster recovery project. The company recently decided that the maximum data loss allowed is 4 hours. You are drafting up the documentation for the project. How should you document the maximum data loss?

**a**. Recovery time objective (RTO)
**b**. Recovery point objective (RPO)
**c**. Mean time between failure (MTBF)
**d.** Mean time to repair (MTTR)

**Correct answer:** B

**Explanation:** The RPO represents the maximum data loss allowed, based on time. The RTO is the maximum amount of time allowed to recover down systems.

5 Your company is undertaking a project to strengthen the privacy of its data. The management team has identified the first task: Find systems that contain private information. Which of the following actions should you do to complete the first task?

**a**. Complete a privacy impact assessment.
**b**. Complete a privacy threshold assessment.
**c**. Complete a risk assessment.
**d.** Complete a threat assessment.

**Correct answer:** B

**Explanation:** A privacy threshold assessment is specifically designed to find systems that contain private information. After a threshold assessment, it is common to go through a privacy impact assessment.

## Domain 6 Cryptography and PKI

1 You are evaluating cryptographic algorithms for a customer. The customer has a specific requirement for encryption that uses shared secrets. You need to recommend an encryption algorithm to meet the requirement. Which algorithm should you recommend?

**a**. Hashing algorithm
**b**. Symmetric key algorithm
**c**. Asymmetric key algorithm
**d.** Elliptic curve algorithm

**Correct answer:** B

**Explanation:** A symmetric key algorithm requires a shared secret. Each communicating party has the shared secret, which enables encryption and decryption. The other algorithms do not use a shared key.

2 Your company is preparing to deploy a new two-tier public key infrastructure (PKI). The security team requires that the implementation have an offline root certification authority (CA). You need to deploy other servers to ensure that certificates can be deployed to clients. Which type of server should you deploy?

**a**. OCSP
**b**. Intermediate CA
**c**. Online root CA
**d.** CRL server

**Correct answer:** B

**Explanation:** In this scenario, you are deploying a two-tier hierarchy. The root CA represents one tier. The other tier must be intermediate CAs or subordinate CAs. In a two-tier hierarchy, the intermediate or subordinate CAs will take on all the PKI online tasks, such as issuing certificates.

3 You are deploying a guest wireless network for a restaurant. The restaurant's legal department requires that restaurant guests agree to the restaurant's wireless terms and conditions before being allowed to use the network. What should you do?

**a**. Deploy an open wireless network with encryption.
**b**. Deploy a wireless network with Wi-Fi Protected Setup (WPS).
**c**. Deploy a wireless network with WPA Enterprise.
**d.** Deploy a wireless network with a captive portal.

**Correct answer:** D

**Explanation:** A captive portal enables you to display terms and conditions, rules and other information and require guests to click "I agree" before being allowed on the network.

4 You are helping your company improve the security of a password database. Presently, the database contains password hashes as computed from the original password. The company wants to improve the way password hashes are stored in the database. Specifically, the company wants to make it harder to crack the password hashes if the password database is compromised. What should you do?

**a**. Use a salt.
**b**. Use key stretching.
**c**. Use obfuscation.
**d.** Use an ephemeral key.

**Correct answer:** A

**Explanation:** The company is presently storing password hashes computed from the password, which can easily be cracked if the password database is compromised. A salt adds random data to the front of the password prior to hashing, which greatly improves the security of the password database and makes stolen password hashes harder to crack.

5 You are implementing security into your organization's email system. The goal is to provide a way that recipients can, with certainty, validate that the sender sent the message and that the message was not modified in transit. Which of the following items should senders add to their email messages to ensure recipients can validate the sender?

**a**. Private key
**b**. Public key
**c**. Digital signature
**d.** Salt

**Correct answer:** C

**Explanation:** A digital signature validates the identity of the sender and confirms that the email message wasn't modified in transit.

# Useful References

## Cybersecurity

### Webinars

Behind the Scenes: 4 Ways Your Organization Can Be Hacked

Top 5 Things to Do to Stop Attackers in Their Tracks

Pro Tips for Defending Your Organization from Data Breaches

Securing Your Network Devices in the Era of Cyber Threats

[Deep Dive] Force IT Risks to the Surface

Withstanding a Ransomware Attack: A Step-by-Step Guide

### Best Practices

Data Security Best Practices

Information Security Risk Assessment Checklist

How to Prevent Ransomware Infections: Best Practices

### eBooks

Addressing Modern Cybersecurity Challenges through Enterprise-Wide Visibility

Defending Against Crypto-Ransomware

### Blogposts

10 Security Tips for Malware Prevention

What to Know about a Data Breach: Definition, Types, Risk Factors and Prevention Measures

Top 5 Human Errors that Impact Data Security

Must-Have Data Security Controls

Cybersecurity Assessment: Definition and Types

Risk Analysis Example: How to Evaluate Risks

# Useful References

## Career Advice

Blogposts

A Perfect Storm in Cybersecurity

Top Certifications to Begin and Advance Your Tech Career

Expanding Your Cybersecurity Skills when You Are No Longer a Beginner

CompTIA Security+ sy0-401 vs. sy0-501: What to Know when Renewing Your sy0-401

Top CompTIA Security+ Boot Camps, Online Training, and Free Courses

How to Pass the Security+ Exam: Tips to Get the Cert on Your First Attempt

# Already Planning the Next Steps in Your Development as a Security Professional?

If your plan includes a next-level security certification, then this free CISSP Exam Study Guide will be exactly what you need. It covers all CISSP domains, with sample questions and answers for each domain. You can use this guide to assess how ready you are to take the exam or identify areas for improvement to focus on when preparing for the CISSP exam.

**Download CISSP Guide**

# About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com.

# Next Steps

**Free trial** – Set up Netwrix in your own test environment: netwrix.com/freetrial

**In-Browser Demo** – Take an interactive product demo in your browser: netwrix.com/browser_demo

**Live Demo** – Take a product tour with a Netwrix expert: netwrix.com/livedemo

**Request Quote** – Receive pricing information: netwrix.com/buy


**CORPORATE HEADQUARTER:**

300 Spectrum Center Drive
Suite 200 Irvine, CA 92618

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

**PHONES:**

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

**OTHER LOCATIONS:**

| | |
|---|---|
| Spain: | +34 911 982608 |
| Netherlands: | +31 858 887 804 |
| Sweden: | +46 8 525 03487 |
| Switzerland: | +41 43 508 3472 |
| France: | +33 9 75 18 11 19 |
| Germany: | +49 711 899 89 187 |
| Hong Kong: | +852 5808 1306 |
| Italy: | +39 02 947 53539 |

**SOCIAL:**

netwrix.com/social