# CompTIA Security+

SY0-601

By Sultan Alangari

# SY0-601 CompTIA Security+

## 4 - Operations and Incident Response

### 4.1 – Security Tools

### 4.2 – Incident Response

### 4.3 – Investigations

### 4.4 – Securing an Environment

### 4.5 – Digital Forensics

# Section 1 – Attacks, Threats, and Vulnerabilities

## 1.1 – Social Engineering

### Phishing

- Pretending to be someone else like my bank that are not who they say they are.
- Social engineering combined with spoofing.
- Typosquatting: try to present to us URL that looks very similar to what we are expecting.
- Pretexting: going to lie to you. For example, calling you and says, hi, we're calling from Visa regarding.
- Pharming: attack an entire group of people simultaneously, everybody who visited the DNS server or visited the website will be automatically directed to the attacker's website. This means that you could be typing in the correct address in your browser, but because the DNS has been poisoned.
- Vishing: Performing this attack over a voice line
- Smishing or SMS phishing or text messages: Performing this attack over (SMS) Short Message Service. where this phishing is all done over a text message communication.
- Spear phishing: directed phishing attacks, person or group of people.
- Whaling: spear phishing attack that goes after a person who has control of a lot of money or a lot of information. like CEO or the head of the accounting department.

### Impersonation

- The attacker was trying to pretend to be someone they were not.

### Dumpster Diving

- Spend your time inside of a garbage bin, looking through pieces of personal information.
- Make sure that your garbage area is locked up and secured.
- Use shredders or burn all of this information.

### Shoulder Surfing

- Looking over your shoulder.

### Hoaxes

- In the world of IT security, a hoax is a situation that seems like it could be real, but in reality, it's not real at all.

## Watering Hole Attacks

- Instead of going attack directly to victim, they're going to go to a third party.
- This third party is the watering hole.
- Attacker need to find out where users visiting. and trying to find a vulnerability on this third-party site.

## Spam

- Spam Over Instant Messaging (SPIM): try to filter out this information before it arrives in your user's inbox.
- Many different strategies for blocking spam and preventing it from getting into our mailboxes:
  - **Email gateway or spam filter.**
  - **Reverse DNS**: look at the IP address
  - **Tar pitting:** does is slow down your mail server send and receive take an amount of time.
  - **Recipient filtering.**
  - **Accepting those messages**.

## Influence Campaigns

- This process usually starts by the bad actor creating a number of fake accounts, and start creating content and it amplifies the effect and the scope of who's able to read these messages and people start to see this content and sharing. And then mass media will pick up this story.

## Other Social Engineering Attacks

- **Tailgating**: unauthorized individual might follow you in through that open door.
- **Invoice Scam:** send fake invoice directly to that person with a bill that needs to be paid.
- **Credential harvesting**: trying to gain access credentials that might be stored on your local computer.

## Principles of Social Engineering

- **Authority** They'll call in and say that they are calling from the CEO's office.
- **Intimidation** They want you to do a function and they are going to intimidate you to be able to do that.
- **Element of scarcity**.
- Familiarity or liking.
- Trust.

## 1.2 – Attack Types

### An Overview of Malware

- Malware is malicious software. It’s software that is going to do something that will probably have a negative impact on you.

### Viruses and Worms

- The virus needs a human being to start the process that can reproduce itself.
- One of the most common virus types is:
  - **Program virus:** virus is part of an application that is running.
  - **Boot sector virus:** virus is started along with the boot sector.
  - **Macro virus:** running inside of another application, commonly associated with Microsoft Office.
  - **Script virus:** running script in the operating system, or runs inside of your browser.
  - **Fileless virus:** It is a virus that never installs itself or saves itself as a file on your file system. This is a method that the virus uses to try to avoid some of the techniques that the antivirus software uses, especially if the antivirus software. the Fileless virus operates solely in the memory of the computer.
- worm can jump from machine to machine without any human intervention whatsoever.

### Ransomware and Crypto-malware

- **Ransomware:** this method of taking away your data and requiring you to pay to get that data back.
- **Crypto-malware:** is new form of ransomware uses cryptography to be able to encrypt all of your personal information. The way that you obtain that key to decrypt is that you send the attackers money or Bitcoin.

## Trojans and RATs

- **Trojan horse software:** is software pretends to be something else and it looks like software that is perfectly normal.
- One type of software that’s commonly downloaded by this Trojan horse software is a PUP. This is a potentially unwanted program. This may not be malicious software, but it could be undesirable and may cause performance problems on your computer.
- one of the things that it tends to do is to open up a back door on your system.
- **Remote Access Trojan (RAT):** A type of software that attackers might install as part of the back door, this is a remote access tool that gives a third party access to your computer to have nearly complete control over the operating system.

## Rootkits

- **Rootkit**: modifying files in the kernel of the operating system.
- Almost impossible to delete it from your system.
- We’ve created new types of BIOS software such as the UEFI BIOS that includes a feature called secure boot. This secure boot feature will look to see if any part of the kernel has been changed. And it will not boot a system that may have been modified, thereby preventing rootkits from being installed on our modern systems.

## Spyware

- **Adware:** when you’re installing application, it will install additional applications advertisement along with it, it causes performance problems in your operating system.
- **Spyware:** is a bit more malicious than adware, because gather information about you.
- Spyware it can be installed often as Trojan horse.

## Bots and Botnets

- **Bot**: stands for robot and it’s a term to describe the automation that occurs behind the scenes when your system is taken over by this type of malware.
- The bot malware on a computer is working along with other computers that are infected with the same bot malware to create a botnet.
- **Botnet:** is controlled through a Command and Control server or C&C server.
- The C&C server is responsible for sending out commands. Those commands will be received by the botnet. And then the botnet will perform whatever function has been asked of it by the C&C.

## Logic Bombs

- **logic bomb:** is a type of attack that occurs when a separate event is triggered.
- One very common type of logic bomb is a time bomb. This is one that occurs when a particular date and time is reached.
- It’s difficult to identify if a logic bomb in a system because it doesn’t follow any known signature.
- difficult to gather evidence after the fact because it will delete themselves once they’ve executed.

## Password Attacks

- The best way to store password is in a format that uses a hash.
- Hashing of a password takes the password and represents the password as a string of text information. We call this a message digest. You’ll sometimes hear this referred to as a fingerprint.
- A spraying attack avoids the results of a locked account for trying the wrong password over and over again without success.

## Physical Attacks

- **USB cable:** tell your operating system that it human interface device (HID). This is the categorization for keyboards and a mouse.
- **Flash drive**.
- **Skimming:** This is stealing our credit card information, the attackers are usually adding additional hardware to the card reader on the device that you’re using, also have a camera that’s monitoring what buttons you press when you put your PIN into the system.

## Adversarial Artificial Intelligence

- Attackers used malicious data or invalid data during the training process in (ML).
- During the learning process that all of the data going into the machine learning is legitimate.

## Supply Chain Attacks

- The supply chain is the chain of manufacturing that gets a product from the very beginning to the very end of its process.
- This includes the raw materials, suppliers, manufacturers, distributors, customers, and consumers. With all of these different points along the chain, there’s a lot of opportunity for someone to be able to attack any one of these and affect anybody else who might be downstream in that chain.

## Cloud-based vs. On-Premises Attacks

- With cloud security everything is centralized, and therefore your costs tend to be lower. You don’t have to worry about having your own data center or purchasing any hardware, and you have a third party that handles all of the IT services for you.
- If all of your data is on-site, you obviously have your own data center. And you have to incur all of those data center costs, but you know where all of your data is, and you’re the one who gets to control what happens with that data.
- One advantage in the cloud is that most cloud providers are providing very large-scale security.

## Cryptographic Attacks

- **A hash collision** is when you have two very different types of plain text, but both of those plain text creates exactly the same hash. This is something that should never happen.
- One way to prevent this is to increase the size of the hash, which decreases the potential to have a collision.
- One well-known collision hash occurred with MD5. This was the Message Digest Algorithm version 5.
- **Downgrade attack:** Normally when you want to communicate securely to another device, there’s a conversation that initially takes place where both sides determine what the best possible encryption algorithm might be. If you’re able to somehow sit-in the middle and influence that conversation, you could have the two sides downgrade to a type of encryption that might be very easy to break.

## 1.3 – Application Attacks

### Privilege Escalation

- **Privilege escalation**: attacker is using a normal user login to somehow gain elevated rights on the system.
- **Data execution prevention:** The operating system itself may have safeguards in place to prevent someone from taking advantage of a privileged escalation. One of these safeguards is it's a way to only allow applications to run in certain areas of memory where that particular function is allowed

### Cross-site Scripting

- **Cross-Site Scripting:** allowed information from one site to be shared with another site.
- **NON-Persistent or reflected cross-site scripting attack:** run scripts within the user input fields on that device. This might be in a search field, or some other input field on the web page. For the reflected cross-site scripting attack, we have to have that user click a very specifically-crafted link for that particular vulnerability to be exploited.
- **Persistent or stored cross-site scripting attack:** scripting attack that stored permanently on a server, Once the attacker posts their malicious message, everyone who reads through that particular post will also get that malicious script and run it on their local machine
- With the reflective attack, the attacker could specify the user that they were targeting, but with something like a stored cross-site scripting attack, that particular script is on the page, and anyone visiting the page would be running this script.

### Injection Attacks

- Attacker puts their own code into an existing data stream.
- You can inject HTML, or LDAP, or SQL code.
- **Dynamic-Link Library (DLL):** is a binary package that implements some sort of standard functionality, such as establishing a network connection or performing cryptography.

### Buffer Overflows

- **Overflow attack**: the threat actor submits input that is too large to be stored in a variable assigned by the application.
- A buffer overflow attack occurs when one section of memory is able to overwrite a different section of memory. This type of overriding or spilling over of memory should not occur.

## Replay Attacks

- **Replay attack:** If the attacker capture information then he can be replayed across the network to make it seem as if it was coming from you.
- Attacker can physically install a network tap that will redirect or send a copy of all network traffic.
- Logical way like ARP poisoning.
- One very simple kind of replay attack is **called pass the hash**. This is referring to the hash value that is associated with a password that is sent across the network during the authentication process. If the attacker can gain access to the hash, they may be able to replay that hash back to the server and pretend that they are the original workstation.
- Another technique developers use is to salt the hash.
- Sure the cookies saved in our browser and configuration on our computers are secure.
- If that attacker gains access to that session ID, they could have used that information to pose as the victim and communicate directly to that service without requiring a username or password.

## Request Forgeries

- Your browser that determines where your browser is going to go to gather the information that's required to make up that page.
- When you visit a website, there's usually a combination of code that's running. Some of the code is running in a browser that's on the client and some of the code is running on the web server itself.
- **Cross site request forgery (XSRF or CSRF):** this is sometimes called a one click attack or session writing.
- You might have already logged into Facebook, for example. So every time you visit facebook.com, it shows as your credentials whenever you're visiting that page.
- This potentially means that an attacker could get your computer to create requests on their behalf using your credentials. And that's why this is a cross site request forgery and not an actual cross site request that's done normally.
- **Server Side Request Forgery (SSRF):** Another type of forgery gets rid of the client completely. We don't have to worry about trusting that a browser is logged in. We'll instead perform the forgery directly on the server side

## Driver Manipulation

- hardware drivers that are effectively the conduit between the hardware of your computer and the software of your operating system. These drivers are trusted by your operating system.
- A shim is something you would use to fit into the gap that's created between two different objects.
- There are also shims built into your operating system. Windows has one called the Windows compatibility mode.
- This also uses an application compatibility shim cache, to be able to cache this information that's being transferred between the existing operating system

## SSL Stripping

- **SSL stripping:** or what's called the HTTP downgrade attack.
- This is the way that an attacker can sit on the path of the communication and modify the communication between the client and a server, so that it's able to see all of the data in that data flow.
- They might use ARP spoofing, or it might be a rogue Wi-Fi hotspot that allows the attacker to get in the middle of this conversation.

## Race Conditions

- **Race condition:** You do have problems that can occur though if multiple things are occurring simultaneously and you weren't expecting them to occur simultaneously.
- Attackers can take advantage of this using something **called a time-of-check to time-of-use attack, a TOCTOU.** This type of attack is checking for things to occur on the system and making changes but knowing that there might be other changes occurring behind the scenes at the same time.

## Other Application Attacks

- In a normal application, memory is allocated for storage or for calculations and when that memory is no longer in use it's returned back to the system.
- **Memory Leak:** memory is never returned back to the system and the application continues to use more and more until uses all of the available memory then crashes application or operating system.
- **Null Pointer Dereference**: attacker make an application point to a null section of memory where nothing exists rather than the part of memory where the application data might exist and causes the application to crash.
- **Overflow.**
- **Directory Traversal Attack**: allows attackers to read from different parts of a server, even areas of a server where normally they should not have access.
- **web server misconfiguration** might allow an attacker to use the two dots and a slash be able to move backwards through the file system.
- **Error Messages**: showing just enough information so that people understand what the error might be and they might be able to report that to someone else.
- **API attack.**
- **Resource Exhaustion**: type of attack that uses up the available resources on a device so that the application or the service that's being used by it is no longer accessible by others.
- **Zip Bomb**: very small zip file but if you uncompressed this file, it would uncompressed to a 4.5 petabyte.

## 1.4 – Network Attacks

### Rogue Access Points and Evil Twins

- **Rogue access point:** is access point that has been added to your network without your authorization.
- **Wi-Fi Pineapple:** tools help you understand the wireless spectrum and can set themselves up as a rogue access point to see if other people on the network happen to use it.
- **802.1x:** network access control mechanisms that requires that everyone connecting to the network provide a username and password.
- **Evil twin:** This is an access point that is designed to look exactly like the access points that are already on your network, but they were put there for a malicious reason. This is usually an attacker that's trying to get your users to connect to their access point by using a similar SSID name, similar configuration settings, or putting the access point in an area where your users might happen to be.
- If the attacker does manage to get the wireless evil twin installed somewhere close by to your users, that evil twin could overpower the signal from the other access points and become the primary access point on the network.

### Bluejacking and Bluesnarfing

- **Bluejacking**: attacker sending unsolicited message over Bluetooth. and low priority security concern.
- **Bluesnarfing** attacker can access data on your mobile using the Bluetooth communications channel. And security concern that is a higher priority is Bluesnarfing.

### Wireless Disassociation Attacks

- **Wireless Disassociation or Wireless Deauthentication Attack**: Wireless keeps coming back and disappearing over and over and over again.
- **Management Frames** manage quality of service communication, they allow devices to associate to access points, and disassociate themselves from the access point.
- **Arrow Dump NG:** Utility that shows me what's running on the network.
- **Air Replay:** Utility to be able to send deauthentication frames.

## Wireless Jamming

- **Radio Frequency Jamming or RF Jamming:** is a way for an attacker to disrupt a wireless network and create a denial of service situation. to decrease the signal-to-noise ratio at that receiving device.
- **The signal-to-noise ratio** describes the relationship between the good signal received by a device and all of the other type of wireless signal that is received by that device.

## RFID and NFC Attacks

- **Radio-Frequency Identification** (**RFID):** It's a technology that's used in anything that you might want to track.
- **Near Field Communication (NFC):** another type of RFID technology that is very common in today's mobile devices
- Bluetooth also uses NFC to simplify the pairing process.

## Randomizing Cryptography

- **Randomization:** core elements of cryptography, the resulting encrypted data looks nothing like the original plain text. To be able to add randomization **we need to add a nonce.**
- **Nonce**: is an arbitrary number that you would use one time.
- **Initialization Vector (IV):** type of nonce.
- **Salt:** This type of password randomization to make sure that the passwords that we're storing are randomized across all users on the system.

## On-Path Attacks

- **On-Path Attack or Man in The Middle attack (MIMA):** is an attacker that sits in the middle between two stations and is able to intercept, and in some cases, change that information that's being sent interactively across the network.
- A common on-path attack on a local IP subnet is **an ARP poisoning.**
- **Address Resolution (ARP) Protocol poisoning:** a protocol does not have any type of security associated with it. Devices receive and modify ARP tables without any type of authentication or any type of encryption. This would allow an attacker to send ARPs to any device on the local subnet, and those local devices would interpret the ARPs as if they were coming from a legitimate source.
- **MIMA** is not an easy attack to execute like ARP poisoning we needed to be on the local network.

## MAC Flooding and Cloning

- **Media Access Control (MAC).**
- **MAC flooding:** when MAC address table fill up, switch will recognize that it's not able to add any more devices to the table. When this happens, a switch will no longer start directing individual frames.
- **Spoof or Clone a MAC address:** This is when an attacker will modify the MAC address of their device to match the MAC address of a legitimate device that is either on the network or has recently left the network.

## DNS Attacks

- **DNS poisoning attack:**
  - One way to perform a DNS poison is to modify the host file that's located on each individual device.
  - Another way to poison DNS is for someone to sit in the middle of the conversation with an on-path attack and be able to modify a query that's being sent to a client.

## Denial of Service

- **Denial of Service:** thousands of people hitting a website at one time and the service to become unavailable.
- **Denial of service can be very simple**:
  - Attacker pulling the power switch is a very effective Denial-of-Service.
  - Plug in the wrong cables to the wrong switch, you may inadvertently create a loop in your network.
  - Turn on Spanning Tree Protocol so that you won't inadvertently cause these types of layer to loops.
- **Distributed Denial of Service attack:** This is where many devices might be used simultaneously to create bandwidth spikes or attack a particular service and cause it to be unavailable.
- **DDOS amplification:** ways to increase the amount of traffic that's being sent during these DDOS attacks. a small attack, and suddenly have it arrive at the victim's machine as a much larger attack.
- **Rapid elasticity**: It's a very common way to maintain uptime, especially on a cloud-based service.

## Malicious Scripts

- Attacker having an automated attack function means that they can sit back and let many different automated functions find the vulnerable systems wherever they happen to be.
- If an attacker wants to control Microsoft Windows, then Windows PowerShell is a perfect jumping off point. They’re able to administer the system, access Active Directory, or modify files that are in the file system.
- Python is used across many different operating systems, including Windows, Mac OS, and Linux. hich means you could create Python scripts that might work across different operating systems.
- if an attacker is interested in hacking cloud based system servers, routers, switches, and other infrastructure devices, then Python might be a good choice.

## 1.5 – Threat Actors and Vectors

### Threat Actors

- **Threat actor or malicious actor:** attacker or the bad guy.
- some of those major categories and examine some of the motivations:
  - **Advanced Persistent Threat (APT):** stay in network until you take them out.
  - **Nation state is usually a government.**
  - **A Hacktivist is** a hacker who has a purpose or goal
  - **Script kiddie** trying to gain access to internal resources.
  - **Organized crime:** set of professional criminals they do for a living.

### Attack Vectors

- **Attack vector:** the method that the attacker will use to gain access to your computer or your network.
- With many operating systems, you can reboot the system into a particular administrative mode, make a change to an administrative password, reboot again, and now you have full access to the operating system.
- **keylogger to a keyboard:** are usually directly on these servers, and the administrators typing in their usernames and passwords, will remain on that system for a certain amount of time, and then the attacker will stop back by, remove the keylogger, and then take it somewhere else to see exactly what everyone typed into that keyboard while that keylogger was attached.
- **portable media** you can simply connect a flash drive or some other type of portable media.

### Threat Intelligence

- **OSINT or Open-source intelligence** This may be directly from the internet and discussion groups, or social media sites, or it may come from a governmental organization.
- One popular database is the **Common Vulnerabilities and Exposures database or CVE**.

## Threat Research

- **Threat research:** researchers attempt to discover the tactics, techniques, and procedures (TTPs) of modern cyber adversaries.
- **Honeynets:** to try to observe how hackers interact with vulnerable systems.
- **Dark net:** a network established as an overlay to Internet infrastructure by software, such as The Onion Router (TOR), Freenet, or I2P, that acts to anonymize usage and prevent a third party from knowing about the existence of the network or analyzing any activity taking place over the network, Onion routing, for instance, uses multiple layers of encryption and relays between nodes to achieve this anonymity.
- **Dark web sites** content, and services accessible only over a dark net, while there are dark web search engines, many sites are hidden from them, Access to a dark web site via its URL is often only available via "word of mouth" bulletin boards.

## 1.6 – Vulnerabilities

### Vulnerability Types

- There are many ways for attackers to find their way inside of your network:
  - The applications vulnerabilities inside of them.
  - leave the door open.
  - leave our accounts open.
  - Misconfiguration.
  - Error message pop up on the screen.
  - Using any outdated hashes, like MD5.
  - Protocols, such as Telnet, FTP, SMTP, and IMAP.

### Third-party Risks

- Because these integrators are on the inside of the network, they’re past the firewalls and the security devices that we commonly put on the perimeter.
- The production services should be on a separate, isolated part of the network, and the development team should not have access to the production site of the network.

### Vulnerability Impacts

- Data loss.
- Financial loss.
- Reputation loss.
- If you don’t lose any data and you don’t lose any money, you could still lose uptime and availability.

## 1.7 – Security Assessments

### Threat Hunting

- Trying to prevent anyone from getting into the network and you can’t stop them until they try to break into the network. The goal then is to speed up this reaction time or perhaps prevent the attack from occurring before the attacker even arrives on your network.

### Vulnerability Scans

- **Vulnerability scan**: determine from the outside if there is the potential to gain access to those systems.
- **Port Scan.**
- **Non Credentialed Scan**: does not have access to the network.
- **Credential Scan:** scans as a user who has rights and permissions to log in.
- **False Positives**: vulnerability scan has positively identified this vulnerability. But after doing research, we find that positive indication was actually false.
- **False negative:** This is when a vulnerability exists on a system but our scanner was not able to identify it and did not tell us anything about that vulnerability existing on that particular device

### Security Information and Event Management

- **Security Information and Event Management Device (SIEM):** is designed to collect information from anything on the network that can create log files, security alerts, or any type of real time information that can tell us about what’s happening on the network right now.
- **Security Orchestration Automation and Response (SOAR):** The goal of SOAR is to take these processes in security that were manual or tedious and automate them so that all of it is done at the speed of the computer.

## 1.8 – Penetration Testing

### Penetration Testing

- Trying to gain access to a system and exploit the vulnerabilities.
- It's important have permission to exploit the vulnerabilities that are on that system
- Type of penetration tests:
  - knows everything about the environment.
  - Unknown environment.
  - And it could be a mix of known and unknown.

### Reconnaissance

- Gather information about the systems that will be attacked.
- **Create a network map**: This may be able to build out an understanding of IP address schemes, the locations of certain devices and perhaps specific VLAN the different devices may be located on.
- **Passive Footprinting** (might be to look at social media pages, corporate website …).
- Another source of data for your passive footprinting might be wardriving or warflying. This is where we're combining Wi-Fi analysis with GPS locations to be able to know exactly where a wireless network might be.
- **Active Footprinting** (gather this information will commonly perform ping scans, port scans, analyze DNS information from the local DNS servers).

### Security Teams

- **Red team or offense or ethical hacking:** These are folks that are performing the penetration test themselves. they're working for us, to try to find the holes that might be in our network.
- **Blue team or defense:** trying to protect themselves against the attacks coming from the red team.
- **Purple team or both red team and a blue team:** both sharing information about what they find on the network, and that way they're able to fix the applications, secure the data and make sure that everything remains secure that much faster.
- **White team:** manager of both red team and a blue team: a particular set of processes, so they can enforce any rules that may be in place between the red team and the blue team.

# Section 2 - Architecture and Design

## 2.1 – Enterprise Security

### Configuration Management

- Document all of these updates and changes so that you have a way to look at where the configurations are for all of these systems.
- Part of the documentation you'll create will be the network diagram.
- Document the way the application is designed.

### Protecting Data

- **General Data Protection Regulation (GDPR):** rules in the European Union. if data is collected on EU citizens, that data must be stored in the European Union.
- **Data Masking:** This is a way to obfuscate data that makes it more difficult to read.
- **Encrypting Data or Ciphertext**: information that we created after the encryption process.
- **Confusion**: information into ciphertext different than in plaintext.
- **Diffusion**: if change one piece of information in the plaintext, ciphertext resulting is going to be dramatically different between these different versions.
- **Data at Rest:** data on a storage device. So this could be a hard drive, an SSD, NMVME, M.2 drive.
- **Data in Transit or Data in Motion**: data that's moving across the network.
- **Data in Use:** data that's in our system RAM, our CPU registers, or the caches that are on our system.
- **Tokenization:** show a completely different data than what was originally there. simply replacing one set of numbers or characters with another set of numbers or characters.
- **Information Rights Management (IRM):** is used to prevent certain things from occurring within document. prevent copying and pasting, controlling screenshots, managing the printing process.

### Data Loss Prevention

- **Data Loss Prevention (DLP):** able to look in different locations and protect our data from prying eyes.
- **DLP network:** that's examining all of the packets going across the network.
- **DLP hardware:** able to allow or disallow access to data that's being stored on a USB-connected drive.
- **DLP cloud:** able to look for all of the traffic going.
- **DLP email:** able to prevent to send and receive emails sensitive.

## Managing Security

- That trusted certificate authority has to sign the certificate for that web server, and that is the certificate the web servers providing to you.
- Hashing is used during encryption, digital signatures, and other processes for cryptography. We often refer to that short string as a message digest. This hashing process is a one-way trip.

## Site Resiliency

- Some disaster recovery locations are what we call:
  - **Hot Sites:** have duplicate hardware, servers, all of the equipment and infrastructure is duplicated.
  - **Cold Site:** This is effectively a room with a bunch of racks in it, and it has none of your equipment currently in place, none of your data, and none of your applications. This means that you'll need to bring the data with you. Maybe there are backup tapes or backup drives that are used.
  - **Warm Site:** is middle between a hot site and a cold site. Instead of being immediately ready to go or having nothing available, it's usually a location that has racks and some equipment that you can at least get up and running in a relatively short period of time.

## Honeypots and Deception

- **Honeypot**: is a system designed to look very attractive to an attacker. the attacker will try to gain access to these fake honeypot systems that are on your network. is effectively a virtual world, you could use Kippo, Google Hack Honeypot, Wordpot.
- **Honeynet:** Adding more honeypots to your network. You may find that an attacker starts on one server and goes to others. Or you may find that multiple attackers arrive at one time performing different functions on different honeypots.
- **Honeyfiles:** put inside of your honeypots and your honeynets.
- **DNS sinkhole:** Another useful tool for a security professional, however, performs the opposite of DNS process. When the client requests the IP address of a particular FQDN, this device gives a response back with incorrect or invalid information about that service.

## 2.2 – Virtualization and Cloud Computing

### Cloud Models

- **Infrastructure as a Service (IaaS) or hardware as a service (HaaS):** providing you hardware required to get your services up and running. You are responsible for the operating system, application, security.
- **Software as a Service (SaaS):** You simply log in and use the application as it's running on that service.
- **Platform as a service (PaaS):** provider you a platform to develop your own applications. They would provide the OS, the infrastructure underneath, some virtualization services, and would provide you with the building blocks you need to write your own applications that are customized just for you.
- **Anything as a Service (XaaS):** any type of service that is provided over the cloud.
- **Managed service provider (MSP):** provide things like network connectivity management, backups and disaster recovery planning, growth management and planning.
- **Managed security service provider (MSSP):** focuses on IT security so they may manage your firewall, patch management, security audits, emergency response services.
- **Public cloud service:** service available on the internet for anyone on the internet to be able to access.
- **Private cloud service:** service internal in your own data center that only you would have access to.
- **Hybrid cloud:** which would be a mix between those public cloud models and the private cloud models.

### Edge and Fog Computing

- **Edge computing:** decisions being made from the data created by these applications are all occurring on the local system and don't have to go out to the internet. For example, a climate control system can look at the temperature in a room and determine if it should cool or heat the room based on what the current temperature might be.
- **Fog Computing:** It's a distributed cloud architecture that allows us to send information into the cloud for processing without requiring that all of this data be consolidated in one single place.

## Designing the Cloud

- **Thin Client or Virtual Desktop Infrastructure or (VDI):** provides enough computing power to be able to connect to a desktop that is running in the cloud.
- **Virtualization:** allows us to run many different operating systems on the same physical device.
- **Hypervisor:** management software to manage different OS that are running on this computer.
- **Containerization:** its application means we would have a single host operating system, and then we would use some type of **container software such as Docker**, to be able to run multiple applications simultaneously in their own separate sandbox, but not have separate host OS for each one of those.
- **Microservice:** Which uses APIs to break up the application into individual services.
- **Serverless Architecture:** this allows us to take the operating system completely out of the equation, and instead perform individual tasks based on the functions that are requested by the application.
- **Virtual Private Clouds (VPC):** this is a pool of application instances used for internal use.
- **Transit Gateway:** You can think of this Transit Gateway as a router that's in the cloud.
- **Service Integration and Management (SIAM):** this is the natural next step when you begin deploying these different application instances to multiple providers.
- **Service Integration and Management Console:** would allow you to bring all of those service providers into a single view, and allow you to manage them from one single interface.

## Infrastructure as Code

- **Infrastructure as code:** We're able to describe the application instance in a series of code that we can then deploy any time we'd like. This is very similar to writing code for an application.
- **Software Defined Networking (SDN):** we are separating the functionality of our networking devices into two planes of operation.
  - **Control plane:** which handles the management and ongoing configuration of the device
  - **Data plane:** is the part of the device that handles the actual operation.
- **Agile:** which means you can make changes dynamically at any time.
- **Software Defined Visibility (SDV):** this allows us to deploy next-generation firewalls, intrusion prevention, web application firewalls, and other security devices while at the same time being able to understand exactly what type of data is flowing between all of these systems.

## Virtualization Security

- **Self-contained:** everything happening within that virtual machine only happens as part of that VM and has no effect on any other VMs that might be running on that network.
- There is an attack type called a virtual machine escape that would allow someone on one virtual machine to be able to gain access to resources that are on a completely separate virtual machine. This is obviously a significant exploit, because these virtual machines should never be able to share resources between each other.

## 2.3 – Secure Application Development

### Secure Deployments

- **Sandbox**: isolated testing environment used by the developers to test different aspects of app.
- **Testing Environment:** developers can check to see if the features and functions of the application are working as expected.
- **Quality Assurance Team (QA):** since they are outside the scope of the development team, they can really put the application through its paces to see if it's working as expected.
- **Staging Environment:** this will perform a final test of the data.
- **Production Environment:** put the application into internet for the end users.

### Provisioning and Deprovisioning

- **Provisioning** is the process of making something available.
- **Provisioning an application**: then you're probably going to deploy a web server, a database server, middleware server and other configuration and settings to be able to use this particular application.
- **Elasticity:** ability to increase or decrease the available resources for this application.
- **Orchestration:** able to automate the provisioning and Deprovisioning of these applications.

### Secure Coding Techniques

### Software Diversity

- This means that the final binary file will be different every time you compile the application.
- If an attacker finds a vulnerability inside of this file in a person's machine, and they create an exploit for that vulnerability, they may find that they're not able to use that exploit on a different person's machine because it's running a different version of that file.

## Automation and Scripting

- For example, if we know that the storage area of log files for an application was to fill up, it would cause the application to fail. So we might want to constantly monitor that particular drive and make sure that it never gets to a point where it gets too full or too highly utilized.
- One important place to use this automation is when we are doing Continuous Integration (CI). This is when the application developers may constantly be updating an application and perhaps even merging it into a central repository many times a day.

## 2.4 – Authentication and Authorization

### Authentication Methods

- **Directory Services:** this is a central database that stores usernames, passwords, computers, printers, and other devices that might be connected to the network. like Microsoft’s Active Directory.
- Commonly use the Kerberos protocol or LDAP to be able to access that database from an external device.
- **Federation:** allow to authenticate to your network, using credentials that are stored with a third party.
- **Attestation:** hardware that is connecting into your network that you originally set up as something trustworthy, that is allowed access to your internal systems.
- **Remote Attestation**: we have checks that occur on that remote device, and that device will provide a report to a verification server, that will then allow that device access to the network or prevent access to the network. This attestation report is usually encrypted and digitally signed using keys that are located on the Trusted Platform Module of that remote device.
- **Short Message Service (SMS) or text message:** less secure than other methods.
- **Particular application Installed:** This is a push notification, relatively safe process and probably more secure than something like SMS.
- **Pseudo-Random Token:** usually about 30 seconds and after that 30 second period is over; a new number is generated.
- Many of these token generators use a functionality **called TOTP that stands for Time Based One Time Password algorithm.**
- **HOTP or HMAC-based One-Time Password algorithm** you have a number that you would use one time during the authentication process

## Biometrics

- **Biometric authentication:** factor refers to something you are like: fingerprint, retina, iris of our eye, voice, facial recognition, gait analysis, vascular.
- **False Acceptance Rate (FAR):** This is how often your biometric system will approve an unauthorized user by looking at these biometric values. This is obviously not something you would want to have happen on your network, so it's common to increase the sensitivity of the biometric reader so that you can decrease the false acceptance rate.
- **False Rejection Rate (FRR)** This is someone who is authorized to get into the system, they put their finger on the fingerprint reader of the biometric system and instead of getting a green light, they get a red light. Even though they are authorized, they are now rejected from that biometric reader.
- **Crossover Error Rate (CER):** This is an area where we have minimized the number of false acceptance rates, and we've minimized the amount of false rejection rates, and effectively gotten both of those down to an equal level.

## Multi-factor Authentication

- **AAA framework** this is authentication, authorization, and accounting.
- **Authentication:** proven that you are who you say you are.
- **Authorization:** what you would have access to.
- **Accounting:** This is keeping track of exactly who may have authenticated onto a network.
- When we are authenticating into a system, there are a set of factors that we would use: Those three factors are something you know, something you have, and something you are.
- You can add on to those factors, some attributes. Those attributes would be somewhere you are, something you can do, something you exhibit, and someone you know.
- **Something you know is**: password, PIN, pattern.
- **Something you have**: smart card, USB token, your phone.
- **Something you are**: this is a biometric factor: fingerprint, an iris scan, voice print.
- **Somewhere you are:** geographically, use IPv4 addressing to determine where a person might be, GPS.
- **Something you can do**: signature.
- **Something you exhibit:** gait analysis way that you walk.
- **Someone you know.**

## 2.5 – Resilience

### Disk Redundancy

- Duplicate parts of a system so that it's always up and running, and available for the users.
- The goal is for the organization to continue operating even failure with part of the systems.
- Another way to maintain the uptime and availability is to create redundancy in a different geographic area.
- **Redundant Array of Independent Disks (RAID):** create redundancy with the drives themselves, this way if you lose one of those physical drives, you have separate pieces of that data stored on other multiple drives as part of that array.
- When a drive fails in a RAID array the users usually don't know that any problem has occurred. The RAID array continues to be up and running, and all of the data continues to be available.
- **RAID 0:** is no redundancy whatsoever; it's usually called striping without parity. but if you lose any drive in that RAID 0 array, you've also lost the data. and there's no redundancy available.
- **RAID 1:** is what we call mirroring, where we can take one physical drive, and duplicate all of the data on that physical drive to a separate physical drive. if we lose any one of those drives, all the information continues to be available and accessible on that separate drive.
- **RAID 5:** where we have striping with parity where we're putting pieces of information on separate physical drives, and then on a last physical drive we're putting some parity information. If we lose any of the drives on that particular array, it will rebuild the data based on the parity information that's put on that extra drive.
- There are combinations of RAID that you can choose, RAID 0 + 1, or 1 + 0, RAID 5 + 1, and other combinations as well. By combining these RAID types together, you can customize the redundancy for your purposes. And you'll be prepared regardless of what physical drive might fail.

### Network Redundancy

- To maintain uptime and availability on the network include a load balancer in infrastructure.
- **Network Interface Cards (NIC teaming) or Load Balancing Fail Over (LBFO):** provide redundancy to a server and allows us to plug in and use these multiple connections to a server, but instead of having a primary connection and a standby connection, we can use both of those connections simultaneously and aggregate the bandwidth between both of them.

## Power Redundancy

- **Uninterruptible Power Supply (UPS):** This is a device that has batteries inside, and if the power goes out, we use the battery power instead of using the primary power source. temporary power source.
- Three different kinds of uninterruptible power supplies:
  - **Offline or Standby UPS:** the simplest and least expensive, If the UPS recognizes that the power source is gone, it will switch over to battery power. So there’s a short time frame between the time when power is lost and then power is made available from the UPS.
  - **Line-Interactive UPS:** If the voltage is slowly diminishing on the line, the UPS can slowly ramp up the amount of power being provided by the batteries.
  - **Online or Double Conversion UPS:** complex and the most expensive, if the power does go out there’s no switching process, because you’re already on battery power.
- **Generator** is a long-term power backup that can keep the power running for days.
- **Power Distribution Unit (PDU):** provides multiple power sources. And each one of those interfaces can be controlled across the network. These PDUs also have monitoring capabilities. So they can report back if there are any type of power problems.

## Replication

- **Storage Area Network (SAN):** is high performance storage with built in redundancy and we’re usually able to access this over very high speed network. Not only does this allow multiple front ends to this data store but we can also replicate the data between storage area networks.
- If real-time replication of data between SANs isn’t available, you can create a SAN snapshot.
- **Snapshot:** will take data from one storage area network. Take the exact makeup of that data and then copy that data to a separate storage area network.

## Backup Types

- **Archive Bit or Archive Attribute**: this archive bit is turned on whenever a file is modified.
- **Full backup:** back up every single file on the system, Once the backup is complete, the archive bit is cleared, signifying that no changes have been made to that file since the last backup.
- **Incremental backup**: occur after the full backup has occurred, and it will back up all of the files that have changed since the last incremental backup.
- **Differential backup**: occurs after a full backup, but the only files that are backed up are the ones that have changed since the last full backup.
- **Magnetic Tape**: this is a sequential storage device. one advantage to tape is that it's relatively easy to store and very easy to ship around.
- **Disk backups**: faster medium to use if you're writing or reading from that drive. And it's also a method that can be used with deduplication and compression of data.
- When you're storing files to a drive over the network:
  - **Network Attached Storage (NAS**): refer to a NAS as file-level access, provides access to a large storage array that's connected over the network. if you need to change any portion of a file on that NAS, you have to rewrite the entire file on that device.
  - **Storage Area Network (SAN**): separate storage drive on your system, it provides block-level access means if you need to change a single portion of a very large file, you only need to change that portion on the disk instead of having to rewrite the entire file to the SAN.
- **Image backup:** back up everything that is on a computer and create an exact duplicate or replica of that entire file system. This means we're backing up the operating system, the user files….
- **Offline backup:** backing up your local devices to this backup component. It's usually something that performs very quickly, and it's over a secure channel.
- **Online backup**: is one that is constantly accessible and constantly updated throughout the day. This is one that occurs over the network, usually over an encrypted channel. Since this backup is always online.

## Resiliency

## 2.6 – Embedded Systems

### Embedded Systems

- **Embedded system**: is a computer and software that has been built for a very specific purpose and does not have any capabilities outside of that scope. running on a **System on a Chip (SOC).**
- May be a single chip which handles multiple functions on that single board.
- **Field-Programmable Gate Array (FPGA):** A common type of hardware that you'll find on embedded systems. It provides a lot of flexibility for the developer, if they want to add new capabilities or modify the functionality of the device, they can simply add new software which will reprogram the FPGA.
- **Supervisory Control and Data Acquisition System (SCADA) or Industrial Control System (ICS):** if you are in a power manufacturing facility all of that equipment can be networked and controlled from a computer using this SCADA network.
- **Real-Time Operating System (RTOS):** OS designed to work on a very deterministic schedule.

### Embedded Systems Communication

- **The fifth generation of cellular communication is 5G**: provide high speed communication over wireless networks and can use high frequencies to be able to get speeds that are upwards to 10 gbps.
- **Subscriber Identity Module (SIM).**
- **International Mobile Subscriber Identity (IMSI):** allows the mobile network provider to be able to recognize this SIM card and be able to add it to the cellular network.
- **Narrowband connection:** If the embedded device is not using the cellular network to communicate, then it may be using communication across a very narrow range of frequencies.
- **Zigbee:** communicating over wireless networks.

### Embedded Systems Constraints

- Not a fully capable computer. NOT have access to the hardware software.
- limited number of features available. limitation in the type of communication.
- Difficult to upgrade.
- limitations over the CPU so no additional cryptography hardware
- The geographical location.

## 2.7 – Physical Security Controls

### Physical Security Controls

- **Barricade or a Bollard:** These are used to prevent people, car from accessing a particular area.
- **Access Control Vestibule:** managing access to the data center to control who may be allowed access.
- **Alarm System, Provide Signage, Security Guard, RFID badges, Lighting, Drones.**
- **Video Surveillance:** this is sometimes seen as a CCTV or closed circuit television.
- **Cable lock to a laptop, USB data blocker, Fences, Opaque Fence.**
- **Faraday cage:** prevents radio signals from traversing through this particular cage.
- **Demilitarized Zone or a DMZ.**
- **Protected Distribution System (PDS):** This means that all of your cables and fibers that are on your networks may be inside of a metal conduit.

### Secure Areas

- **Air Gap:** is a way to provide a physical separation between devices or between networks. This might be a common way to prevent access between a secure network and an insecure network.
- **Vault or an entire secure room.**
- **Safe.**
- **The hot and the cold aisles** that are used in that data center.

### Secure Data Destruction

- Physically destroying the drives better idea than simply throwing them out with the trash.
- If you're throwing out printed material, you want to be sure that your garbage facility is secure.
- Shred all of these important documents or Burn any of the documents.
- Pulp this paper or removing the ink from the paper and recycling the paper.
- Shredder or a Pulverize hard drive or simply use a drill to put a hole directly.
- Use a strong magnetic field which is a degausser hard drive would never be able to be used again.
- Incinerate your digital information.
- Purge on that data.

## 2.8 – Cryptographic Concepts

### Cryptography Concepts

- Cryptography provide Confidentiality, Authentication, NON-Repudiation, Integrity.
- **Cryptanalysis:** art of cracking the encryption that already exists.
- **Key Stretching or Key Strengthening:** take small encryption key and find ways to make it larger. For example, we could hash a password and then hash the hash of the password.
- There are a number of libraries that already exist to do this. For example**, the bcrypt library.**
- **Bcrypt:** uses the Blowfish cipher to perform these multiple rounds of hashing on the plain text.
- Another common **key-stretching library is the PBKDF2**. This is the **password-based Key Derivation Function Number Two.**
- **lightweight cryptography:** a type of cryptography that's focused on providing these cryptographic functions without having a high-end CPU, and without using a lot of power.
- **homomorphic encryption (HE):** during encrypted data, difficult to perform action to that data.

### Symmetric and Asymmetric Cryptography

- **Symmetric Encryption or secret-key algorithm or a shared secret:** use a single key to encrypt and decrypt the data. requires relatively fewer and it's difficult to scale.
- **Asymmetric Encryption or public-key cryptography**: use multiple keys public key and a private key.
- **Private key as the name implies:** is the key that only you have access to.
- **Public key:** This is the key that you give to everybody.

## Hashing and Digital Signatures

- **Hash referred to as a message digest**: is designed to take any type of input and create a very specific unique string of text that's associated with that input.
- This hash is a one-way trip and its perfect solution for storing passwords.
- **SHA256 hash:** which is a 256-bit hashing algorithm.
- Usually don't use MD5 to be able to perform a hash because collision.
- **Salt:** add some randomization during the hashing process, useful for digital signatures.
- **Digital signatures**: allow us to send information to another party and have that person confirm that what they received is exactly the information that we originally sent.
- Digital signature is created with the private key it's verified with the public key.

## Cryptographic Keys

- **Symmetric encryption** tends to see keys that are about 128-bits or larger.
- **Asymmetric keys** using very large keys tend to be 3,072 bits 4,096 bits or even larger.
- **Out-of-Band Exchange:** where you might want to call someone on the telephone or use a carrier to send that key from one person to another. It's out-of-band because you are transferring this key outside of the network.
- use asymmetric encryption to be able to send a symmetric key to someone else.
- **Diffie-Hellman key exchange**: Another way to share a symmetric key between two devices without sending that symmetric key over the network.
- **Perfect Forward Secrecy (PFS**): this changes the encryption process so that you're not using the same private key every time.

## Steganography

- Obfuscation is the process of taking something that would commonly be relatively easy to understand and make it very difficult to understand.
- Steganography: type of obfuscation is used to hide information within an image.

## Quantum Computing

- **Traditional computers:** use classical mechanics which uses bits those bits are 0s and 1s.
- **Quantum computing:** have something called quantum bits, or qubits. These bits are not 1s and 0s, but they exist somewhere in the middle between 1 and 0.
- One place that quantum computing has a direct effect on technology with this scaling is cryptography.
- **NTRU:** this is a new way of performing encryption with quantum computing that instead of using very large prime numbers.
- **Quantum Key Distribution (QKD):** this allows us to send our encryption keys across the network to the other side without the worry of someone being able to intercept that key somewhere in the middle.

## Stream and Block Ciphers

## Blockchain Technology

- **Blockchain:** is a distributed ledger. It's a way to keep track of a particular event. This is something that many people can participate in, so that this ledger can be distributed throughout many different devices. Because this ledger is distributed across multiple devices, we can now have checks and balances. We can have an efficient form of processing these transactions, and everyone can see exactly what's happening on the blockchain.

## Cryptography Use Cases

## Cryptography Limitations

# Section 3 – Implementation

## 3.1 – Secure Protocols

### Secure Protocols

- **Real-Time Transport Protocol (RTP):** use for voice over IP or a voice over IP telephone.
- **Secure Real-Time Transport Protocol (SRTP):** encrypted version of real-time transport protocol.
- **POP 3 and IMAP:** send and receive email, both uses SSL.
- **Secure Sockets Layer (SSL)** newer version of SSL called TLS which is Transport Layer Security.
- Sending encrypted data over that connection it's using the HTTPS secure protocol that stands for HTTP over TLS or HTTP over SSL and sometimes you'll see it referred to as HTTP secure.
- **Internet Protocol security (IPsec)**: to communicate between two locations across the internet in a secure. form, then you'll need to use this protocol for encrypted tunnel. the tunnel using two protocols
- IPsec
  - **Authentication header or AH which provides the integrity.**
  - **Encapsulation security payload or ESP that provides the encryption.**
- Most common secure protocol for transferring files between devices:
  - **File Transfer Protocol Secure (FTPS): using SSL to provide the encryption.**
  - **SSH File Transfer Protocol (SFTP): using SSH to provide that encryption.**
- **Lightweight Directory Access Protocol (LDAP):** access to central directory that stored on the network.
- **LDAPS:** uses SSL to be able to communicate securely to an LDAP server.
- **Simple Authentication Security Layer (SASL):** LDAP uses SASL and it can communicate using Kerberos, client certificates, and other methods as well.
- **Secure Shell (SSH):** used to provide a terminal screen that is encrypting the information between the client and the server. SSH effectively replaces the older telnet protocol which was no encryption.
- **Domain Name System Security (DNSSEC):** update version of DNS, it gives us a way to validate the information we're getting from a DNS server.
- **Simple Network Management Protocol (SNMPv3):** querying your routers or switches for information in secure way.
- **Dynamic Host Configuration Protocol (DHCP):** to automatically assign IP addresses to the devices on our network. DHCP does not include any particular security functionality so we've added additional controls outside of the DHCP protocol. For example, with active directory you can avoid rogue DHCP servers by authorizing what devices are able to act as DHCP devices on your network.

# 3.2 – Host and Application Security

## Endpoint Protection

- **Antivirus and anti-malware**: most common security features that we might add to our devices.
- **Signatures:** pattern that may be within the file, memory that is being used by this malicious software.
- **Endpoint Detection and Response (EDR):** use other mechanisms to find malicious software other than just signatures. So instead of looking for a signature, we can look at what the file is doing.
- This EDR solution can often perform:
    - Root cause analysis to determine why this particular behavior occurred in the first place.
    - Find the code that was being used as that malicious software.
    - Isolating the system from the rest of the network.
    - Quarantine that malicious software into a different part of the operating system.
- **Data Loss Prevention (DLP):** is designed to stop data leakage. It's designed to prevent this sensitive data from being sent across the network in the clear or even set across the network in encrypted form.
- **Next-Generation Firewall (NGFWs):** you might also hear it called an application layer gateway, stateful multilayer inspection, or deep packet inspection.
- Next-Generation Firewall cannot only identify the applications running over the network, it can identify individual features within the application.
- **Host-Based Intrusion Detection System (HIDS).**
- **Host-Based Intrusion Prevention System (HIPS).**

## Boot Integrity

- **Boot process** would be a perfect place to try to get into an operating system and stay there.
- **secure boot, trusted boot, and measured boot**, which are all different parts of the boot process.
- **Hardware Security Modules (HSM).**
- **Trusted Platform Module (TPM):** designed to help with cryptographic functions that are used by applications within the operating system.
- You might also have memory on this **Trusted Platform Module** that's able to store keys.
- **TPM**: built an anti-brute force technology, so that you're not able to find the password.
- **TPM**: providing hardware security, BIOS provides the software security.
- **UEFI BIOS**: has a function within it called secure boot.
- **Measured boot process:** process to measure if any changes have occurred with the operating system.

## Database Security

- **Tokenization:** use it to protect data inside database.
- **Hash**: another way to store information secure in a database.
- **Salt.**
- **Rainbow Table:** is a pre-computed set of hashes and original values.

## Application Security

- **Quality Assurance (QA):** team to making sure the application is working and secure.
- **Normalization:** that process of checking and correcting the data that's being input.
- It's important that the application developer understand exactly what input is being used, and how that input is being handled by the application.
- Attackers use third party tools such as **fuzzers.**
- **Fuzzing:** is referring to a task called dynamic analysis where random data is simply being put into the input of an application. You may hear this referred to as fault injecting, robustness testing, syntax testing, negative testing.
- **Cookies:** another important security concern is the information stored on your PC from your browser.
- **Static Application Security Testing (SAST):** we can use the static code analyzers to go through the source code and identify places where there may be vulnerabilities such as buffer overflows, database injections, or other well-known types of attacks.

## Application Hardening

- **Firewall:** can limit what IP addresses and port numbers are accessible, and in some cases you can use a next-generation firewall to also limit the applications that can flow over that particular IP address and port number.
- **Windows Registry:** is a large database that contains configuration settings for the Windows operating system and the applications that run on that operating system.
- **Full Disk Encryption (FDE):** utility that is built into the Windows operating system, to prevent third party access to the data that we store on our computers is to use hard drives and storage devices that will encrypt the information that we're storing.
- If you are purchasing or implementing a self-encrypting drive, you want to be sure that drive follows the Opal standard.
- always keep the operating system up to date with the latest versions.
- Patch management.

## 3.3 – Secure Network Designs

### Load Balancing

- **Load balancing is** a way to distribute the load that is incoming across multiple device.
- The load balancer performing that SSL encryption and decryption in the hardware of this device.
- This load balancer might also **provide caching services**, **quality of service.**
- Many ways to configure the operation of a load balancer:
  - **Round-Robin Form**: assures that all servers are going to get exactly the same amount of load
  - **Weighted Round-Robin**: one of the servers would receive half of load, and the other servers would make up the rest of that load.
- load balancer needs to support **Affinity is defined as being a kinship or a likeness.**
- **Affinity:** means that a user communicating through that load balancer will always be distributed to the same server, this is usually tracked using a session ID or a combination of variables.

### Network Segmentation

- **Segmentation:** allowing or disallowing traffic between different devices. For example, we might have database servers that contain sensitive information and we may segment our users so they can't talk directly to those servers.
- **Physical Segmentation:** to keep devices separate from each other. For example, one switch may contain all of our web servers, and the other switch may contain all of our database servers. Challenges with this design is separately maintained, separately upgraded, and separately powered.
- **logical segmentation using VLANs or Virtual Local Area Networks:** can have customers on one part of the switch, and another customer on another part of the switch.
- **Screened Subnet or Demilitarized Zone (DMZ):** build a completely separate network to allows people to come from the internet usually they connect to a firewall, then redirects them to the screen subnet.
- **Extranet:** separate network designed as an extranet and we still have our internal network but we've built out this separate extranet for vendors, suppliers and has additional authentication.
- **Intranet:** because an intranet is only accessible from the inside of your network so you might be at your headquarters network, your remote site number one. The only way to access the intranet is if you are on an internal network already, or you're accessing the internal network through a VPN.

## Virtual Private Networks

- **Virtual private network (VPN):** send information between two points on the internet without anyone in the middle being able to understand anything that's being sent.
- **VPN concentrator:** device that's doing all of the hard work encrypting data sending out over the network and then decrypting anything that it happens to receive.
- VPN can be hardware devices or implemented as software.
- Browser that supports HTML5 will be able to use these capabilities for your SSL VPN.
- **Full Tunnel:** everything transmitted and sent to the VPN concentrator. The VPN concentrator will then decide where that data happens to go.
- **Split Tunnel:** the administrator of the VPN can configure some information to go through the tunnel and other information can go outside of the tunnel.
- Ways to send encrypted data over an IPSec tunnel:
  - **Transport Mode:** data are not encrypted.
  - **Tunnel Mode:** data are encrypted.

## Port Security

- **Port Security:** the goal is maintaining uptime, availability of the communication across the network.
- One challenge we have on our networks **is with broadcasts**. Broadcasts are packets that are sent from one device that are addressed to everybody else who happens to be on the network.
- **Broadcasts:** can also be malicious traffic, or unwanted traffic.
- **Switches:** can be used to control broadcasts.
- **Spanning Tree Protocol (STP):** standard for preventing loops on switch networks that is from the IEEE.
- Spanning Tree is also good at finding problems that occur.
- **Bridge Protocol Data Unit (BPDU)**: protocol used by the Spanning Tree Protocol.
- The switches control MAC filtering.
- **MAC filtering:** allows the administrator of this device to either allow or disallow traffic based on the Mac address that's communicating through the network.

## Secure Networking

- **Domain Name System Security**: ability to confirm the responses that we're getting from a DNS server.
- **Sinkhole Address**: we can tell our DNS server if a user ever tries to visit unknown malicious location, don't give out the actual IP address of that location instead give a different IP address.
- **Out-Of-Band Management** to work around problems that may be occurring on the network.
- **Physical Taps:** allow someone to disconnect a link, put the tap in the middle of the link and now they can receive a copy of all of the traffic going over the network.
- **Port Mirror or port redirection or switched port analyzer (SPAN):** is often a software base tapping mechanism that's usually built into a switch.
- **File Integrity Monitoring (FIM**): monitors files that would never change things like your OS files.
- **System File Checker (SFC):** type of on demand file integrity monitoring can be done with Windows. and **in Linux with the tripwire application.**

## Firewalls

- **Firewall:** This is a component that allows us to control the flow of traffic.
- **A traditional firewall:** is able to control traffic based on the IP address and port numbers.
- **Newer Next-Generation Firewalls**: identify the applications that may be flowing across the network.
- Very common for your firewall to act, as a layer 3 device.
- **Stateless Firewall:** firewall is not going to keep track of any of these flows going back and forth.
- **Stateful devices:** more secure and more intelligent, how they allow traffic through the network.
- **Unified Threat Management (UTM) or web security gateway**: newer version device of the firewalls. These devices include a number of additional features over simply being a firewall.
- **Newer Next-Generation Firewalls (NGFW)** devices or application layer gateways or stateful multilayer inspection devices, or deep packet inspection devices.
- **Web Application Firewall (WAF):** specifically built for web web-based applications, is going to allow or deny traffic based on the input to that particular application. Like SQL injection vulnerability.
- **Payment Card Industry Data Security Standard (PCI DSS):** use it if you're accepting credit card numbers to your website.
- **Access Control List (ACL) or security policy**: list of rules that the firewall will follow to decide whether information should be allowed or denied through the firewall.

## Network Access Control

- This edge connection is usually managed using rules that we put inside of that firewall.
- **Access control:** approaches the idea of allowing or disallowing access to the network, could be a user that’s on the inside of the network trying to access resources.
- These rules are different than the rules we might have in a firewall.
- **Bringing Your Own Device (BYOD):** we can perform a posture assessment to check security.
- **Dissolvable Agent**: not installing software this means that when we connect to the network, the software will run on that local device and perform that posture assessment. When that assessment is done, the software terminates and is no longer located on that machine.
- Device that can’t meet the minimum requirements for these posture assessments. In that case, the device is not allowed access to the network and very often is put into a quarantine network that is specifically built for devices that don’t pass their health check.

## Proxy Servers

- **Proxy Server** is a device that sits between the users and the rest of the network.
- **Proxy server** receives requests from the users, it creates its own request out to the service on behalf of the users, receives the response to that request, performs some type of security checks, it provides the answer to that request to the original user.
- **Proxy Server** perform caching, provide your URL filtering or content scanning.
- **Some proxy servers are configured to be explicit:** configuration of each of user’s devices and tell proxy servers located at a particular IP address and uses a particular port number.
- **Transparent Proxies:** users have no idea that proxy server sitting in the middle of the conversation.
- When we refer to proxies on a network its almost always an application level proxy.
- Proxy server that has support one or multiple applications.
- **Forward Proxy or Internal proxy:** used to control the users access to the internet.
- **Reverse Proxy:** users from the internet are hitting a proxy so they can gain access to internal services on your network.
- **Open Proxy:** installed on the internet for anyone to be able to use.

## Intrusion prevention

- **(IPS) and (IDS)** Designed to look at traffic going through your network identify any known attacks that may be inside of that traffic and block or mitigate those attacks in some way.
- **Intrusion Detection System (IDS):** is designed to alarm or alert if a problem occurs.
- **Intrusion Prevention System (IPS):** is designed to block information in real time.
- **Passive Monitoring System:** way to connect an IDS or IPS to your network is through a passive monitoring system.
- **If IPS is not in line** with the actual traffic flows from one device to another and If the IPS is in one of these passive modes cannot block that traffic in real time. If IPS identified malicious traffic it can send a TCP reset frame to these devices effectively disabling that particular traffic flow.
- Common implementation for an IPS is **to have the IPS in line on the** network evaluating all traffic that sent through it.
- **IPS is in-band it's** able to block the traffic in real time. And prevent any of the malicious traffic from getting inside the network.

## Other Network Appliances

- **Jump Server:** allows us to access usually internal devices through a private connection that we're making to a single device on the inside. No one would be able to gain access to that device except authorized users.
- **Hardware Security Module (HSM):** designed to help you manage and control these large number of keys and certificates in your environment. This is a device that is usually installed in clusters with redundancy.
- **Security Information and Event Management (SIME): tool** that is able to collect log files from switches, routers, servers, and almost anything else in your environment.

# 3.4 – Wireless Security

## Wireless Cryptography

- **Integrity Check or a Message Integrity Check (MIC):** sure that all of the traffic that we're sending across this wireless network is encrypted.
- The update to WPA2 security is WPA3.
- **Wi-Fi Protected Access 2 (WPA2).**
- **Wi-Fi Protected Access 3 (WPA3).**
- **WPA3 also includes perfect forward secrecy:** means that the session keys are created whenever we're performing the sessions, and once the session is over, the key is thrown away.
- **Simultaneous Authentication of Equals (SAE):** create a session key that's used on both sides of the conversation without actually sending that session key across the network.
- Sometimes hear this key exchange process referred to as the dragonfly handshake.

## Wireless Authentication Methods

- Two major ways to authenticate to a wireless network:
  - Everyone use the same password and we refer to this as a pre-shared key or shared passwords because we've created the key previously.
  - 802.1X: This provides for centralized authentication. So we're using RADIUS, TACACS or LDAP to be able to centralize everyone's username and password.
- The configuration for pre-shared key or 802.1X is usually configured on the wireless access point itself.
- **Captive Portal:** is a method of providing authentication using a separate login screen from your browse. and often have a time out function associated with them.
- **Wi-Fi protected setup (WPS):** allows different methods to be used for authentication.

## Wireless Authentication Protocols

- **Extensible Authentication Protocol (EAP):** Many of the types of authentication we'll use for wireless networks are built in it.
- **802.1X is also referred to as port-based Network Access Control (NAC):** this means that if you're trying to connect to the network, you don't gain any access to this wired or wireless network, unless you're providing the proper credentials using 802.1X.
- **Flexible Authentication via Secure Tunneling (EAP-FAST):** transfer information between each other over a secure tunnel.
- **Protected Extensible Authentication Protocol (PEAP):** Another form of an encrypted tunnel being used. using a digital certificate only needed on the server.
- **Microsoft's Challenge Handshake Authentication protocol (MS-CHAPv2):** authenticating to a Microsoft network.
- **Transport Layer Security (EAP-TLS):** performing a very strong encryption of data between our clients and our servers. requires digital certificates on all devices.
- **Tunneled Transport Layer Security (EAP-TTLS):** only needs a single digital certificate on the authentication server.
- **Federation** is when you can link a user's identity across multiple authentication systems.

## Installing Wireless Networks

- **Site Survey:** going to get information about the wireless infrastructure that may already be in place.
- **Heat Map:** one way to visually see the results of these site surveys. you would need to do is move around your building and have this system create, visually, where your wireless networks happen to be, and where the largest signal strengths might be for that network.
- To avoid any type of interference between access points, we need to make sure that access points that are near each other are not using the same frequencies.
- it's so important to perform your site surveys prior to an installation, so that you don't install an access point on the wrong channel, and create interference for all of the other devices on the wireless network.
- **Wireless Controller:** centralized management device, allows us to configure, update, and maintain all of the access points.

# 3.5 – Mobile Security

## Mobile Networks

- **One-to-one:** connection between the two devices communicating on that network.
- **Point-to-multipoint:** not necessarily full connectivity between all of these devices.
- **Cellular network that we use for mobile devices or cell phones:** popular wireless network type.
- **Bluetooth networks or a Personal Area Network (PAN):** used to connect our mobile devices and their accessories all to each other.
- **Radio-frequency identification (RFID):** used in access badge to gain access through doors at work.
- RFID chips inside: can track them and find them if they happen to get lost.
- **Near Field Communication (NFC):** technology that builds on RFID, this is a two-way wireless communication with two devices that are very close to each other. Like payment systems.
- **Infrared (IR):** connecting to some type of media center, or entertainment center, and you're able to control the devices on that entertainment center.
- **Universal Serial Bus (USB):** is a physical connection, connect to our mobile phones to transfer data, charge the devices.

## Mobile Device Management

- **Mobile Device Management (MDM):** management can be very important if users are bringing their own devices into the workplace and then we're putting sensitive company information on the user's own device.
- **Manage Applications:** good way to manage this application installation process is through the use of allow lists of known trusted applications.
- **Mobile Content Management (MCM):** to secure the data that's on these mobile devices.
- **Remote Wipe:** usually managed from MDM and allows you to click a button and erase all of the data on that device, even though we may not know exactly where that device happens to be.
- **Geolocation**: allows us to know where that device is physically located in the world.
- **Geofencing**: allows the mobile device to enable or disable certain features, depending on the location of where that device is at any particular moment.
- **Context-aware authentication**: combines different characteristics together to build a profile of who may be trying to authenticate to a particular device.
- **Containerization:** creating separate areas or partitions on the mobile device where we can keep private information in one partition and company information in another.
- **Full Device Encryption (FDE):** use to ensure that all of the data stored on that device is encrypted.

## Mobile Device Security

- **Hardware Security Module (HSM):** is a physical device that provides cryptographic features for your computer or mobile devices through a much smaller form factor of the HSM called a microSD HSM.
- This means that we can associate a piece of hardware with the cryptographic functions for encryption, key generation, digital signatures or authentication.
- **Unified Endpoint Management (UEM):** able to have exactly the same data available across all of devices. And to maintain security across all of devices.
- **Mobile Application Management (MAM):** manage the app that are running on those mobile devices.
- **Security Enhancements for Android (SEAndroid):** This is effectively taking the SELinux functionality and including it as part of the Android operating system.
- This provides some additional access controls security policies and includes different policies for configuring the security of these mobile devices.

## Mobile Device Enforcement

- **Rooting / Jailbreaking**: replace the operating system that's currently running on that system, with one that would allow you access to the operating system itself.
- Receiving updates over the air or OTA. This means that you don't have to plug it into your system, you don't have to download any software, all of these updates are automatically pushed down to your mobile device when they're ready.
- **MDM** is able to enable or disable the features of the camera. And it may configure them based on where you happen to be.
- **MDM** can also set security policies that might allow or disallow access to these flash drives from our mobile devices.
- **On-The-Go (USB OTG):** way to transfer data would not even use a flash drive, instead will simply plug in a cable between two devices to transfer information to your mobile device.

## Mobile Deployment Models

- **Bring Your Own Device (BYOD):** you may see this also referred to as bring your own technology.
- **Corporate Owned but Personally Enabled (COPE):** organization chooses what device you're going to carry around, this means you'll use it as a corporate device and a personal device, but you only have to carry around one device.
- **Choose Your Own Device (CYOD):** you get to decide the device that you're going to use, and then the organization purchases that device for you.
- **Corporate Owned:** organization owns the device and you can't use it for personal use. If you need your own smartphone for personal use, then you'll need to purchase one yourself and carry around both your personal smartphone and your corporate owned smartphone.
- **Virtual Desktop Infrastructure (VDI) or Virtual Mobile Infrastructure (VMI):** This means that all of your data is stored securely and separate from your mobile device.
- if you lose your mobile device, you're not losing any of that data. You can easily replace the mobile device and simply reconnect to that data store that's located somewhere else.

## 3.6 – Cloud Security

### Cloud Security Controls

- **Availability Zones (AZ):** referred to as a region within the cloud services.Each one would have independent power, a separate HVAC system, separate networking configurations.
- **Identity and Access Management (IAM):** This determines who gets access to a particular cloud resource. what they get access to.

### Securing Cloud Storage

- The permissions that we assign to the data were storing in the cloud is our first step in securing it.
- It's important to remember the data being stored in the cloud must have these permissions set.
- It's also common to have data replication in the cloud, encryption

### Securing Cloud Networks

- We can have virtual switches, virtual routers, and build an entire virtual infrastructure with different IP addressing, different routing configurations all within a cloud-based system.
- **private cloud:** only way that you'd be able to connect to those systems is using VPN.
- **Public Cloud.**
- **Hybrid Cloud.**

### Securing Compute Clouds

- **Rapid Elasticity:** very common way to maintain the uptime and availability of your cloud based applications

### Cloud Security Solutions

- **Cloud Access Security Broker (CASB):** enforce the security policies that we've already created with data that were storing in the cloud.
- **The CASB** is able to operate based on four primary characteristics.  visibility, compliance, threat prevention, data secure.
- One of the biggest concerns on application in cloud is a misconfiguration of the application itself.
- **Next-Gen secure web gateway (SWG):** this is going to provide security for all of our users.

## 3.7 – Identity and Account Management

### Identity Controls

- **Identity Provider (IDP):** when application is running in the cloud you need IDP service use it for authentication.
- IDP will be responsible for identifying and controlling users based on who the user name might be and what devices they might be using.
- There are many standards available that can help with this identity control, including SAML, OAuth and OpenID Connect.
- Attribute.
- Digital Certificate.
- **Secure shell (SSH):** allows us to get this command line prompt on these remote devices. But instead of using a username and password we might want to use public and private keys to be able to provide this authentication.
- To create the key pair, I'll simply run ssh-keygen.

### Account Types

- User Accounts.
- Shared Account.
- Guest Accounts.
- Service Account.
- Privileged Account: In Microsoft Windows, administrator is the privileged account. And in Linux, your privileged account is called root.

### Account Policies

- Perform Periodic Audits.
- Password Policies.
- Account Lockout Policy.
- Location Policies.

## 3.8 – Authentication and Authorization Services

### Authentication Management

- **Password vault:** store all of your passwords in one central secure area.
- The core database of this password manager would all be encrypted data.
- **Trusted Platform Module (TPM):** feature that's either part of the motherboard that you're using, or it might be a module that you can add to the motherboard. This is going to provide you with additional secure cryptography functions to be able to create random numbers or key generators from this Trusted Platform Module.
- **Hardware Security Module (HSM):** server has specialized hardware inside that allows it to perform cryptographic functions very, very quickly. This means this HSM can be used for centralized storage of all of our encryption and decryption keys.
- **Knowledge-Based Authentication (KBA):** you may find that you're asked for some very specific information that only you might know.
- **Static KBA**: some type of secret that we've previously configured in our system.
- **Dynamic KBA**: question that's being posed to you is not a question that you previously configured in the system.

### PAP and CHAP

- Common methods ways to provide authentication to a network, one is called **PAP and CHAP.**
- **Password Authentication Protocol (PAP):** designed for some very simple authentication, sends all of this information through the network in the clear.
- **Challenge Handshake Authentication Protocol (CHAP):** provide an encrypted challenge sent across the network, additional security, not sending the password in the clear across the network we're sending either a challenge or a response to that challenge, CHAP has a three-way handshake that occurs.
- **AAA server:** server designed to provide authentication, authorization and accounting, and it's going to provide a way to check a username and password to see if it's valid.
- **Microsoft CHAP (MS-CHAP):** used commonly with Microsoft's point to point tunneling protocol or PPTP, is a very weak type of encryption.
- we commonly do not use MS-CHAP or MS-CHAP V2 any longer. Instead, we prefer to **use L2TP, IPsec, 802.1X** or some other method of secure authentication.

## Identity and Access Services

- **Remote Authentication Dial-in User Service (RADIUS):** One of the more common authentication authorization and accounting protocols.
- This is a very common way to centralize authentication for your users, they could use RADIUS to be able to authenticate the username and password.
- **Terminal Access Controller Access-Control System (TACACS):** It is a remote authentication protocol.
- Cisco updated it to (Extended TACACS) that provided accounting and auditing.
- Latest version of TACACS which is TACACS+.
- **Kerberos:** more robust authentication method. is able to use single sign on.
- **Kerberos:** provides Mutual Authentication, which means you're not only authenticating to the server, the server is also authenticating to you.
- other methods that can provide single sign-on**, such as SAML, or smart cards, or even cloud-based** single sign-on services, but Kerberos is certainly one of the most popular you might find.
- **Network Access Control (NAC) or (802.1X) or port-based Network Access Control:** This means you can prevent people from accessing the network until they've gone through this specific authentication method.
- It's common to see 802.1X used with wireless network authentication, but 802.1X can also be used for wired authentication as well.

## Federated Identities

- **Federation**: this means that you can use authentication credentials that you already use and maintain without having to recreate additional login credentials for the site.
- **Security Assertion Markup Language (SAML):** it was designed to provide both authentication and authorization for users to access third party resources.
- SAML was never designed to be used for mobile applications.
- Common way to provide authentication and authorization for our mobile devices use these protocols **(OpenID Connect) and (OAuth).**
- **OpenID Connect**: is providing all of the authentication functionality.
- **OAuth:** is determining what types of data is accessible by that third party app

## Access Control

- **Mandatory Access Control (MAC):** we would assign these objects with labels such as confidential, secret, top secret, or perhaps others as well.
- **Discretionary Access Control (DAC):** you would create an object, and you, as the owner of that object, would assign rights and permissions to it.
- **Role-Based Access Control (RBAC):** This is associated with the role that an employee might have in that company. So this might be a technician. Or might be a manager. It could be someone responsible for a particular project. And they have been assigned rights and permissions based on their role.
- **Rule-Based Access Control:** The rule is generally associated with the object that they're trying to access.
- **Conditional Access:** this allows us to set certain conditions. We may check to see whether someone is an employee or whether they're part of a third-party organization or what type of application they're trying to access.
- **Privileged Access Management (PAM):** This is a centralized way to be able to handle elevated access to system resources.

## 3.9 – Public Key Infrastructure

### Public Key Infrastructure

- **Public Key Infrastructure (PKI):** is the process of managing practically every aspect of digital certificates, policies and procedures, the hardware and software, behind these digital certificates.
- Foundation for this PKI is the trust.
- Managing PKI have responsibilities:
  - creating the keys.
  - generating the certificates which associate these keys with a particular user.
  - safely and securely distribute those keys to their users.
- **Digital Certificates:** are public key that is combined with a digital signature.
- **Digital Signature:** is from the Certificate Authority.
- **Certificate Authority**: is the central point of trust.
- **Certificate Signing Request (CSR):** providing that public key to the certificate authority.
- **Registration Authority (RA):** process of identifying who the requester happens to be, they perform some validation of that requester, and then ultimately decide if that certificate should be signed.
- **Common Name (CN):** fully qualified domain name (FQDN) associated with the certificate.
- **Certificate Revocation List (CRL):** revoked certificate before they expire.
- **Online Certificate Status Protocol (OCSP):** another way to check the validity of these certificates.

### Certificates

- **Domain Validation Certificates (DV certificates):** is a certificate that allows you to encrypt communication to a web server.
- **Subject Alternative Name (SA):** allows to add many different DNS names into this certificate configuration.
- **Self-Sign Certificates:** own internal certificate authority to providing your own signatures to your internal certificates.
- **Computer Certificates:** if a device is connecting to your network you need that device is a trusted.
- **Email Certificates.**
- **User Certificates.**

## Certificate Formats

- **X.509 standard:** It’s a standard format for these digital certificates. And allows us to move these certs between different systems.
- **Distinguished Encoding Rules (DER) format:** format with set of rules that allows us to encode many different kinds of data.
- **Public Key Cryptography Standards number 12 (PKCS # 12):** transfer multiple certificates at one time. ( .P12 or .PFX file).

## Certificate Concepts

- We can have some CAs act as online CAs, and others certificate authorities might be offline CAs.
- **OCSP stapling:** able to determine if a certificate may have been revoked.

# Section 4 - Operations and Incident Response

## 4.1 – Security Tools

### Reconnaissance Tools – Part 1

Commands:

- tracert in Windows, traceroute in Linux, Unix, or Mac.
- nslookup / dig.
- ipconfig in Windows and ifconfig in Linux, Unix, or Mac.
- ping.
- pathping: ping + traceroute.
- netstat.
- arp.
- route print in Windows, netstat -r in Linux and Mac OS.
- dnsenum.

### Reconnaissance Tools – Part 2

Softwares:

- curl.
- IP scanning.
- Hping.
- Nmap.
- harvester.
- sniper.
- scanless.
- nessus
- cuckoo.

### File Manipulation Tools

Command:

- cat in Linux or Mac OS.
- head.
- tail.
- grep.
- chmod.
- logger.

## Shell and Script Environments

- **Secure Shell Command (SSH):** This provides for an encrypted communication channel so you can put in your username, your password.
- **Telnet:** sending this information in the clear.
- **PowerShells:** used by system administrators on Windows devices to be able to control almost every aspect of the Windows operating system. (.ps1 file extension).
- **Python:** scripting language that works across many different operating systems.
- **OpenSSL:** not really a shell or a scripting language but still has extensive use in our applications and operating systems today, is a library and a series of utilities that allows us to manage SSL or TLS certificates on our systems.

## Packet Tools

- **Wireshark:** has both graphical and text based packet capture capabilities, and it can provide us with a decode of every packet so that we can see exactly what information may be contained within this network traffic.
- **tcpdump**: utility command prompt, packet capture capabilities.
- **tcpreplay**: utility allows us to take the information that we've gathered and simply send it right back out our network interface card so that other devices on the network can see that traffic as well. This is a great way to test your security devices. also a good way to test firewall rules to see if the information you're sending through the network will either be allowed or denied access at the firewall.

## Forensic Tools

- **DD Command:** allows you to create a bit-by-bit copy of all of the information that may be on a drive or in a directory.
- **Memdump utility**: That will take all of the information and system memory and send it to a particular location on your system.
- Commonly store the memory dump somewhere outside of the system, we would commonly use Memdump in conjunction with Netcat, stunnel, openssl, or some other host that we would send to across the network.
- **WinHex utility in Windows:** This is a third-party editor that allows you to view information in hexadecimal mode, so you can pull out information that's located in a file, in memory, in disks that you may have, and be able to not only view, but edit that information as well. Also perform disk cloning capabilities and perform secure wipes.
- **FTK Imager:** utilities can capture images from other drives and be able to store them in a format that can be read it.
- **Autopsy tool:** able to search through that drive to find other pieces of information that is stored on a storage device, or in an image file, and it allows us to view and recover data from these devices as well.
- **Metasploit**: exploitation framework used to create custom attacks, where you build the attack type, and what's contained within it. it has a number of known vulnerabilities.
- **Social-Engineer Toolkit:** exploitation framework allows for spear phishing, website attack vectors, infectious media generators, and so much more.
- **Password Cracker:** able to perform brute force attacks to be able to identify those passwords.
- **Data Sanitization:** take an entire drive, clean it of anything that might be on it, and then use that drive again internally, or sell it on the open market. there's no way to recover it later.

## 4.2 – Incident Response

### Incident Response Process

- **Computer security incident handling guide:** NIST created a document that can help you understand the process you'd go through to handle these types of security incidents. This includes preparation, detection and analysis, containment, eradication, and recovery, and lastly your post-incident activity.

### Incident Response Planning

- Performing exercises to be testing yourself, and everyone in your organization, on what they would do if an incident occurs.
- **Tabletop exercises:** getting everyone around the table, being presented with a particular scenario, and then we're stepping through what we would do if this particular incident occurred, instead of actually performing the tasks.
- **Walkthrough:** allows you to test all of your processes and procedures, not only with the management of your organization, but with everyone who would be responding to this particular incident.
- Simulations like phishing attack or a password request.
- Stakeholders.
- Disaster Recovery Plan.
- **Continuity Of Operations Planning (COOP):** this is something that we would put together well before a disaster occurring, so that we know what to do if we don't have our normal systems in place.
- Incident Response Team.

### Attack Frameworks

- **MITRE ATT&CK framework:** you can identify broad categories of attacks, you can find exact intrusions that could be occurring, understand how those intrusions are occurring and how attackers move around after the attack, and then identify security techniques that can help you block any future attacks.
- **Diamond Model of intrusion analysis framework:** This guide is focused on helping you understand the intrusions that have occurred in your environment.
- **Cyber Kill Chain:** phases of cyber-attacks.

## 4.3 – Investigations

### Vulnerability Scan Output

- National Vulnerability Database, Microsoft Security Bulletins are place to get information vulnerability.
- **False positives**: are problems that don't exist at all miscategorized or misidentified as a vulnerability.
- **False negative**: vulnerability exists on that device but the vulnerability scan did not identify it.

### SIEM Dashboards

- **SIEM** can gather information from switches, our routers, our firewalls, and other device We can of course gather log files from operating systems like Windows or Linux, and have that information sent into the central SIEM database.

### Log Files

- **Event Viewer**: perform filter this information in operating system log files.
- Firewall logs.
- Web application logs.
- DNS server logs.
- Authentication log.
- **Dump Files:** we can create on demand log files.

## Log Management

- **Syslog**: standard methods for transferring log files from one device to a centralized database.
- **Linux has a utility called journalctl,** which allows you to query the information that's in that system journal and provide output on what may be contained in there. And you can search and filter on those details, or view it as plain text.
- **Bandwidth Monitoring:** shows you the percentage of the network that has been used over time.
- **Metadata:** is data that describes other types of data, and usually, metadata is contained within the files that we're using on our devices. Like if you take a picture or store video on your mobile device, it could keep in that metadata the type of phone that was used to take that picture or the GPS location where the picture was made.
- **NetFlow:** is one of these standardized methods of gathering network statistics from switches, routers, and other devices on your network. This NetFlow information is usually consolidated onto a central NetFlow server, and we're able to view information across all of these devices on a single management console.
- **IP flow information export (IPFIX):** This is the which you can think of as a newer version of NetFlow. It was one that was created and based on NetFlow version nine. This allows us with some flexibility over what data we would collect and what information would be reported to a centralized server. This is very similar to NetFlow, except we can customize exactly what kind of data we'd like to receive from those collectors.
- **sFlow or sampled flow:** where we're looking at a portion of the network traffic to gather metrics on.
- **Protocol Analyzer:** get detailed information of exactly what's going over your network.

## 4.4 – Securing an Environment

### Endpoint Security Configuration

- Applications are allowed or not allowed.
- Quarantine Area.
- Applications are approving Example: application hash, certificate, network zone.

### Security Configurations

- Firewalls.
- Mobile Device Manager (MDM).
- Data Loss Prevention (DLP).
- URL filter.
- Certificates update or revoke.
- Isolation.
- Containment.
- Segmentation.
- SOAR.

## 4.5 – Digital Forensics

### Digital Forensics

- **Digital Forensics:** describes the process of collecting and protecting information that is usually related to some type of security event.
- **RFC 3227:** is guidelines for evidence collection and archiving. And it's a great best practice to get an idea of what's involved with the digital forensics process.
- This RFC describes three phases for the digital forensics process: the acquisition of data, the analysis of that data, and the reporting of that data.
- One of the first notices you might get relating to digital forensics is something called a legal hold.
- **legal hold**: often describes what type of data needs to be preserved for later use.
- Another good source of information to gather would be in a video form.
- **Chain of Custody:** Anyone who comes in contact with this data or uses it for analysis, needs to document what they did with this chain of custody.
- Document the time zone information associated with the device that you're examining.
- Event logs.
- Interviews.
- Report.

## Forensics Data Acquisition

- Most volatile and then we'll work down to the data that is the least volatile.
- CPU registers or CPU cache.
- Router tables, ARP cache, process tables.
- Temporary file.
- Disk.
- Remote logging and monitoring data.
- Physical configuration and typology of the network.

## On-Premises vs. Cloud Forensics

- Cloud-based complex to the forensics process.
- Right to audit clause in the agreement.
- Regulations regarding the use and access to data.
- legal jurisdiction

## Managing Evidence

- Hash of that data.
- **Checksum:** this is very commonly done with network communication to make sure that the information that we've sent from one side of the network to the other has shown up without any type of corruption.
- Preserve this information and to verify that nothing has changed with this information while it's been stored.
- **Discovery:** Digital technologies (e-discovery).
- Recovering.
- Non-repudiation.

# Section 5 - Governance, Risk, and Compliance

## 5.1 – Security Controls

### Security Controls

- **Security Controls:**
  - **Managerial Control:** focuses on the design of the security or the policy implementation associated with the security. like security policies for our organization , standard operating procedures that everyone is expected to follow.
  - **Operational Controls:** managed by people. Like security guards , awareness program to let people know that phishing is a significant concern.
  - **Technical Controls:** use our own systems to prevent some of these security events from occurring. like implemented antivirus , firewall connecting you to the internet.

- **Control Types:**
  - **Preventive Control:** prevents access to a particular area. like locks, security guard ,firewall.
  - Detective Control: identifies and is able to record that a security event has occurred, but it may not be able to prevent access. like motion detector, IDS.
  - **Corrective Control:** is designed to mitigate any damage that was occurred. like IPS.
  - **Deterrent Control:** deter someone from performing an intrusion. like warning sign , login banner , lights around your building that might deter someone from breaking in.
  - **Compensating control:** attempts to recover from an intrusion by compensating for the issues that were left behind. Like if someone Stole a laptop with all of our data, we could compensate for that by purchasing a new laptop and restoring that data from backup. Or if someone cut the power to our data center, we could have backup power systems or generators that would compensate for that lack of power.
  - **Physical Control:** in the real world that would prevent the security event. like a fence or a door lock would certainly prevent someone from physically gaining access to our facility.

# 5.2 – Regulations, Standards, and Frameworks

## Security Regulations and Standards

- One of the reasons you're going to track this so closely, is that there could be significant penalties associated with not following these regulations.
- **General Data Protection Regulation (GDPR):** is a set of rules and regulations that allows someone in the European Union to control what happens with their private information.
- **Payment Card Industry Data Security Standard (PCI DSS):** series of guidelines that's administered by the payment card industry.

## Security Frameworks

- **Frameworks**: can help you understand the different security processes available, and they can help you understand what you need to do to follow those particular processes.
- Many of these frameworks can help you build security processes from scratch, or you can build on the processes that you already are using.
- **Center for Internet Security critical security controls (CIS CSC):** framework designed to help you improve the security posture of your organization, focused into critical security controls in 20 different areas, different recommendations depending on the size of the organization
- **National Institute of Standards and Technology Risk Management Framework (NIST RMF)**: if you handling data for the federal government and has six different steps:
  - **The first step** is to categorize or define the environment that you're working in.
  - **The second** is to select or pick appropriate controls for security and privacy.
  - **The third** is to implement or define the proper implementation of these particular policies.
  - **The fourth** is to determine if the policies you put in place are actually working properly, that is, the assess step.
  - **The fifth step** is the authorize step, where you make a decision to authorize a particular system,
  - **The sixth step** is to constantly monitor to ensure that you are still in compliance. This is an extensive framework, and it's available to download directly from NIST, the National Institute of Standards and Technology.

- **Cybersecurity Framework (CSF):** designed for commercial implementations, three major areas:
  - **The first** is the framework core identify, protect, detect, respond, and recover.
  - **The second** area is the framework implementation tiers: what their approach will be to cybersecurity, and what tools and processes need to be in place to manage the risks.
  - **The third** area is the framework profile, where policies, guidelines, and standards.

- **International Organization for Standardization, and International Electrotechnical Commission (ISO/IEC):** frameworks for international level.
  - **ISO/IEC 27001** which is a standard for Information Security Management Systems (ISMS).
  - **ISO/IEC 27002** which is a code of practice for information security controls.
  - **ISO/IEC 27701** which focuses on privacy with the Privacy Information Management Systems (PIMS).
  - **ISO 31000** risk management side.

- **Statement on Standards for Attestation Engagements System and Organization Controls (SSAE SOC 2):** auditing standard focuses on topics that can include firewalls, intrusion prevention, or intrusion detection, or multi-factor authentication.
- **cloud security alliance (CSA):** focuses on security in the cloud.
- CSA creates a cloud controls matrix framework (CCM) where they map controls to standards, best practices, and regulations that you need to follow in the cloud.

## Secure Configurations

- Default configuration is not secure.
- Manufacturer or the developer of the software can help you understand what configurations are safe for the system.
- **Web Server configurations:** how to prevent information leakage by adding banner information and disabling any type of directory browsing. provide best practices for understanding how this service should run in the operating system.
- **User accounts configurations:** should be a minimum password length and complexity.
- **Application Server configurations:** sure is up to date with the latest security patches, ability to perform the functions that it needs.
- **Networking Infrastructure configurations:** sure to check with the manufacturer so that you're running the latest software on these systems.

## 5.3 – Organizational Security Policies

### Personnel Security

- **Acceptable Use Policy (AUP):** documentation that covers how all of the different technologies in your environment should be used, telephones, computers, mobile devices, tablets, and anything else that is technology in your company.
- **Job Rotation:** help to minimize risk.
- **Require Vacations:** limit the ability of any one person to commit a type of fraud.
- **Separation of Duties:** split knowledge for safe combination.
- **Dual Control:** users have keys and to be able to open the safe both users have to turn both keys simultaneously.
- Clean Desk policy.
- Least Privileged policy.
- **Background checks:** if you want to hire that person.
- **Non-Disclosure Agreement:** This is a confidentiality agreement where both sides will agree what information can be shared, and what information should be kept private.
- **On-boarding process**: where we'll bring on a new person, or bring in a transfer to the organization. On the IT side, agreements that need to be signed such as the employee handbook, or an acceptable use policy, accounts to log in.
- **Off-boarding process:** turning in that equipment and verifying that it has been returned, disable the account.
- **Capture The Flag (CTF):** security related competition, a good way to keep your skills up and to be aware of some of the most recent vulnerabilities and attacks.

## Third-party Risk Management

- Important from a security perspective to understand the risk associated with providing that data to a third party.
- It may be useful to have a list of these security requirements in the original contract that you have with a third party.
- It may be useful to perform an assessment of the supply chain so that you understand the security risks.
- Understand what the best practices are for that connection between ourselves and the business partner.
- **Service Level Agreement (SLA):** sets a minimum set of service terms for particular service or product.
- **Memorandum of Understanding (MOU):** This is a memo that is sent between two different parties so that they understand what the requirements might be for a particular business process.
- **Measurement System Analysis (MSA)**: This provides a way for a company to evaluate and assess the quality of the process used in their measurement systems.
- **Business Partnership Agreement (BPA):** This provides details about what the owners stake might be, you can understand what the contractual agreement is for the finances.
- **End of Life (EOL):** not selling the product any longer, but they do continue to support the product.
- **End of Service Life (EOSL):** not selling the product, and no longer support the product.

## Managing Data

- **Data Steward:** person responsible for data privacy, data is accurate and ensuring data remain secure.
- **Data Retention:** process save different versions of a file, sometimes over a number of days or weeks.

## Credential Policies

- Always good to have two-factor authentication, or multi-factor authentication.
- Mobile Device Manager (MDM).
- It’s common to use different credentials for different services, depending on the access that they need to the operating system.

### Organizational Policies

- **Change Control:** formal process for making these changes, you can avoid unnecessary downtime confusion that may surround these changes and making mistakes during the change process.
- Once we understand the scope and the risks, we can create a plan for performing this particular update.
- One of the most important steps of this entire process is that you have a back plan.
- Once we make these changes we need to document everything so that we understand what the current state might be.

## 5.4 – Risk Management

### Risk Management Types

- Identify all of the assets.
- If you know the risk associated with the asset, you can then start making business decisions on how to better protect that asset.
- Handle application licensing.

### Risk Analysis

### Business Impact Analysis

## 5.5 – Data Privacy

### Privacy and Data Breaches

- It's important to understand the entire lifecycle of information.
- **Consequence:** damage reputation, identity theft, fines, intellectual property (IP).
- **Privacy Impact Assessment (PIA):** how these new processes or products will affect the privacy of our customers' data.
- This allows us to understand how the data flows will occur prior to implementing these particular projects.

### Data Classifications

- **Personally Identifiable Information (PII):** any type of data that could be tied back to an individual.
- **Protected Health Information (PHI):** any type of data health associated with an individual.
- Data have different levels:
  - **Public data - Unclassified Data**: anyone would have access to this information.
  - **Private - Classified - Restricted – internal**: should only be shown to certain individuals.
  - **Sensitive**: intellectual property or PII, PHI.
  - **Confidential**: view if you've been granted the correct permissions.
  - **Critical**: information that is publicly available.

### Enhancing Privacy

- **Tokenization:** take data that normally and we replace it with a completely different bit of data.
- **Data Minimization**: only collect data that would be used to perform the needed function.
- **Data Masking:** not display it.
- **Anonymization**: not displaying anything associated with that data.
- No way to convert back to the actual data once the information has been anonymized.
- **Pseudo-Anonymization - pseudonymization**: has a way to convert the data back if we need it.

### Data Roles and Responsibilities

- **Data Owner:** person in the organization who is responsible for a certain set of data.
- **Data Controllers:** responsible for the purposes and means by which the data is processed.
- **Data Processor:** working on behalf of the data controllers.
- **Data Custodians or Data Stewards:** responsible for the accuracy of the data, for keeping all of your data private, and the security associated with the data that's stored in your systems.
- **Data Protection Officer (DPO):** responsible for the organization's overall data privacy policies. define exactly what the privacy policies are for your organization, make sure processes are in place.