

CYBER SECURITY

IMPORTANT INFORMATION
SECURITY CONCEPTS

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer.

VIRUS

- A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Today, with different kinds of malware infecting the cyber world, computer viruses have become rather uncommon; they comprise less than 10% of all malware.

WORMS

- A worm is self-replicating and spreads without end-user action, causing real devastation. Viruses need end users to kick them off so that they can go on and infect other files and systems. On the other hand, worms don't need any such end-user action. They'd simply spread by themselves, self-replicating in the process and destroying systems, devices, networks and connected infrastructure as well.

TROJAN HORSE

- A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data, install more malware, modify files, monitor user activity etc.

ROOTKITS

- A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, etc. Rootkit detection can be very difficult.

RANSOMWARE

- It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange. Most ransomware programs are Trojans, which means they must be spread through social engineering of some sort. Once executed, most look for and encrypt users' files within a few minutes, although a few are now taking a "wait-and-see" approach.

KEYLOGGER

- Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send it back to a third party through mail or upload on a website. Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. Keyloggers are a form of *Spyware*.

GRAYWARE

- The term grayware was coined in September 2004 and describes unwanted applications or files that aren't malware but worsen the performance of the computer and can cause cybersecurity risk. At a minimum, grayware behaves in an annoying or undesirable manner and at worst, monitors the system. Malwares like *Adware* and *Spyware* fall under Grayware.

FILELESS MALWARE

- While traditional malware travels and infects systems using the file system, fileless malware travels and infects without directly using files or file systems. Such malware exploits and spread in memory only; they also spread using ‘non-file’ OS objects, like APIs, registry keys etc. Fileless malware attacks are harder to detect and stop.

ADWARE

- Adware is nothing but attempting to expose users to unwanted, potentially malicious advertising. These ads most likely end up infecting a user’s device. There are adware programs that redirect a user, during browser searches, to look-alike web pages that have promotions of other products. Removing adware is easier. You just need to find the malicious executable and remove it.

MALVERTISING

- Malvertising is the use of legitimate ads to covertly deliver malware to unsuspecting users' computers. For example, a cybercriminal might pay to place an ad on a legitimate website. When a user clicks on the ad, code in the ad either redirects them to a malicious website or installs malware on their computer. In some cases, the malware embedded in an ad might execute automatically without any action from the user.

SPYWARE

- The Spyware is malware that gathers information about a person or organization and sends the information to the attacker without the victim's consent. Spyware usually aims to track and sell your internet usage data, capture your credit card or bank account information or steal personally identifiable information (PII). Some types of spyware can install additional software and change the settings on your device. Spyware is usually simple to remove because it is not as nefarious as other types of malware.

BOTS & BOTNETS

- A bot is a computer that is infected with malware that allows it to be remotely controlled by an attacker. The bot (or zombie computer) can then be used to launch more cyber attacks or become part of a botnet (a collection of bots). Botnets are a popular method for distributed denial of service (DDoS) attacks, spreading ransomware, keylogging and spreading other types of malware.

BACKDOORS

- A backdoor is a malware that covertly bypasses the normal authentication or encryption in a computer, product, embedded device (e.g. router) or other part of a computer. Backdoors are commonly used to secure remote access to a computer or gain access to encrypted files. From there, it can be used to gain access to, corrupt, delete or transfer sensitive data. Backdoor malware is generally classified as a *Trojan*.

BROWSER HIJACKER

- A browser hijacker or hijackware changes the behavior of a web browser by sending the user to a new page, changing their home page, installing unwanted toolbars, displaying unwanted ads or directing users to a different website.

CRIMEWARE

- Crimeware is a class of malware designed to automate cybercrime. It is designed to carry out identity theft through social engineering or stealth to access the victim's financial and retail accounts to steal funds or make unauthorized transactions. Alternatively, it may steal confidential or sensitive information as part of corporate espionage.

BUGS

- A bug is a flaw in a piece of software which produces an undesired outcome. Minor bugs only slightly affect a program's behavior and as a result can go for long periods of time before being discovered. More significant bugs can cause crashing or freezing. Security bugs are the most severe type of bugs and can allow attackers to bypass user authentication, override access privileges, or steal data.

HYBRID MALWARE

- Today, we have malware that could be a combination of more than one stream of traditional malware. For example, some malware is part virus, part Trojan, and part worm. Such a malware might appear as a Trojan during the initial stage, after which it would perhaps spread like a worm.

TYPES OF ATTACKS

Social
engineering

Phishing
attack

Social
phishing

Spear phishing
attack

Watering hole
attack

Whaling

Vishing (voice
phishing or
VoIP phishing)

Port scanning

Spoofing

Network
sniffing

DoS attack
& DDoS attack

ICMP smurf
Denial of serv

Buffer
overflow
attack

Botnet

Man-in-the-
middle attack

Session
hijacking
attack

Cross-side
scripting attack
(XSS attack)

SQL injection
attack

Bluetooth
related attacks

*Denial of Service Attack

*Distributed Denial of Service Attack

SOCIAL ENGINEERING

- Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or get access to your computer to secretly install malicious software that will give them access to your passwords and bank information as well as giving them control over your computer.
- Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

PHISHING ATTACK

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

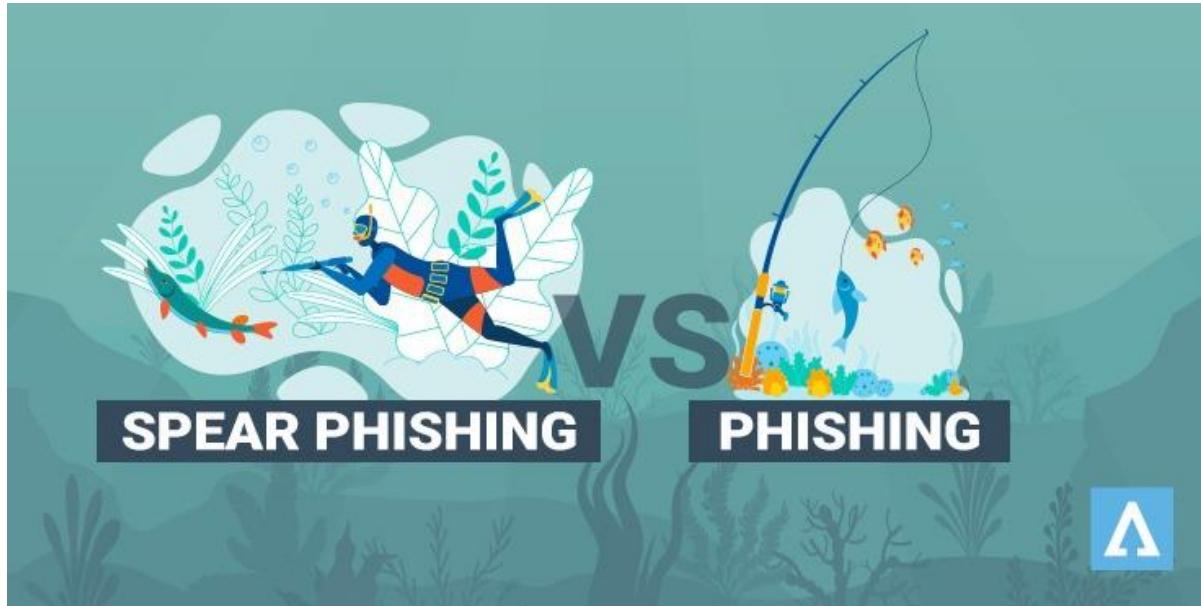
NOTE: Phishing attacks can also be done through phone calls or text messages. But emails are mostly used.

SOCIAL PHISHING

- In the recent years, phishing techniques evolved much to include social media like Facebook or Twitter. This type of Phishing is often called Social Phishing. The means of the attack may include special links or posts posted on the social media sites that attract the user with their content and convince them to click on them. The link redirects then to malicious website or similar harmful content.
- The websites can mirror the legitimate Facebook pages so that unsuspecting user does not notice the difference. The website will require user to login with his real information. At this point, the attacker collects the credentials gaining access to compromised account and all data on it.
- Other scenario includes fake apps. Users are encouraged to download the apps and install them, apps that contain malware used to steal confidential information.

SPEAR PHISHING ATTACK

- Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online. The attackers then disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging. This is the most successful form of acquiring confidential information on the internet, accounting for 91% of attacks.



WATERING HOLE ATTACK

- The name is inspired by the predators in the wild who prowl near watering holes, waiting for the opportunity to attack a potential prey. In a Watering Hole attack, the “predator” (Attacker) lurks on specific websites which are popular to its “prey” (target), looking for opportunities to infect them with malware making these targets vulnerable.
- In other words, rather than using a Spear Phishing email campaign to lure victims, hackers infect vulnerable sites that share a common interest to their targets, and then redirects the victim(s) to the attacker’s site which contains malware. The goal is to infect a victim's computer and gain access to the network within the victim's place of employment.

WHALING ATTACK

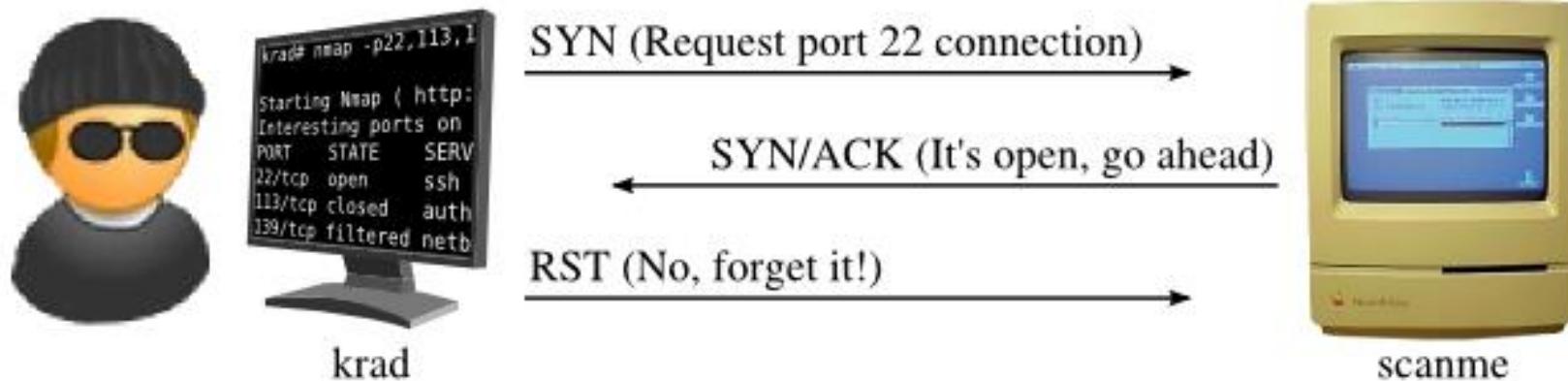
- A whaling attack is a method used by cybercriminals to masquerade as a senior player at an organization and directly target junior officials at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes.
- Also known as *CEO fraud*, whaling is similar to phishing in that it uses methods such as email, call or text to trick a target into performing specific actions, such as revealing sensitive data or transferring money. However, whaling differs from phishing in the fact that the attacker pretends to be a senior or influential person in the organization so that the junior officials are forced to accept the request.

VISHING ATTACK

- The word ‘vishing’ is a combination of ‘voice’ and ‘phishing.’ Phishing is the practice of using deception to get you to reveal personal, sensitive, or confidential information. However, instead of using email, regular phone calls, or fake websites like phishers do, vishers use an internet telephone service (VoIP).
- Using a combination of scare tactics and emotional manipulation, they try to trick people into giving up their information. These vishers even create fake Caller ID profiles (called ‘Caller ID spoofing’) which make the phone numbers seem legitimate. The goal of vishing is simple: steal your money, your identity, or both.

PORt SCANNING

- A port scan is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. It is also valuable for testing network security and the strength of the system's firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

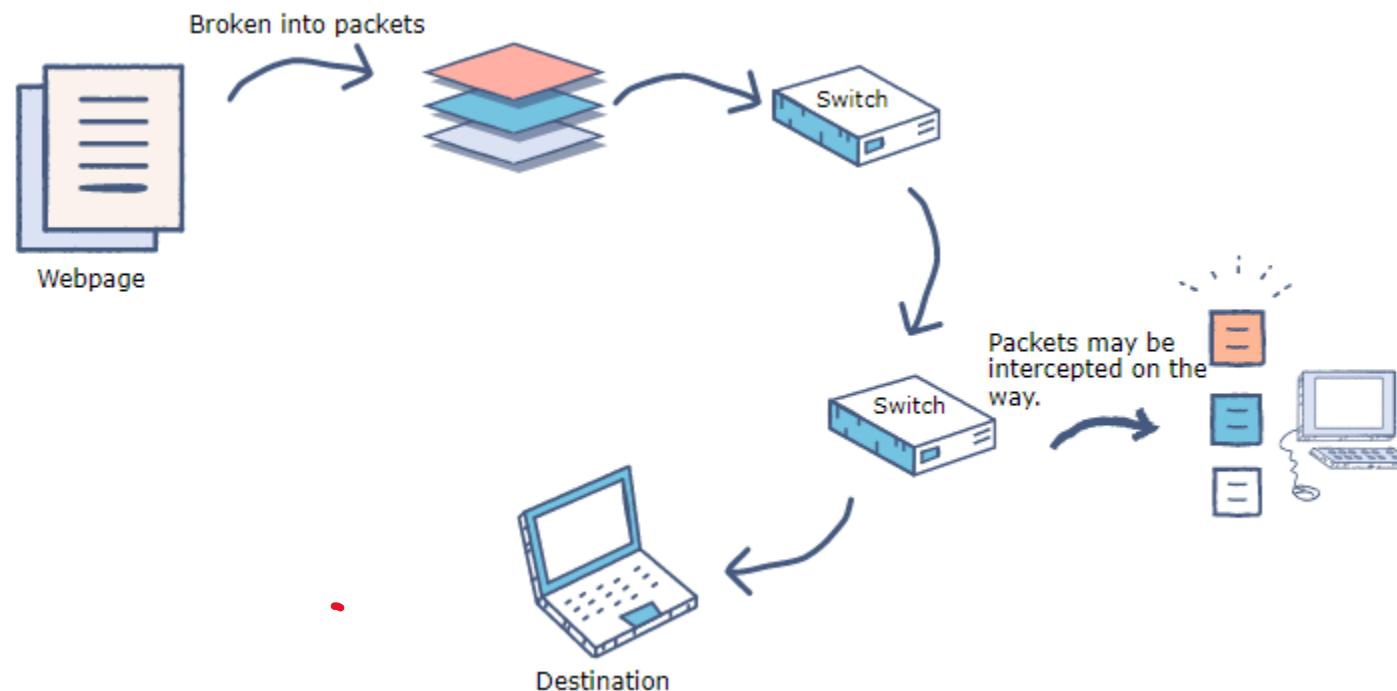


SPOOFING

- Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
 1. **ARP Spoofing:** In ARP spoofing attack, a malicious attacker links the hacker's MAC address with the IP address of a company's computer. This allows the attacker to intercept data intended for the company computer.
 2. **DNS spoofing (DNS Cache Poisoning)** – An attack where the wrong data is inserted into DNS Server cache, causing the DNS server to divert the traffic by returning wrong IP addresses as results for client queries.
 3. **IP Spoofing:** The most commonly-used spoofing attack is the IP spoofing attack. This type of spoofing attack is successful when a malicious attacker copies a legitimate IP address in order to send out IP packets.

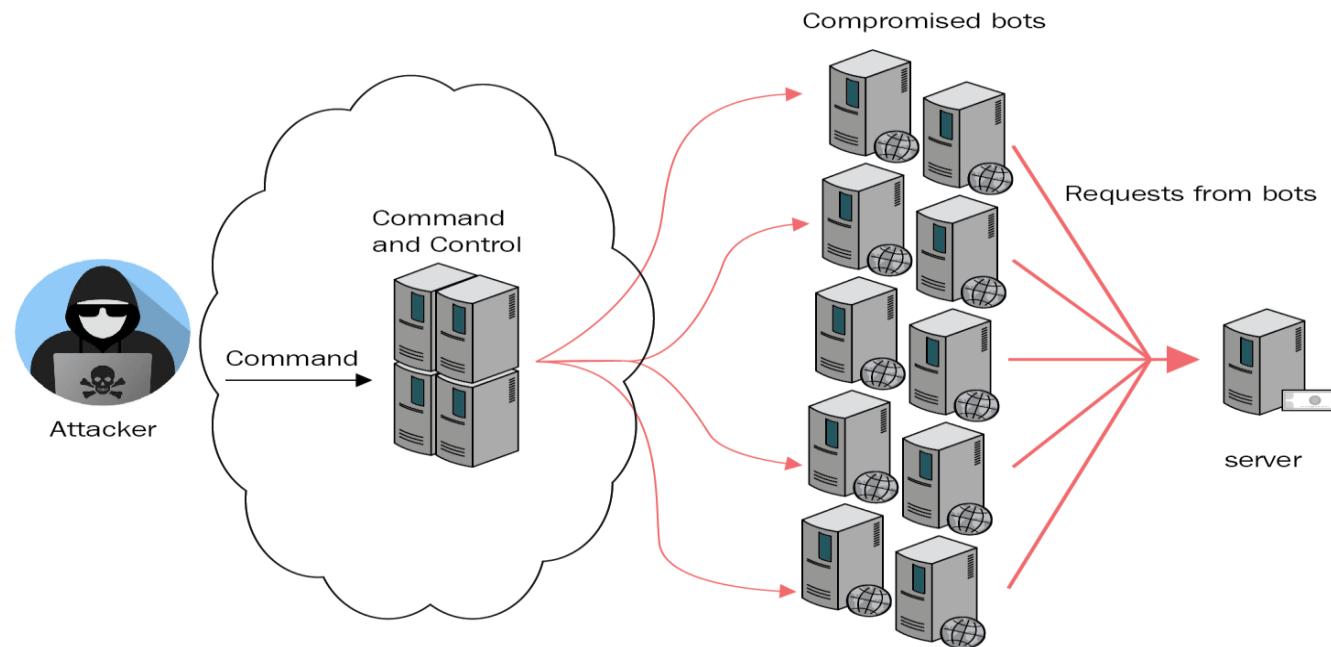
NETWORK SNIFFING (PACKET SNIFFING)

- It is the act of capturing packets of data flowing across a computer network. The software or device used to do this is called a *Network Sniffer*. Network sniffing can be used both by IT professionals to analyse and monitor the traffic for example, in order to find unexpected suspicious traffic, but as well by perpetrators to collect data sent over clear text that is easily readable with use of network sniffer.



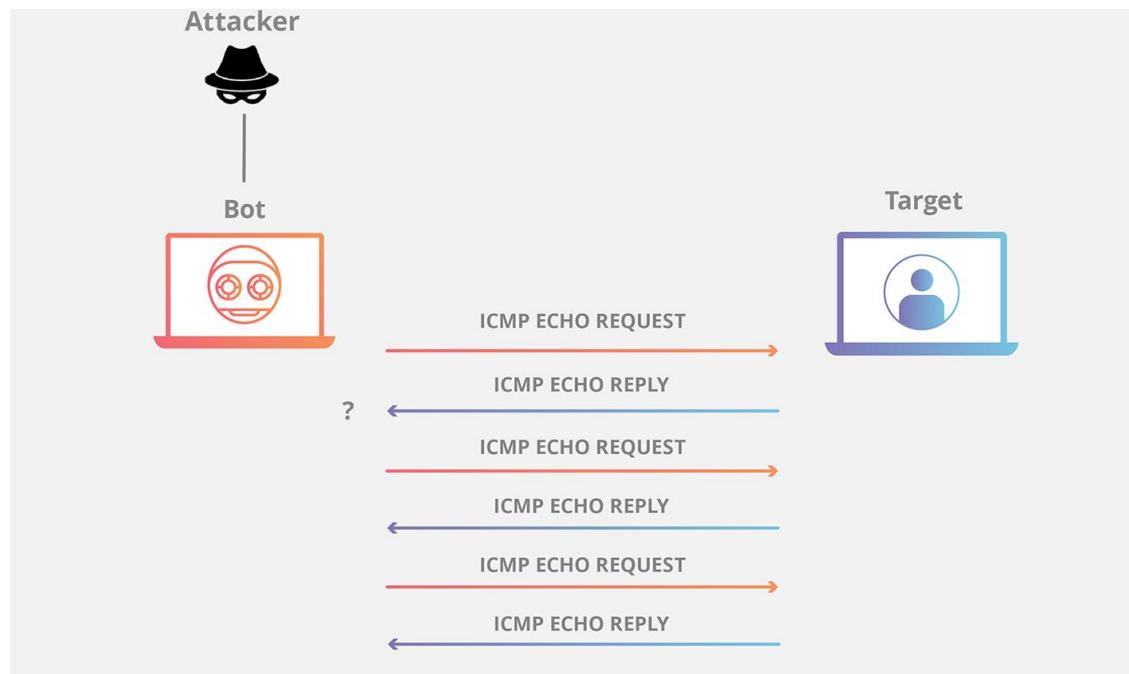
DoS and DDoS ATTACKS

- Denial of Service Attack (DoS Attack) is an attack designed to cause an interruption or suspension of services of a specific host/ server by flooding it with large quantities of useless traffic or external communication requests.
- When the DoS attack succeeds the server is not able to answer even to legitimate requests anymore, this can be observed in numbers of ways – slow response of the server, unavailability of software or web page. Distributed Denial of Service Attack (DDoS Attack) occurs where multiple compromised or infected systems (botnet) flood a particular host with traffic simultaneously.



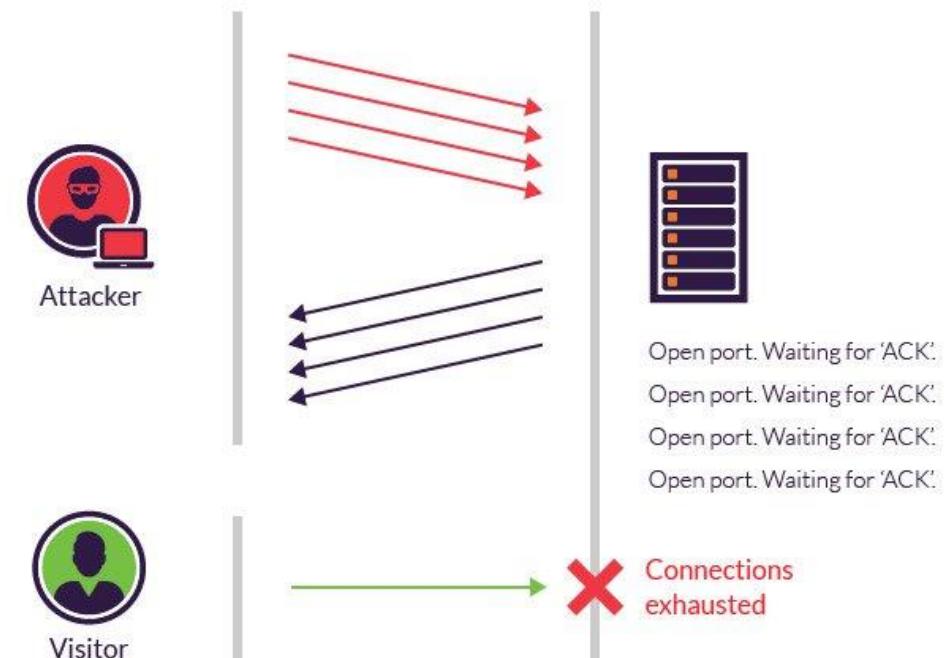
ICMP FLOOD (PING FLOOD) ATTACK

- An **ICMP flood (Ping flood)** is a DoS attack that overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting in a significant overall system slowdown.



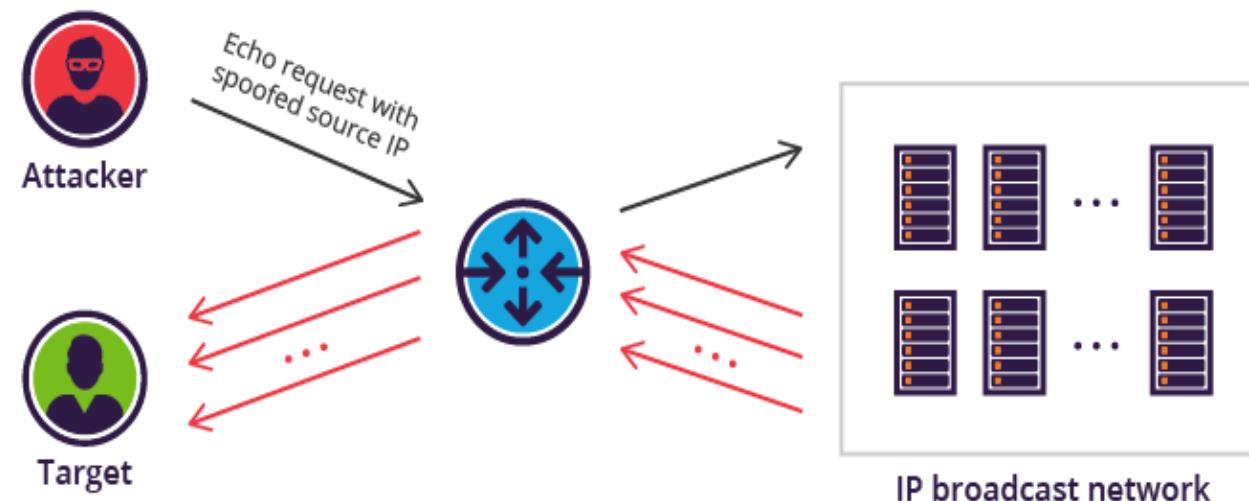
SYN FLOOD ATTACK

- In **SYN flooding** (DoS attack), the sender is the attacker and the receiver is the victim. The attacker sends a SYN packet and the server responds with SYN-ACK. But the attacker does not reply with an ACK packet. The server expects an ACK packet from the attacker and waits for some time. The attacker sends a lot of SYN packets and the server waits for the final ACK until timeout. Hence, the server exhausts its resources waiting for ACK.



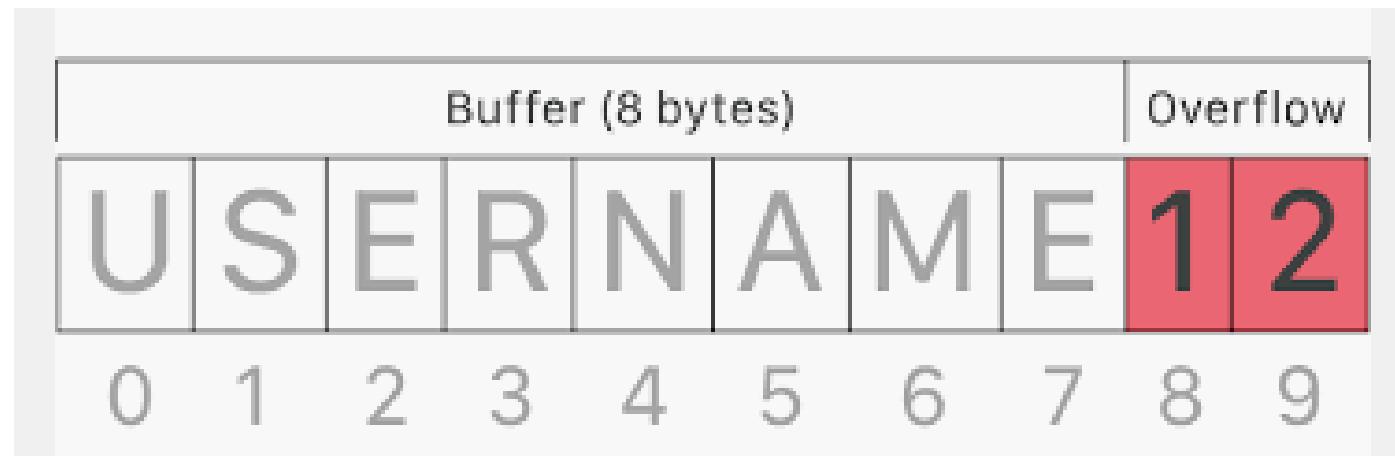
SMURF ATTACKS

- A Smurf Attack is a DoS attack that involves sending ICMP echo requests (ping) traffic to the broadcast address of routers and other network devices in large computer networks with a spoofed source address (the address of the desired DoS target). Since the device receiving the original ICMP echo request broadcasts it to every other device it's connected to, each one of these devices sends out an echo reply to the spoofed source address (the DoS target). This will generate a high rate of ICMP traffic and could cause DoS or instability for the target network.



BUFFER OVERFLOW ATTACKS

- A buffer is a temporary area for data storage. When more data (than was originally allocated to be stored) gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding. In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.

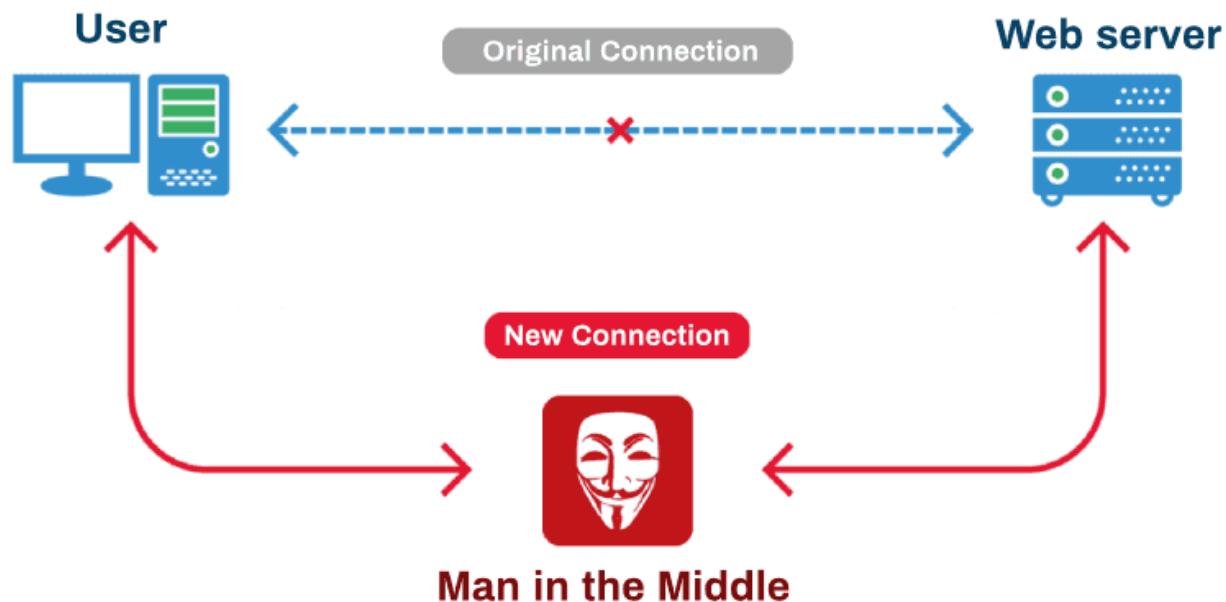


BOTNET

- A **botnet** (short for “robot network”) is a network of computers infected by malware that are under the control of a single hacker. Each individual machine under the control of the hacker is known as a **bot**. From one central point, the hacker can command every computer on its botnet to simultaneously carry out a coordinated criminal action.
- The scale of a botnet enables the hacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under control of a remote hacker, infected machines can receive updates and change their behavior on the fly. The botnet can be used to launch DDoS attacks, send spam mails, etc.

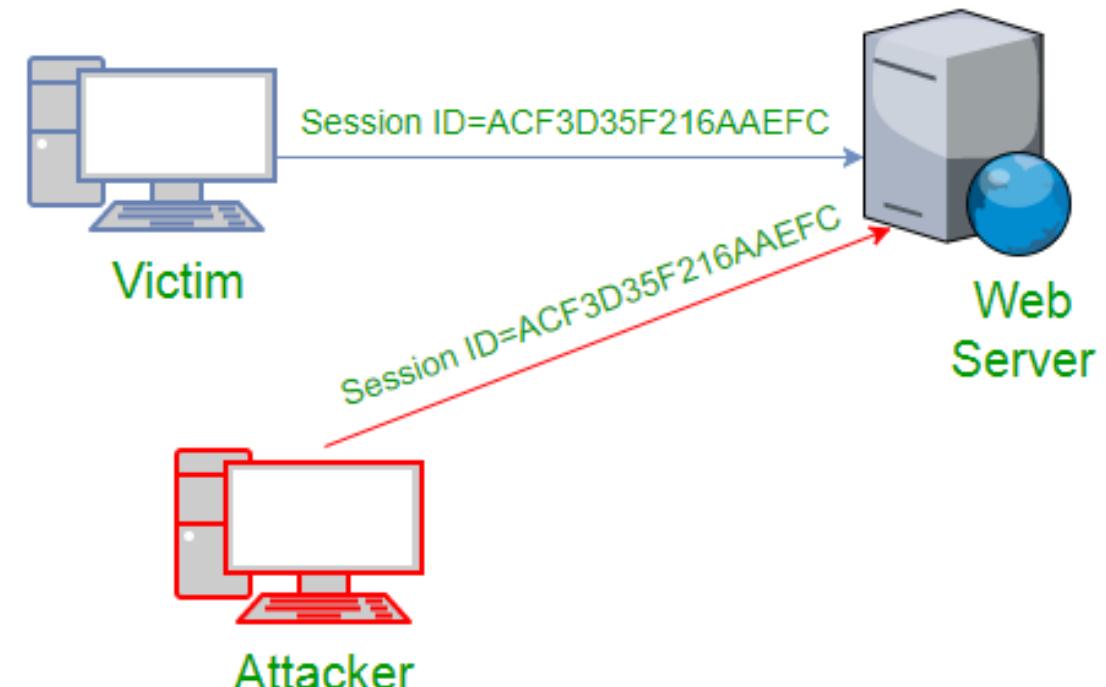
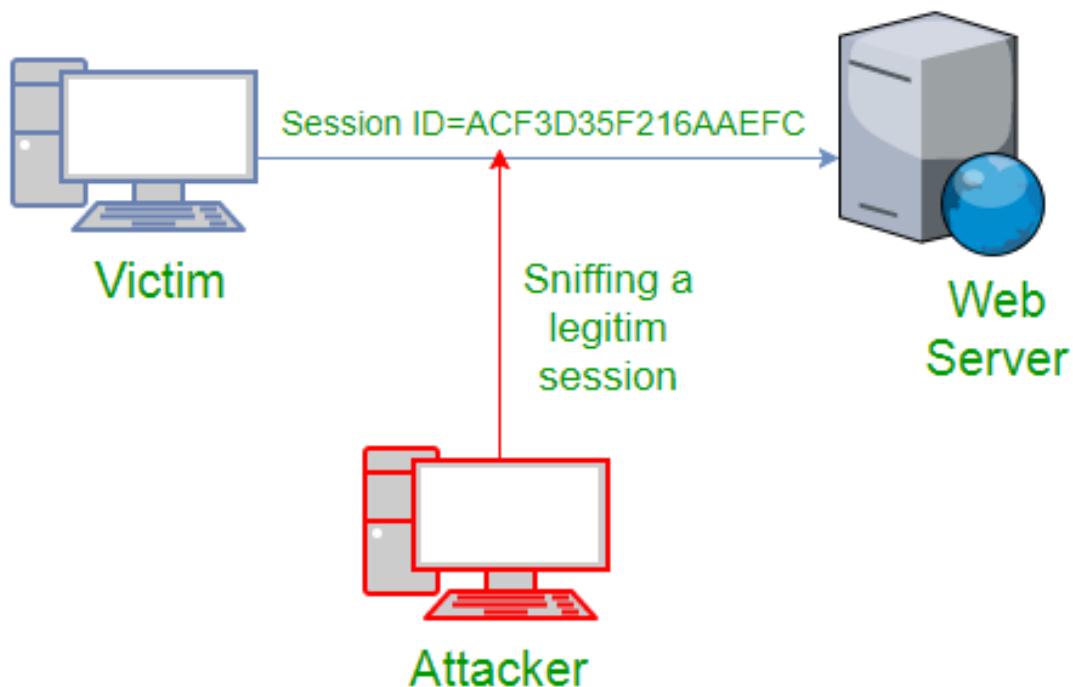
MAN-IN-THE-MIDDLE ATTACK

- A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.



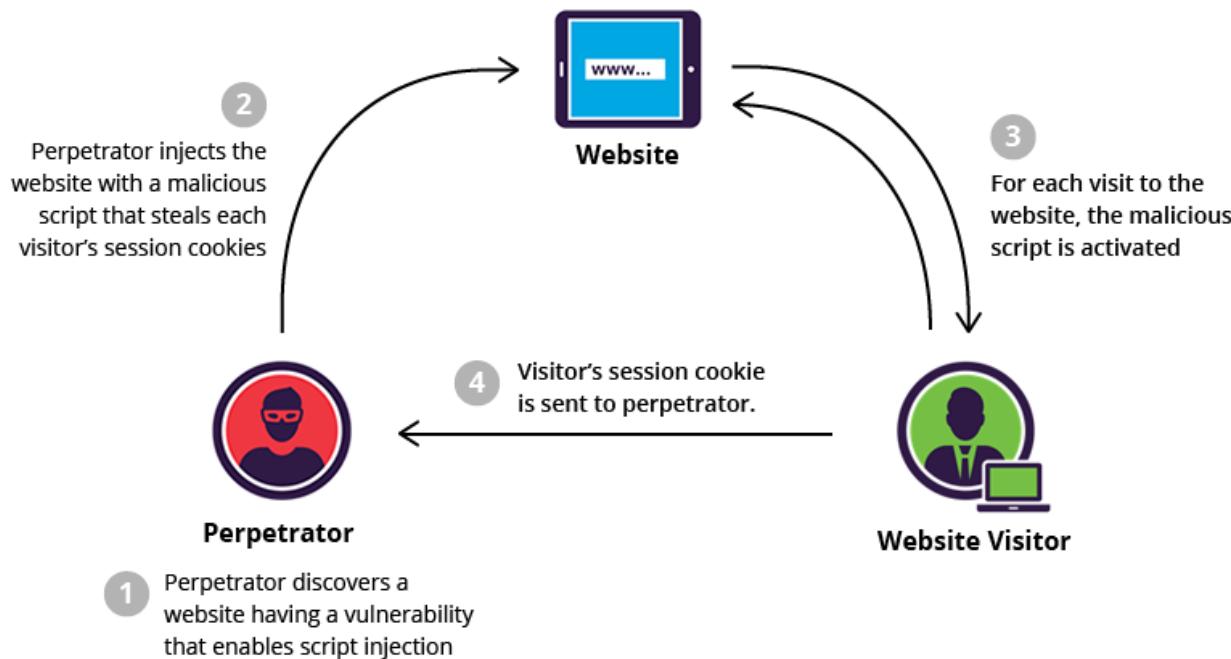
SESSION HIJACKING ATTACK

- Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out. The attack relies on the attacker's knowledge of your session cookie, so it is also called cookie hijacking or cookie side-jacking. To perform session hijacking, an attacker needs to know the victim's session ID (session key).



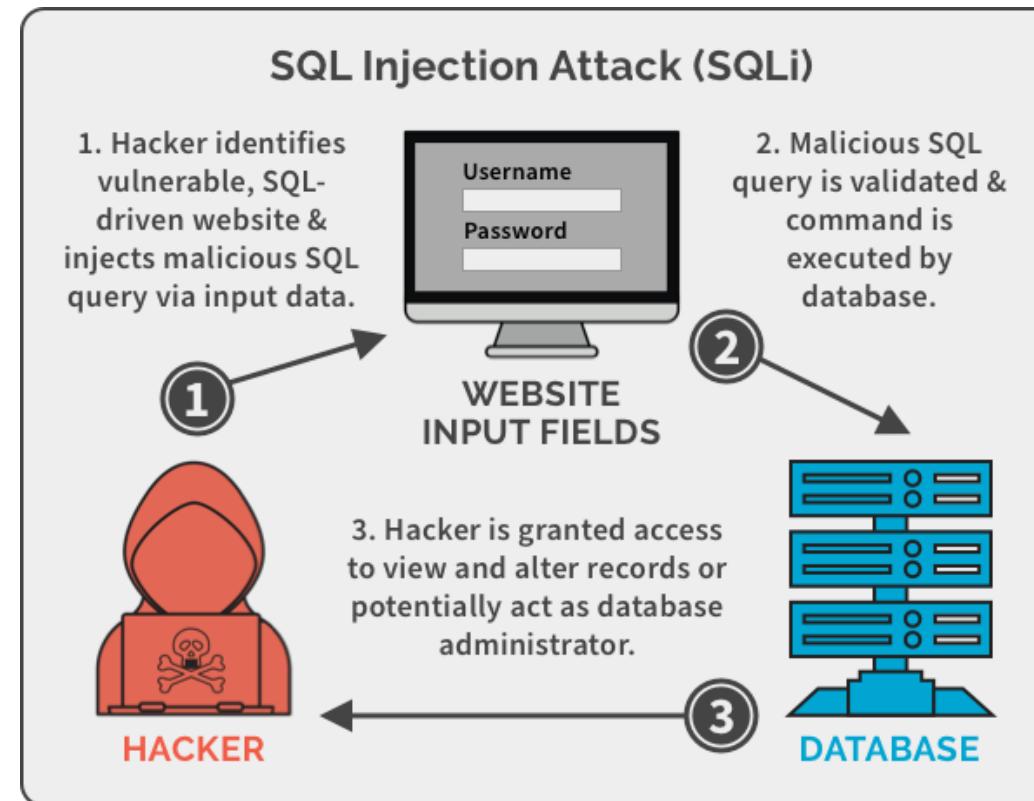
CROSS-SITE SCRIPTING ATTACK

- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.



SQL INJECTION ATTACK

- Websites and applications all need to interact with their users, which means users must have some way to input data, whether it's a text box on a website or a form within an application. When this kind of input data is directly turned into a SQL query, the program or website allowing the input can be vulnerable to malicious code. This is known as SQL injection. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS).



BLUETOOTH RELATED ATTACKS

- **Bluesnarfing** (or a Bluesnarf attack) is a device hack that involves the theft of data including contact lists, calendars, emails, or text messages from a Bluetooth-enabled wireless device set to “discoverable” mode. It’s easy to become a victim of a bluesnarfing attack if you have the habit of using Bluetooth in public places and your phone is usually in a discoverable mode.
- **Bluejacking** is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius. First, the hacker scans his surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices. At worst, bluejacking is an annoyance.

MODULE – 1

PART – 1: Information Security Fundamentals

- **Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security.
- Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices.
- A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.
- Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it

Types of Cyber Security

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Cloud security** is a software-based tool that protects and monitors your data in the cloud, to help eliminate the risks associated with on-premises attacks.
- **Data loss prevention** consists of developing policies and processes for handling and preventing the loss of data, and developing recovery policies in the event of a cyber security breach.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices.

The three main pillars of information security are **Confidentiality**, **Integrity** and **Availability**, also known as the CIA triad.

- **Confidentiality** refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data.
- **Integrity** ensures that information are in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have.
- **Availability** ensures that information and resources are available to those who need them.

Two additional concepts that supplement the purpose of information security are **Authenticity** and **Accountability**.

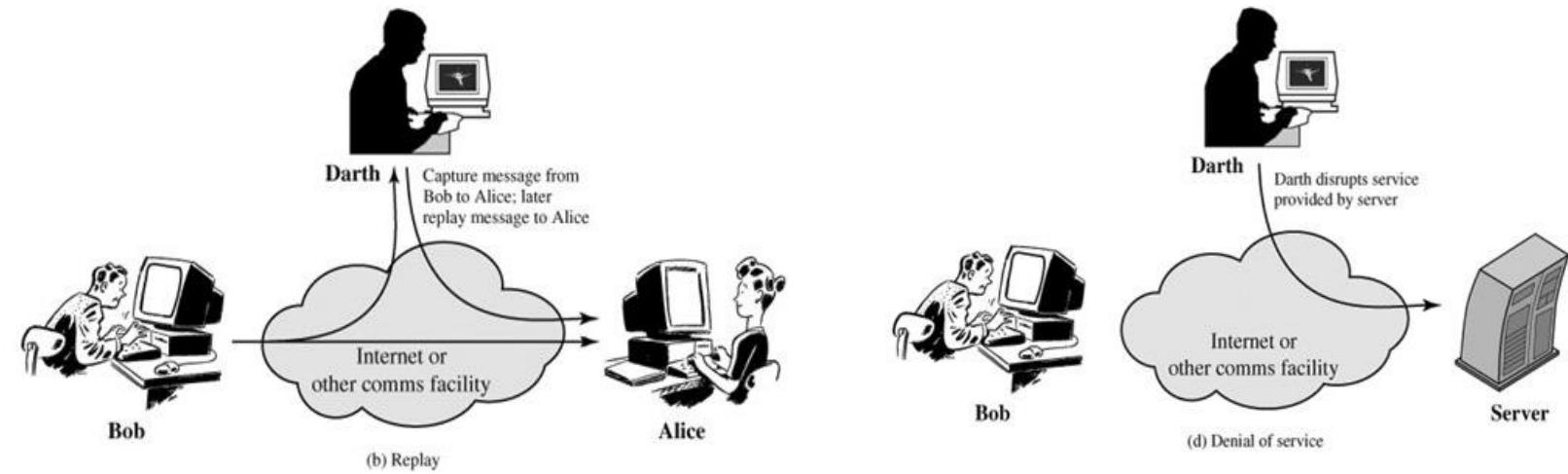
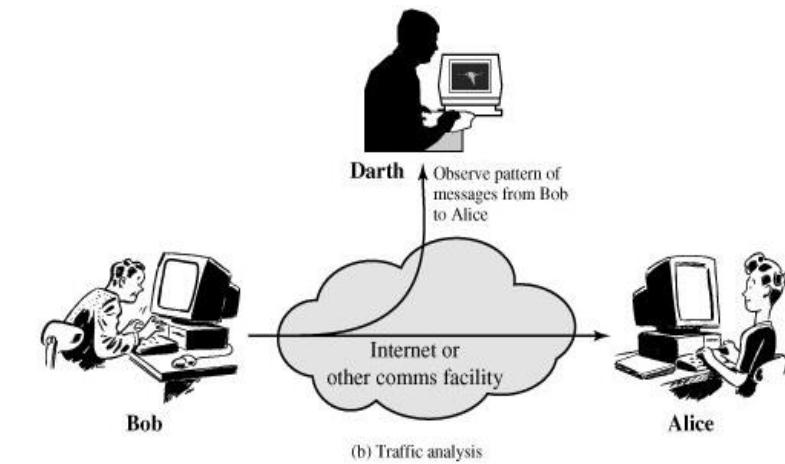
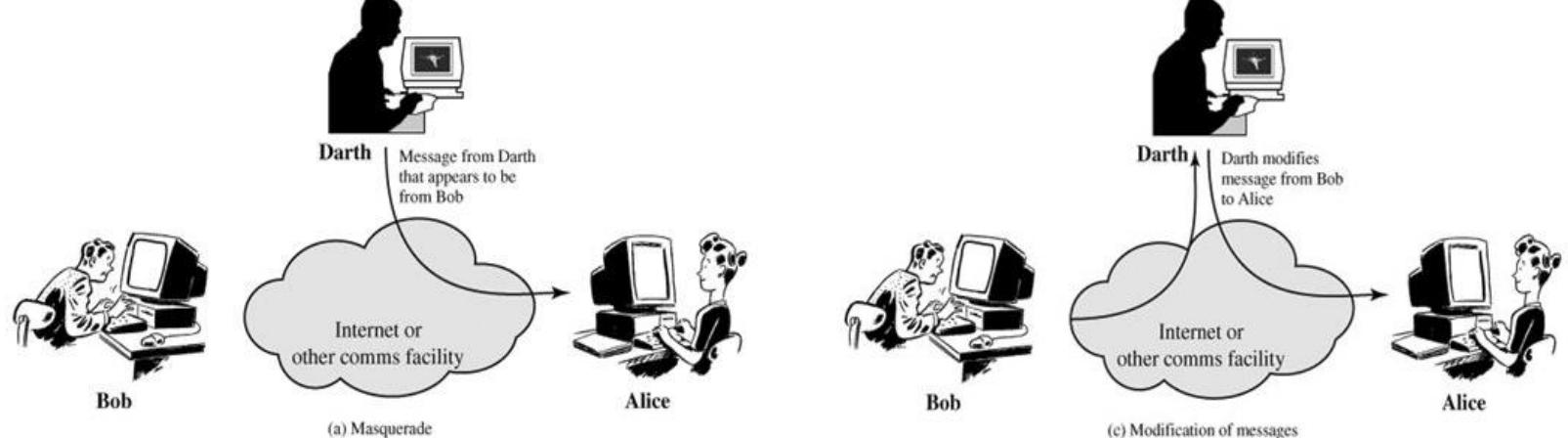
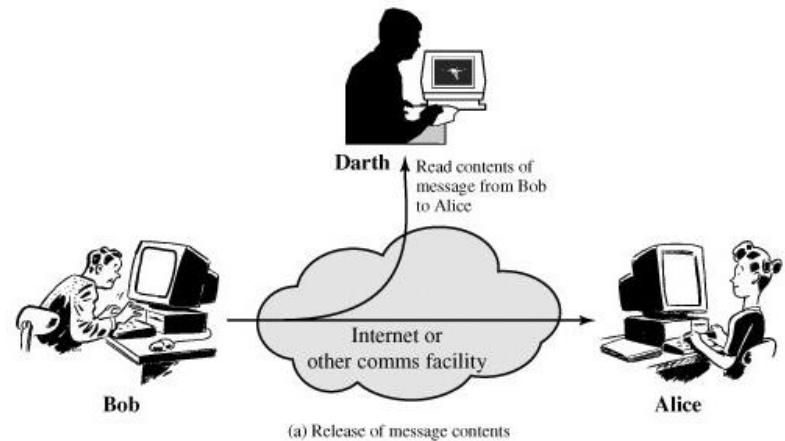
- **Authenticity** is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Accountability** is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.

The **OSI security architecture** is useful to managers as a way of organizing the task of providing security. The OSI security architecture focuses on **security attacks**, **security mechanisms**, and **security services**.

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

A **security attack** can be basically classified into an **Active Attack** or a **Passive Attack**.

- A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission.
- An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement.



MODULE – 1

PART – 2: Information Security Fundamentals

Security Services

OSI Security Architecture divides security services into five categories:

- **Authentication:** The assurance that the communicating entity is the one that it claims to be.
- **Access Control:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
- **Data Confidentiality:** The protection of data from unauthorized disclosure.
- **Data Integrity:** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
- **Nonrepudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication

Security Mechanisms

- Specific Security Mechanisms
 1. **Encipherment:** Use of mathematical algorithms to transform data into a form that is not readily intelligible.
 2. **Digital Signature:** A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
 3. **Access Control:** A variety of mechanisms that enforce access rights to resources.
 4. **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
 5. **Authentication Exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.

Security Mechanisms (contd.)

6. **Traffic Padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
7. **Routing Control:** Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
8. **Notarization:** The use of a trusted third party to assure certain properties of a data exchange.

Security Mechanisms (contd.)

- Pervasive Security Mechanisms
 1. **Trusted Functionality:** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
 2. **Security Label:** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
 3. **Event Detection:** Detection of security-relevant events.
 4. **Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
 5. **Security Recovery:** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Access Control

Access control models define how computers enforce access of subjects (such as users, other computers, applications and so on) to objects (such as computers, files, directories, applications, servers and devices). Three main access control models exist.

Discretionary Access Control (DAC)

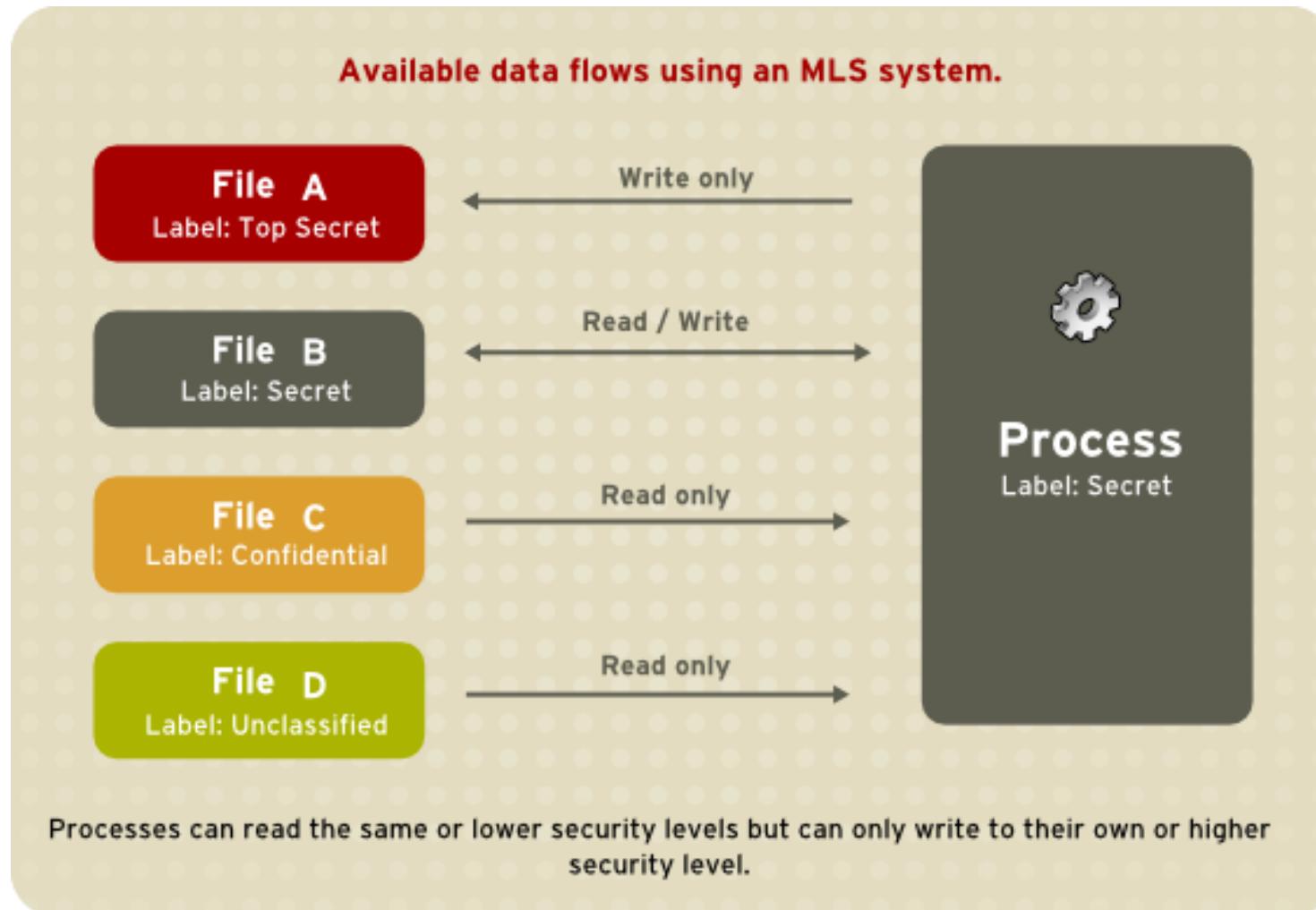
- In the DAC model, the owner (creator) of information (file or directory) has the discretion to decide about and set access control restrictions on the object in question.
- It is the most widely used model. The advantage is its flexibility. Users may decide who can access information and what they can do with it — read, write, delete, rename, execute and so on.
- At the same time, users may make wrong decisions regarding access control restrictions or maliciously set insecure or inappropriate permissions.

Access Control (contd.)

Mandatory Access Control (MAC)

- In systems utilizing MAC, users have little or no discretion as to what access permissions they can set on their information.
- Instead, mandatory access controls specified in a system-wide security policy are enforced by the operating system and applied to all operations on that system.
- MAC based systems can be more secure than DAC based systems when used appropriately. But they are also much more difficult to use and administer because of the additional restrictions and limitations imposed by the operating system.
- MAC based systems are typically used in government, military and financial environments where higher than usual security is required and where the added complexity and costs are tolerated.

Access Control (contd.)



Bell-Lapadula MLS access model

Access Control (contd.)

Role-Based Access Control (RBAC)

- In the role based access control model, rights and permissions are assigned to roles instead of individual users. This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.
- For example, access to marketing files may be restricted only to the marketing manager role, and users Ann, David, and Joe may be assigned the role of marketing manager.
- Later, when David moves from the marketing department elsewhere, it is enough to revoke his role of marketing manager, and no other changes would be necessary.

	<i>objects</i>			
	F₀	F₁	Printer	
<i>domains of protection (subjects)</i>	D ₀	read	read-write	print
	D ₁	read-write-execute	read	
	D ₂	read-execute		
	D ₃		read	print
	D ₄			print

Access Control Matrix

MODULE - 1

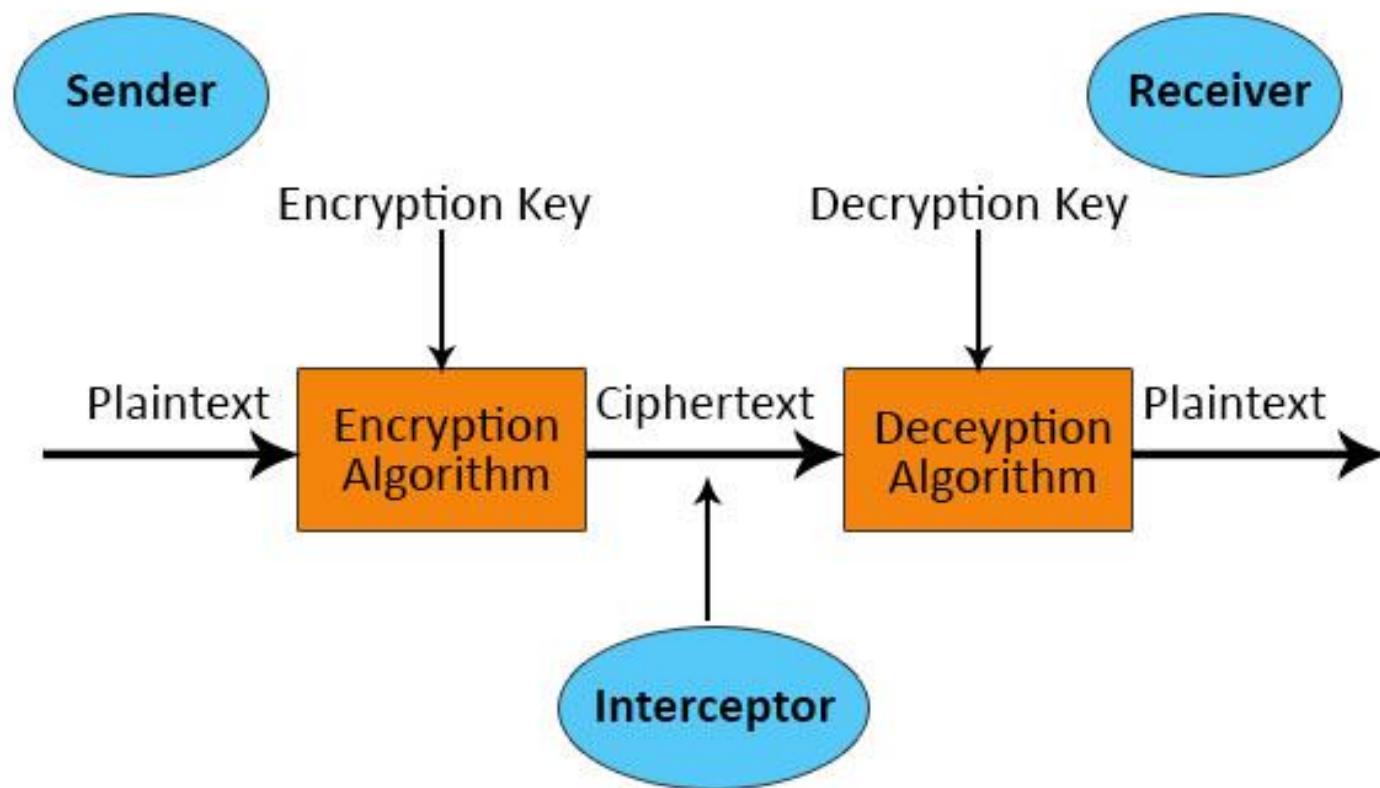
PART – 3: CRYPTOGRAPHY

- **Cryptology** is the science of secret messages. Therefore, anything that has to do with making or breaking codes falls into cryptology's domain.

Cryptology = Cryptography + Cryptanalysis

- **Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries.
- In Cryptography, **Cryptosystem** is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality.
- **Cryptanalysis** is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

- A simple model of a cryptosystem that provides confidentiality to the information being transmitted is shown below.



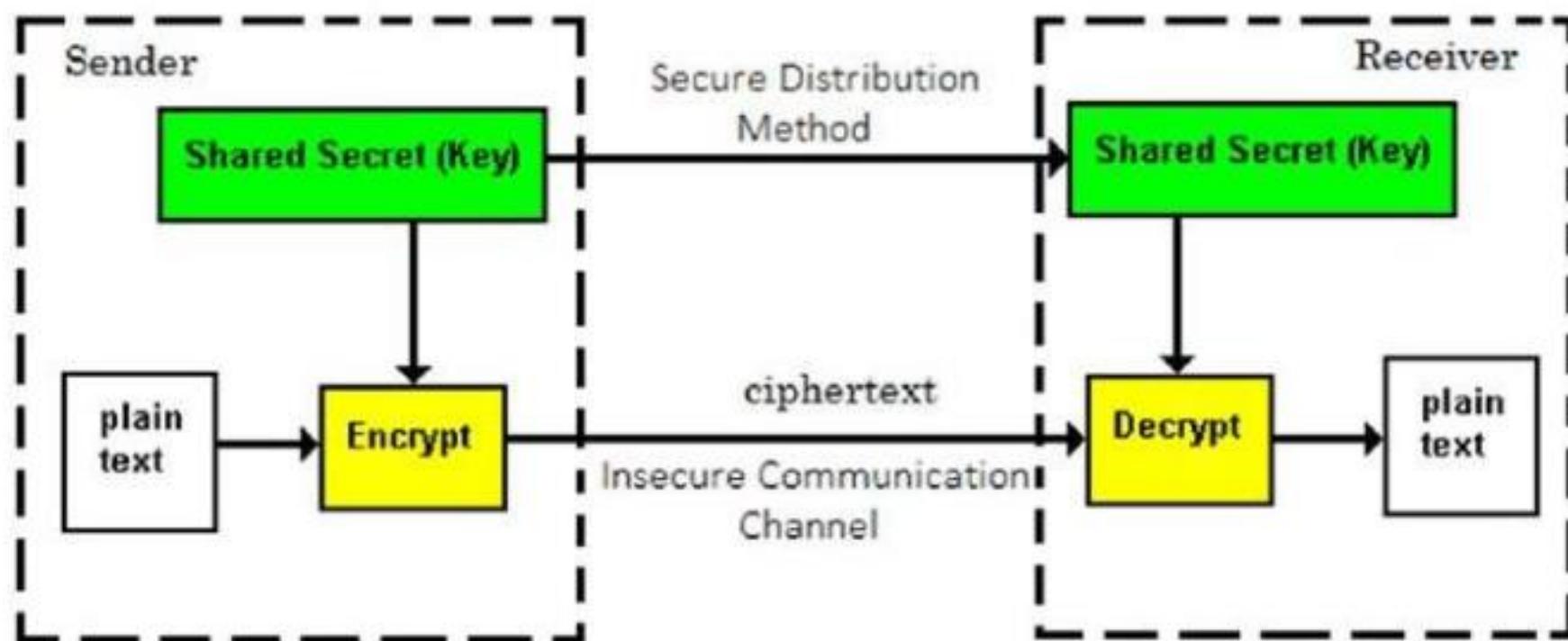
The various components of a basic cryptosystem are as follows.

- **Plaintext**. It is the data to be protected during transmission.
- **Encryption Algorithm**. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Encryption Key**. It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Ciphertext**. It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel.
- **Decryption Algorithm**. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext.
- **Decryption Key**. It is a value that is known to the receiver. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

Fundamentally, there are two types of cryptosystems as shown.

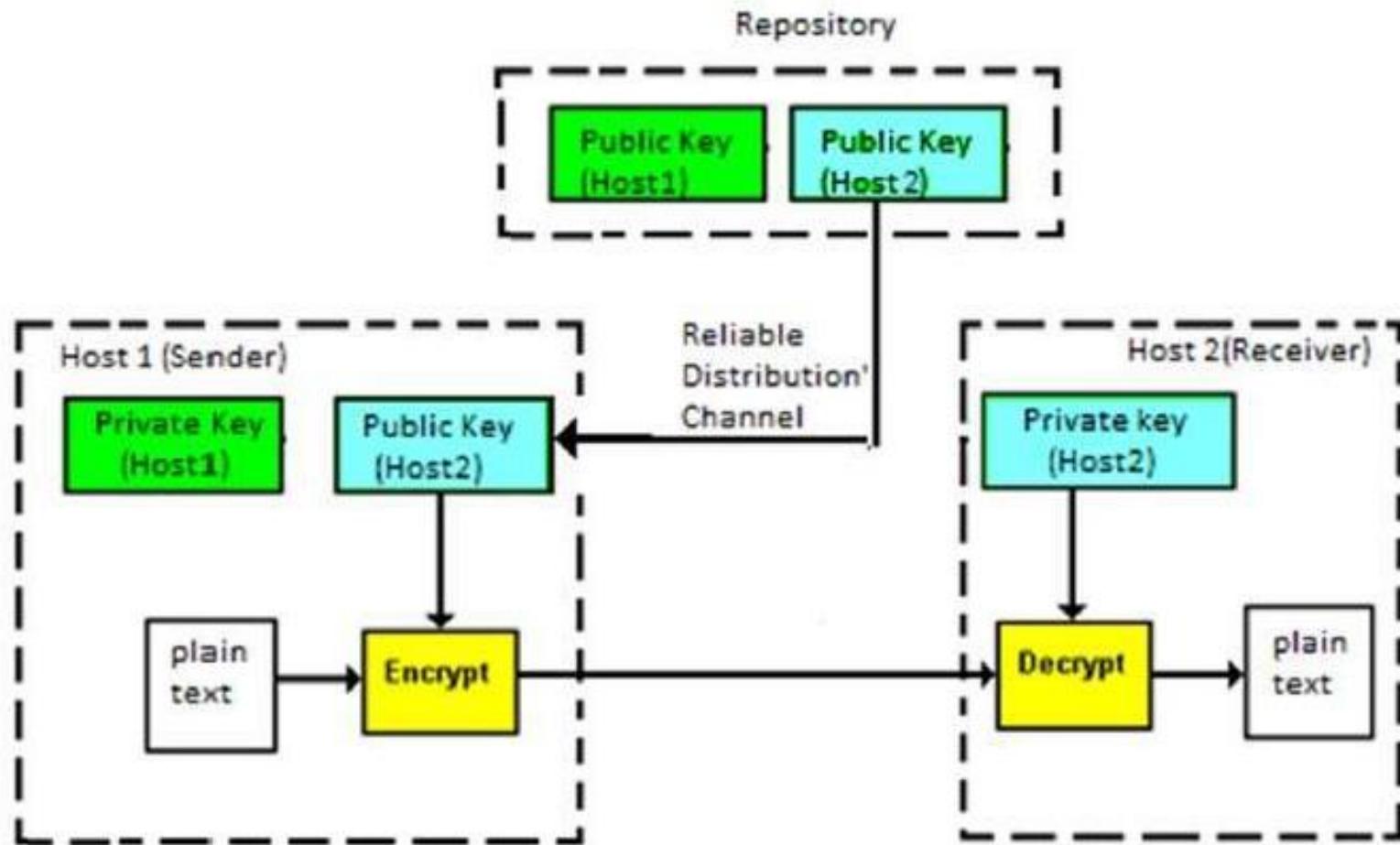
Symmetric Cryptosystem (Secret Key Cryptosystem)

- The encryption process where *same keys* are used for encrypting and decrypting the information is known as **Symmetric Encryption**.
- The study of symmetric cryptosystems is referred to as **Symmetric Cryptography**.



Asymmetric Cryptosystem (Public Key Cryptosystem)

- The encryption process where different keys are used for encrypting and decrypting the information is known as **Asymmetric Encryption**. Though the keys are different, they are mathematically related.
- Study of asymmetric cryptosystems is referred to as **Asymmetric Cryptography**.



SYMMETRIC ENCRYPTION VERSUS ASYMMETRIC ENCRYPTION

SYMMETRIC ENCRYPTION

Method of using the same cryptographic keys for both encryptions of plaintext and decryption of ciphertext

Simple since only one key used in both operations

Has a faster execution speed

RC4, AES, DES, 3DES are some common algorithms

ASYMMETRIC ENCRYPTION

Method of using a pair of keys: the public key, which is disseminated widely, and a private key, which is known only to the owner

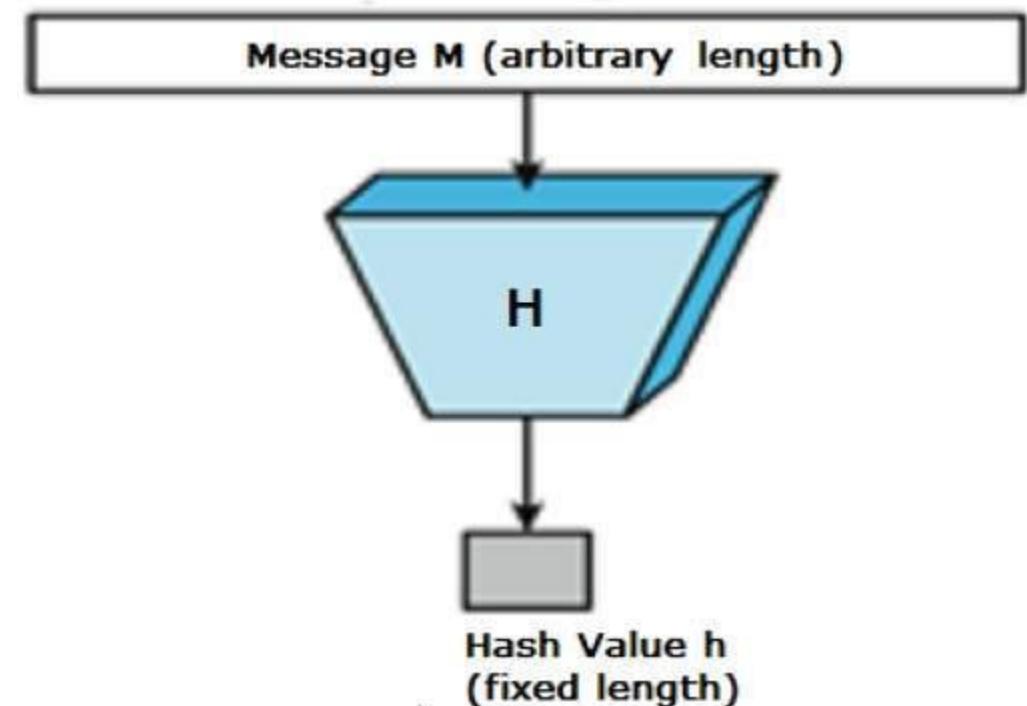
More complex as it uses separate keys for both operations

Comparatively slower

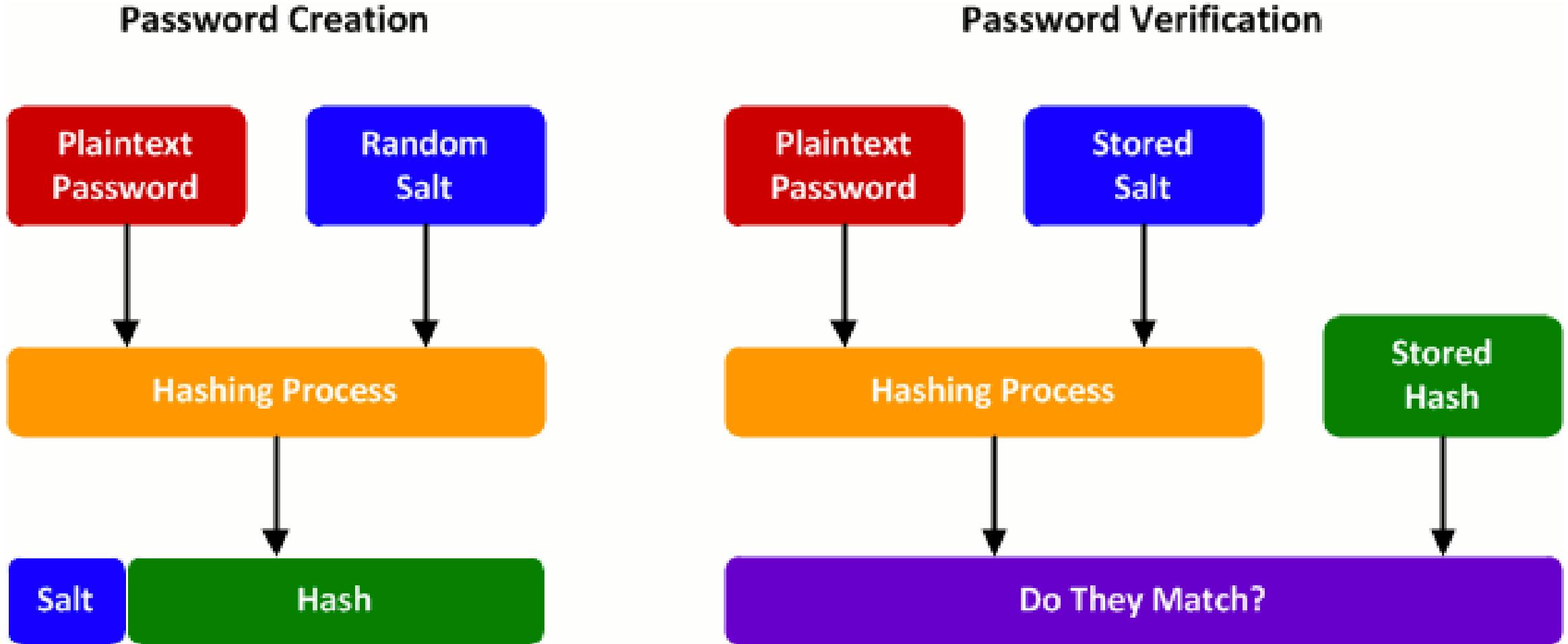
Diffie-Hellman and RSA algorithm are some common algorithms

Cryptographic Hash Function

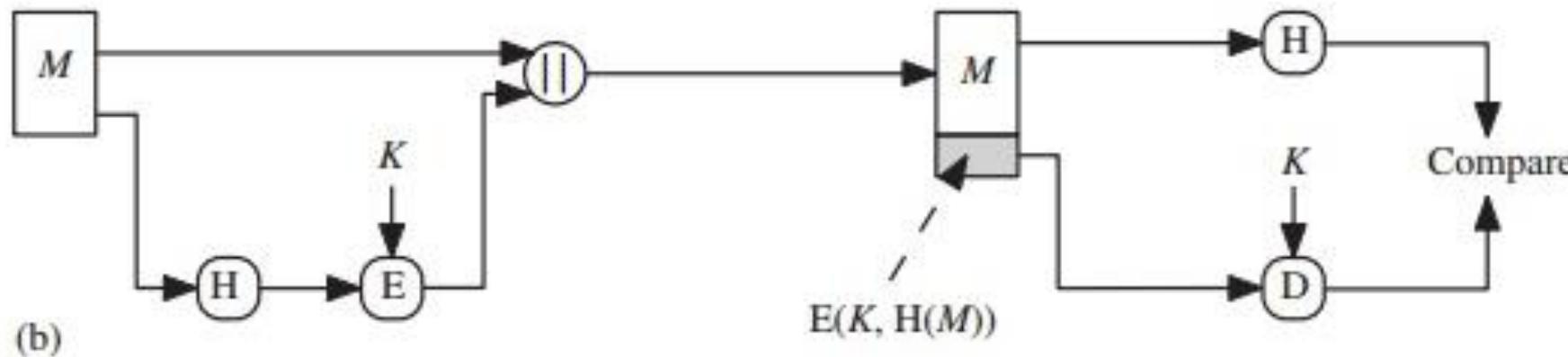
- A cryptographic hash function is an algorithm that takes an arbitrary amount of data input and produces a fixed-size output called the **hash value, hash, or message digest**.
- There is no practical way to recover the input from the output, hence, it is also called **one-way function**.
- Also, two or more different inputs may result in same output. How will you know which is the correct input?
- Common Hash algorithms are:
 1. Message Digest 5 (MD5)
 2. Secure Hash Algorithm 1 (SHA-1)
 3. Secure Hash Algorithm 2 (SHA-2)



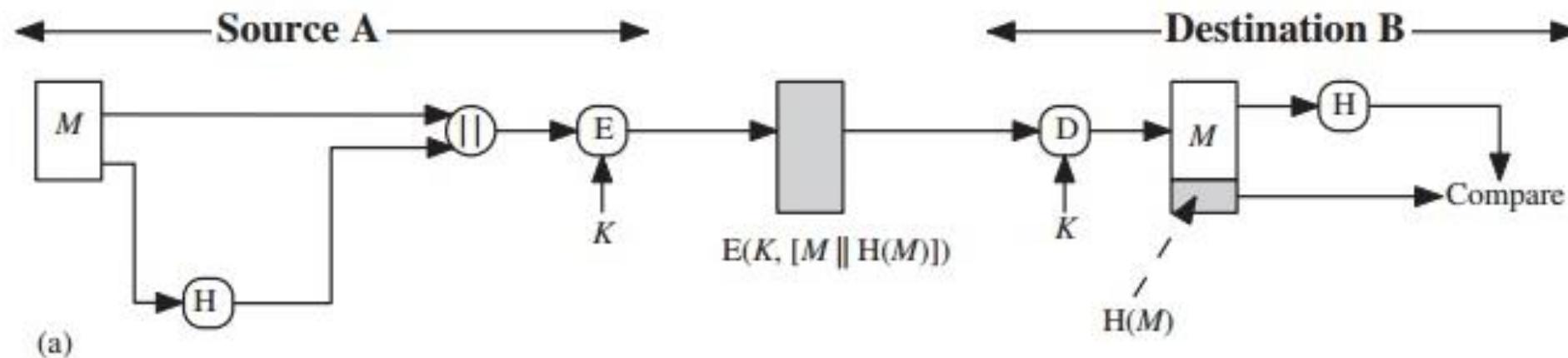
Applications of Hash Functions (Password Storage)



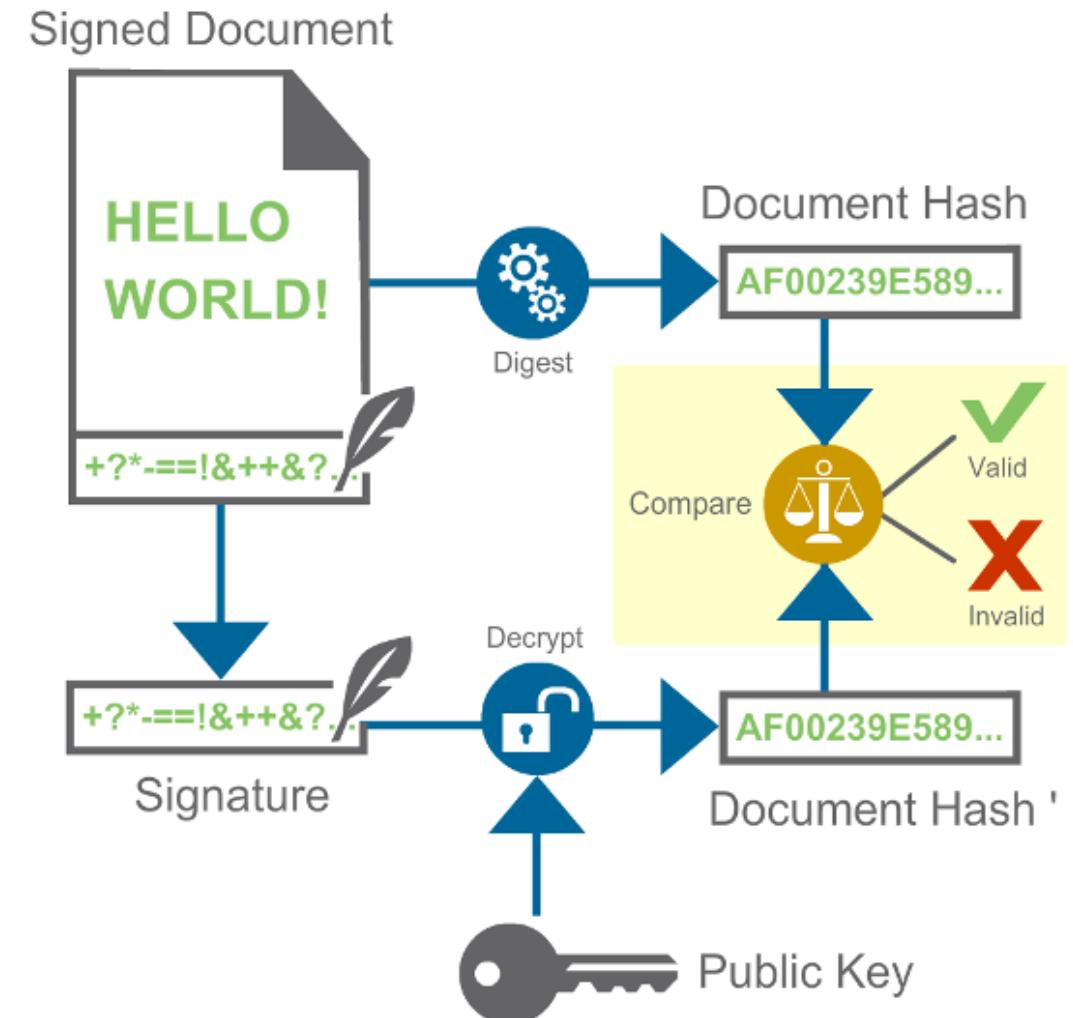
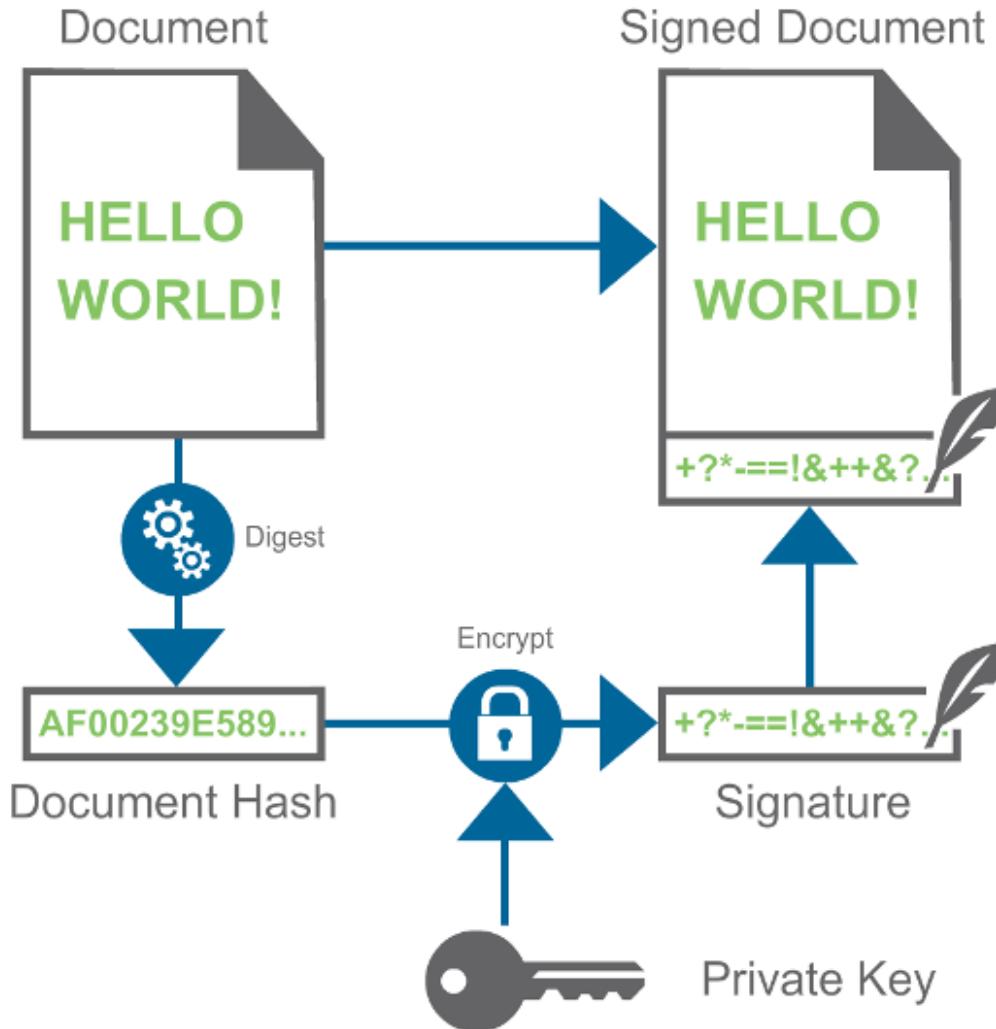
Applications of Hash Functions (Integrity + Authenticity)



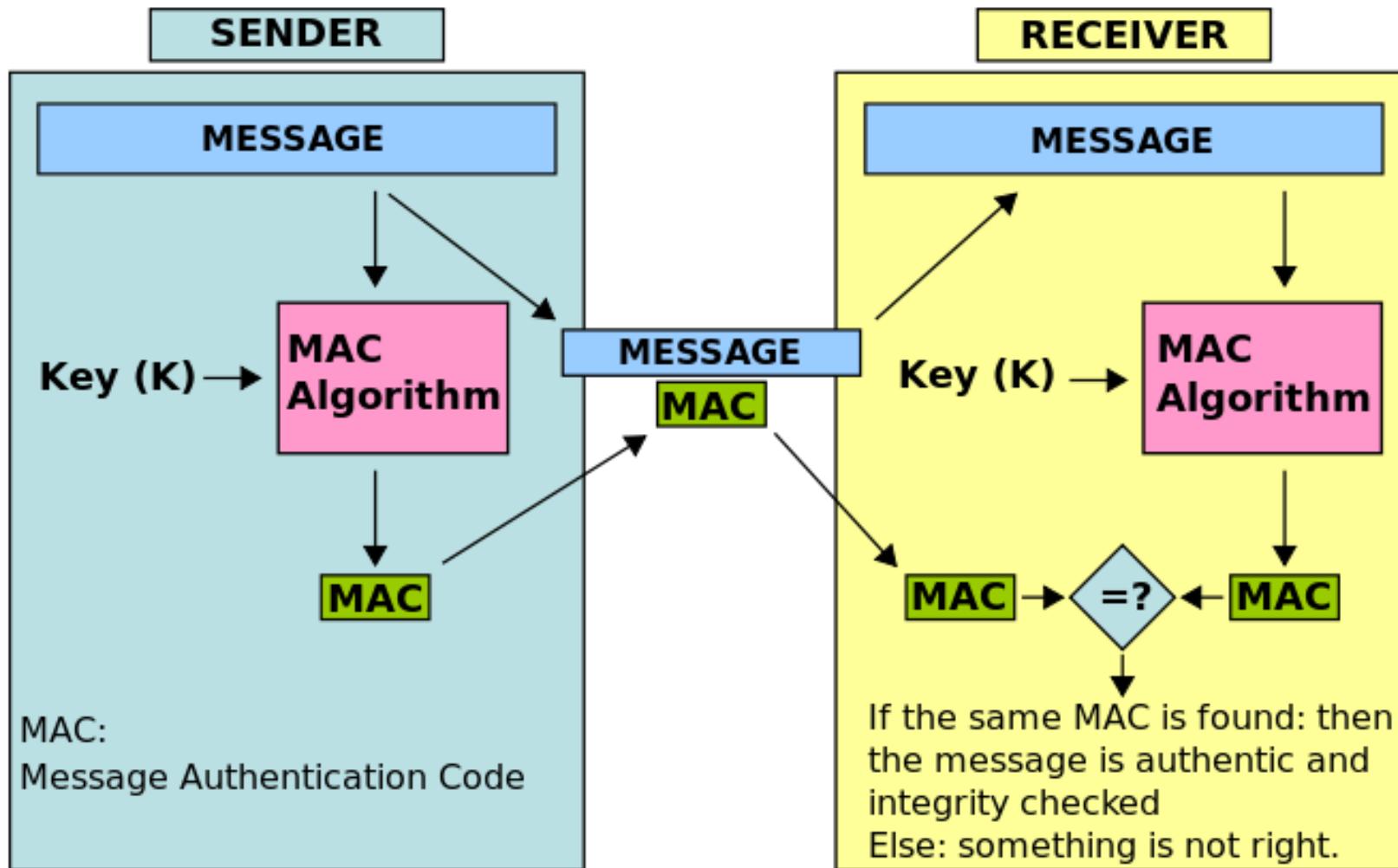
Applications of Hash Functions (Confidentiality + Integrity + Authenticity)



Digital Signature



Message Authentication Code



MODULE - 1

PART – 4: DECEPTION TECHNOLOGY

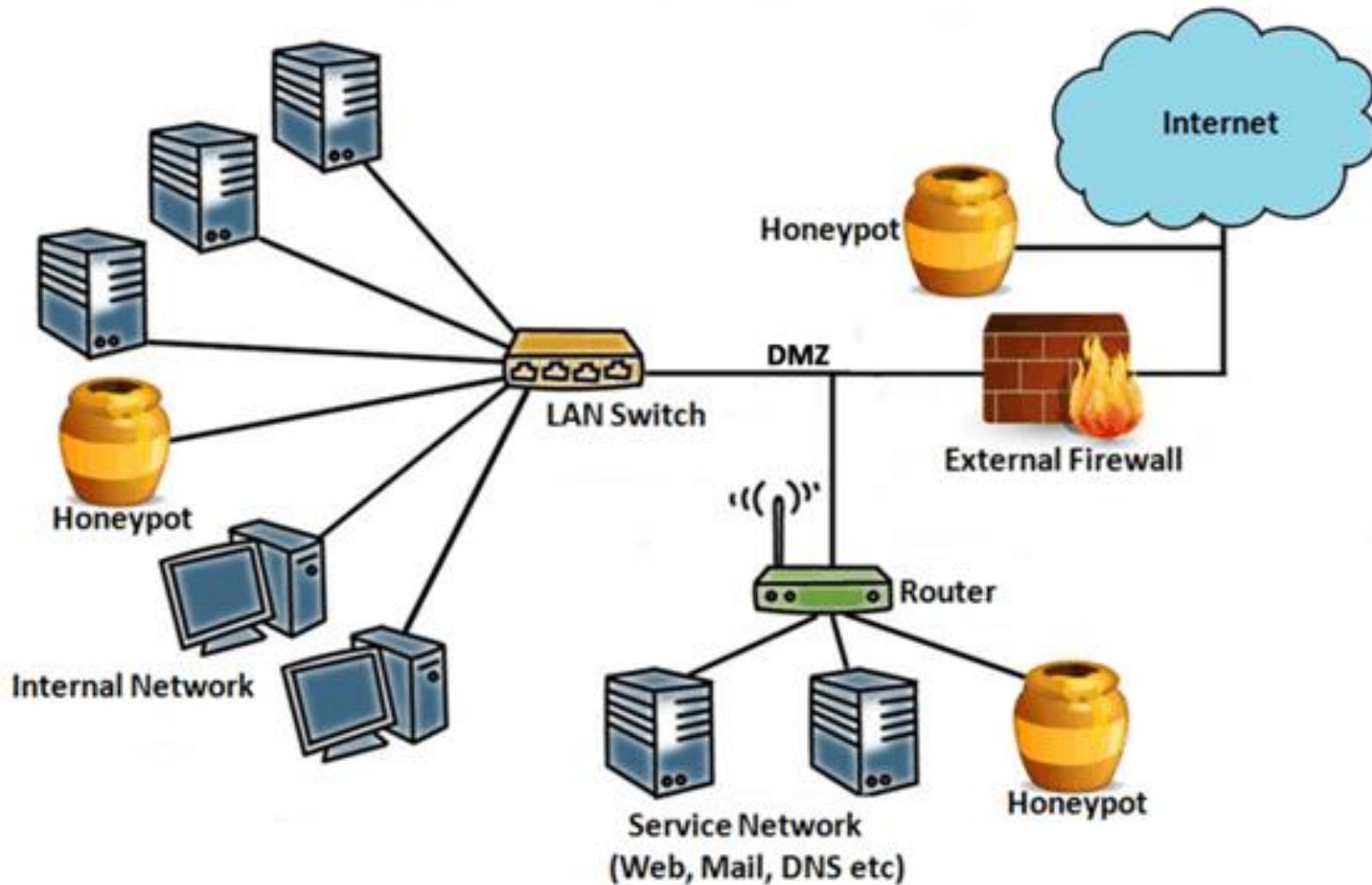
What is Deception Technology in Cyber Security?

- The aim of **Deception technology** is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage.
- The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure.
- These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials.
- Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal.

Honeypot as a Deception Technology

- A **honeypot** is a network-attached system set up as a decoy to lure cyberattackers and to detect, deflect or study hacking attempts. They're used by security researchers as well as IT companies.
- There are many applications and use cases for honeypots, as they work to divert malicious traffic away from important systems, get an early warning of a current attack before critical systems are hit, and gather information about attackers and their methods.
- For a honeypot to work, the system should appear to be legitimate. It should run processes a production system is expected to run, and contain seemingly important dummy files.

Honeypot as a Deception Technology (Contd.)



Honeypot as a Deception Technology (Contd.)

- It's also a good idea to place a honeypot behind your corporate firewall—not only does it provide important logging and alerting capabilities.
- In terms of objectives, there are two types of honeypots: research and production honeypots.
- **Research Honeypots** - Research honeypots gather information about attacks and are used specifically for studying malicious behavior out in the wild.
- **Production Honeypots** - Production honeypots, on the other hand, are focused on identifying active compromise on your internal network and tricking the attacker.

Honeypot as a Deception Technology (Contd.)

- Honeypots can be categorized according to their build and complexity - Low-interaction and High-interaction Honeypots.
- **Low-interaction Honeypots** – They use fewer resources and collect basic information about the level and type of threat and where it is coming from. They are easy and quick to set up. There's nothing in the honeypot to engage the attacker for very long.
- **High-interaction Honeypots** – They aim to get hackers to spend as much time as possible within the honeypot, giving plenty of information about their intentions and targets, as well as the vulnerabilities they are exploiting and their method of working.

Honeypot as a Deception Technology (Contd.)

- Several honeypot technologies in use include the following:
- **Email traps (Spam Traps)** – They place a fake email address in a hidden location where only an automated address harvester will be able to find it . It's 100% certain that any mail coming to it is spam. The source IP of these senders can be added to a blacklist.
- **Decoy database** – It can be set up to monitor software vulnerabilities and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse.
- **Malware honeypot** - It mimics software apps and APIs to invite malware attacks. The characteristics of the malware can then be analyzed to develop anti-malware software or to close vulnerabilities in the API.

Honeypot as a Deception Technology (Contd.)

- **Spider honeypot** – It is intended to trap webcrawlers ('spiders') by creating web pages and links only accessible to crawlers. Detecting crawlers can help you learn how to block malicious bots, as well as ad-network crawlers.
- **Honeynets** - Honeynets are a logical extension of the honeypot concept. A honeynet is a series of networked honeypots. By watching attackers move across the network from file servers to web servers, for instance, we'll have a better sense of what they're doing and how they're doing it.

Honeypot as a Deception Technology (Contd.)

- **Benefits of using Honeypots**

- Honeypots can be a good way to expose vulnerabilities in major systems.
- They can also suggest ways in which security could be improved.
- They break the attacker kill chain and slow attackers down.
- Honeypots have a low false positive rate as compared to IDS.
- Honeypots can give reliable intelligence about how threats are evolving.
- Honeypots are also great training tools for technical security staff.
- Honeypots can also catch internal threats.

Honeypot as a Deception Technology (Contd.)

- Disadvantages of using Honeypots**

- Just because a certain threat hasn't been directed against the honeypot, you can't assume it doesn't exist.
- An attacker can create spoofed attacks to distract attention from a real exploit being targeted against your production systems.
- A smart attacker could potentially use a honeypot as a way into your systems.
- Deployment, maintenance and analysis costs are involved.

MODULE - 1

PART – 5: ETHICAL HACKING

Ethical Hacking

- **Hacking** is the process of identifying and exploiting weakness in a system or a network to gain unauthorized access to data and system resources.
- **Ethical Hacking** sometimes called as *Penetration Testing* is an authorized practice of bypassing system security to identify weak points that malicious hackers can exploit or destroy.

Important terms in hacking

- a. **Threat:** Anything that has potential to cause harm. There are various threats like Virus, Worm, Adware, Ransomware, etc.
- b. **Vulnerability:** A weakness or a flaw in the system which an attacker may find and exploit for e.g. Outdated security features, Weak authentication mechanism, substandard backup and recovery etc.

- c. **Attack:** A security attack is an unauthorized attempt to steal, damage, or expose data from an information system.
- d. **Attack vectors:** Path or means by an attacker gains access to an information system to perform malicious activities for e.g. email attachments, pop-up windows, Web pages etc.

Phases of Hacking

- 1. **Reconnaissance:** It is also called as *Footprinting* or *Information Gathering Phase*. There are two types of Footprinting:
 - a. **Active:** Directly interacting with the target to gather information about the target for e.g. Using Nmap tool to scan the target.
 - b. **Passive:** Collect information about the target without directly accessing the target i.e. from social media, public websites.

2. Scanning: Three types of scanning are involved:

- a. *Port scanning:*** This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.
- b. *Vulnerability Scanning:*** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.
- c. *Network Mapping:*** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information.

3. Gaining Access: This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

- 4. Maintaining Access:** Hacker may want to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.
- 5. Clearing Track:** An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Types of Hackers

- **Black-hat Hackers** are also known as an *Unethical Hacker* or a *Security Cracker*. These people hack the system illegally to steal money or to achieve their own illegal goals. Black Hat hacking is always illegal.
- **White Hat hackers** are also known as *Ethical Hackers*. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking is legal.
- **Grey hat hackers** are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Types of Penetration Testing

- **Black box:** The penetration tester will not be given any details pertaining to the network, or infrastructure of the network/organization.
- **Grey box:** The penetration tester typically has some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network.
- **White Box:** The penetration tester is provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc.

Common Hacking Techniques

- 1. Bait and Switch:** Using bait and switch hacking technique, an attacker can buy advertising spaces on the websites. Later, when a user clicks on the ad, he might get directed to a page that's infected with malware.
- 2. Cookie Theft:** The cookies in our browser store personal data such as browsing history, username, and passwords for different sites we access. Once the hacker gets the access to your cookie, he can even authenticate himself as you on a browser.
- 3. DoS/DDoS:** A Denial of Service attack is a hacking technique of taking down a site or server by flooding that site or server with a huge amount of traffic so that the server is unable to process all the requests in real-time and finally crashes down.

Common Hacking Techniques (contd.)

4. **Eavesdropping:** A passive technique used by hackers to listen in on a network connection and observe and record as much high-value information as possible.
5. **Phishing:** An attacker masquerades as a reputable entity or person in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions.
6. **Fake WAP:** Setting up a fake wireless access point (WAP) is a great way for hackers to gain a captive audience whose data streams can be monitored, intercepted, or hijacked for various purposes.

Common Hacking Techniques (contd.)

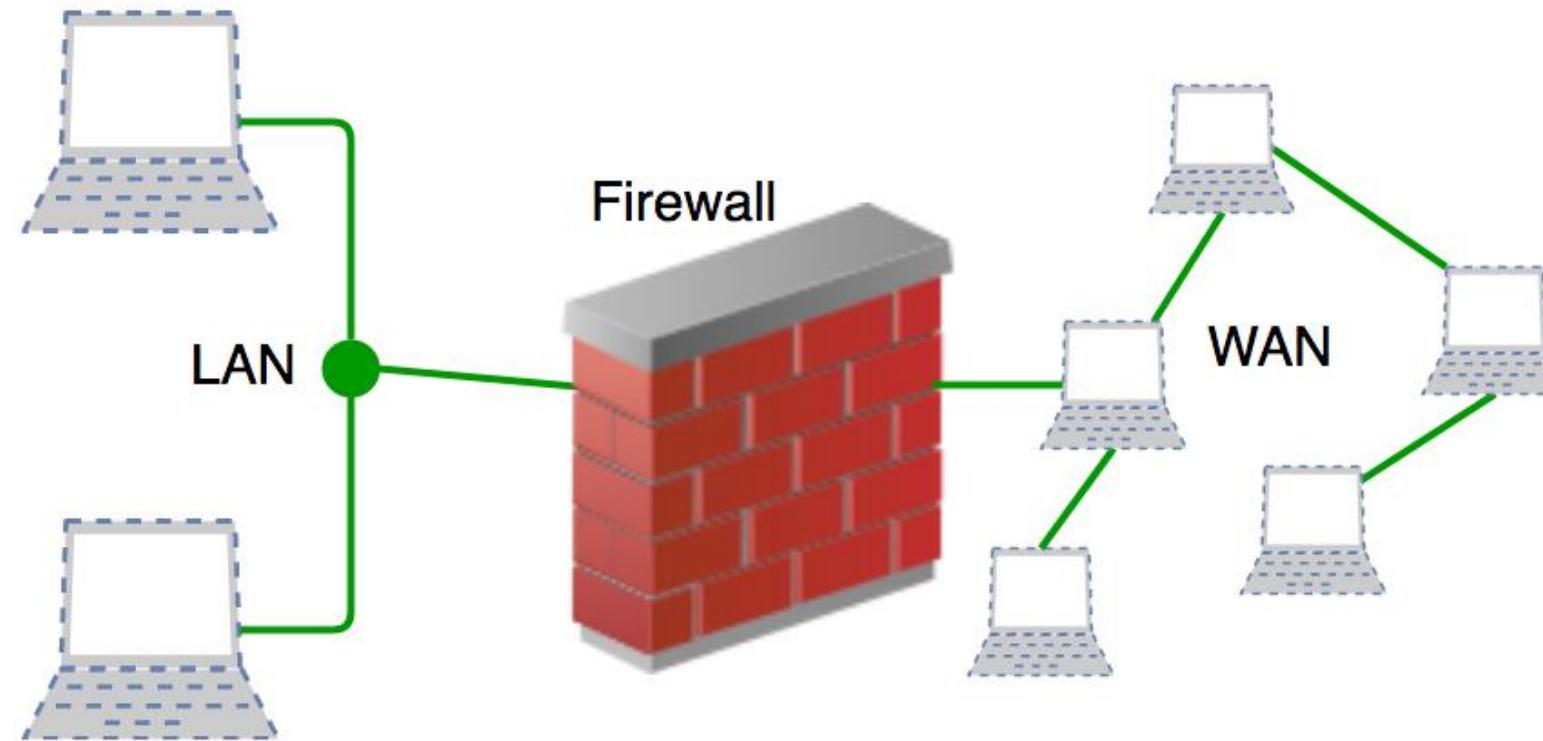
7. **Waterhole attack:** Setting up a bogus but attractive website to assemble a herd of unwitting victims in one place – where you can harvest data, or spread a malware infection to the maximum number of recipients.
8. **Keylogging:** Using keylogger software to record the key sequence and strokes of your keyboard into a log file on your machine. These log files might even contain your personal email IDs and passwords.
9. **Malware:** The attacker uses a virus, Trojan and other malicious code and installs them on the victim's computer to get unprivileged access. These softwares keep sending data to the hacker regularly and can also perform various tasks on victim's system like sniffing your data and diverting traffic etc.

MODULE - 1

PART – 6: FIREWALLS

Firewall Basics

- A **firewall** is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.



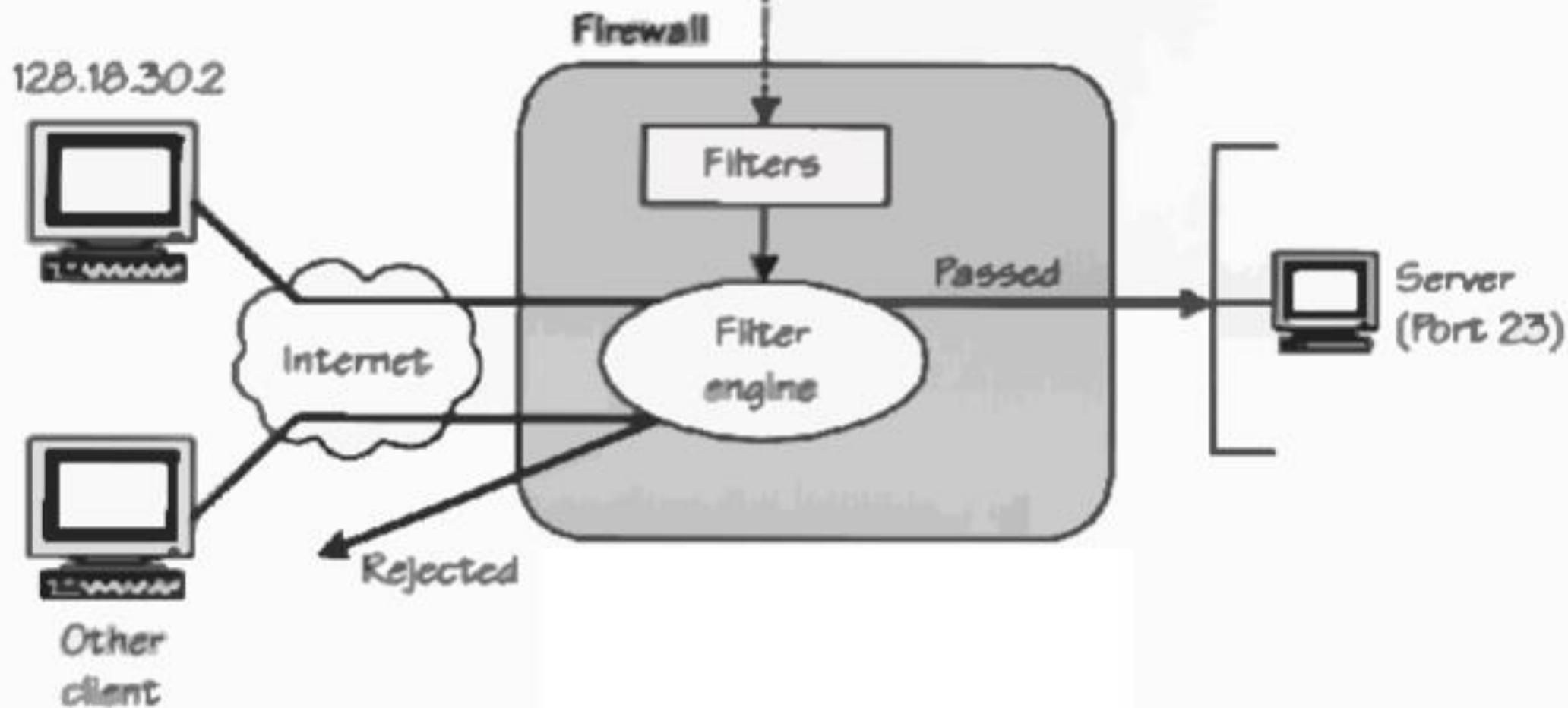
Firewall Types

1. Packet Filtering Firewalls

- Packet Filtering Firewall operates at the network layer of OSI model. Packet filters look only at the headers of the packets.
- It is responsible for filtering (inspecting) data packets coming into the network based on an established rule-set (or criteria) – like allowing data from only certain IP addresses, packet types, port numbers etc.
- For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol or restrict all traffic arriving at firewall except for port 80 (the standard http port).
- ***Advantages:*** Low Cost, Lower Resource Usage and best suited for Smaller Networks.
- ***Disadvantages:*** Hard to configure complex filtering rules, Vulnerable to IP address spoofing, don't support user authentication of connections.

Example filters:

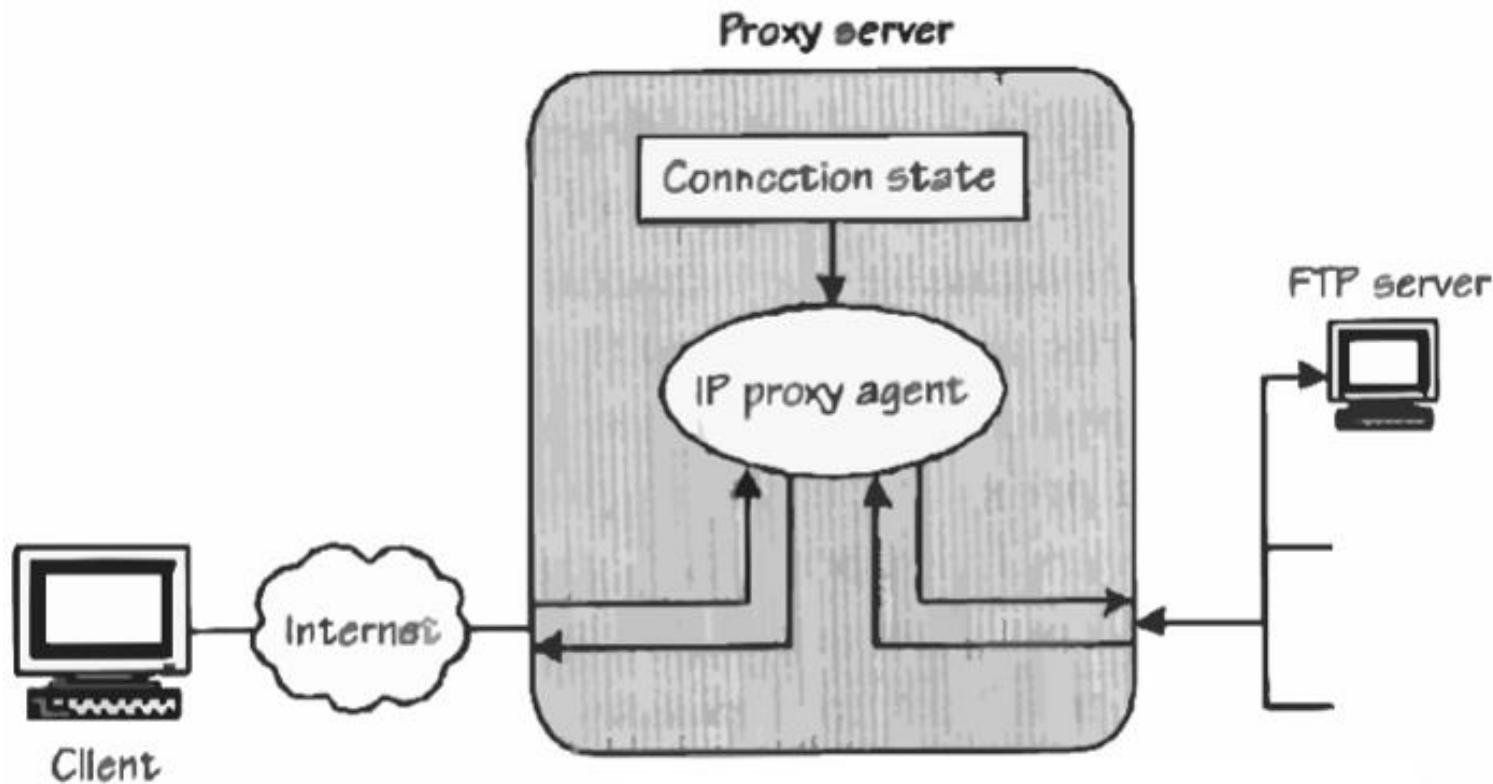
<u>Do</u>	<u>Protocol</u>	<u>Source</u>	<u>Destination</u>
Deny	TCP	All	Inside Port 23
Permit	TCP	128.18.30.2	Inside Port 23



2. Circuit Level Firewalls

- Circuit level firewalls are deployed at the Session layer of the OSI model. It closely monitors the TCP three way handshake between remote host and internal user to determine whether a requested session is legitimate.
- If so, the gateway establishes a connection. From this point on, the circuit-level gateway simply copies and forwards packets back and forth without further filtering them.
- The gateway maintains a table of established connections, allowing data to pass when session information matches an entry in the table.
- Circuit Level Firewalls are also called **pipe proxies** because they establish a virtual circuit, or pipe, between two networks and then allow packets to pass through this pipe. They do not examine the application data like application gateway.
- They put their own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

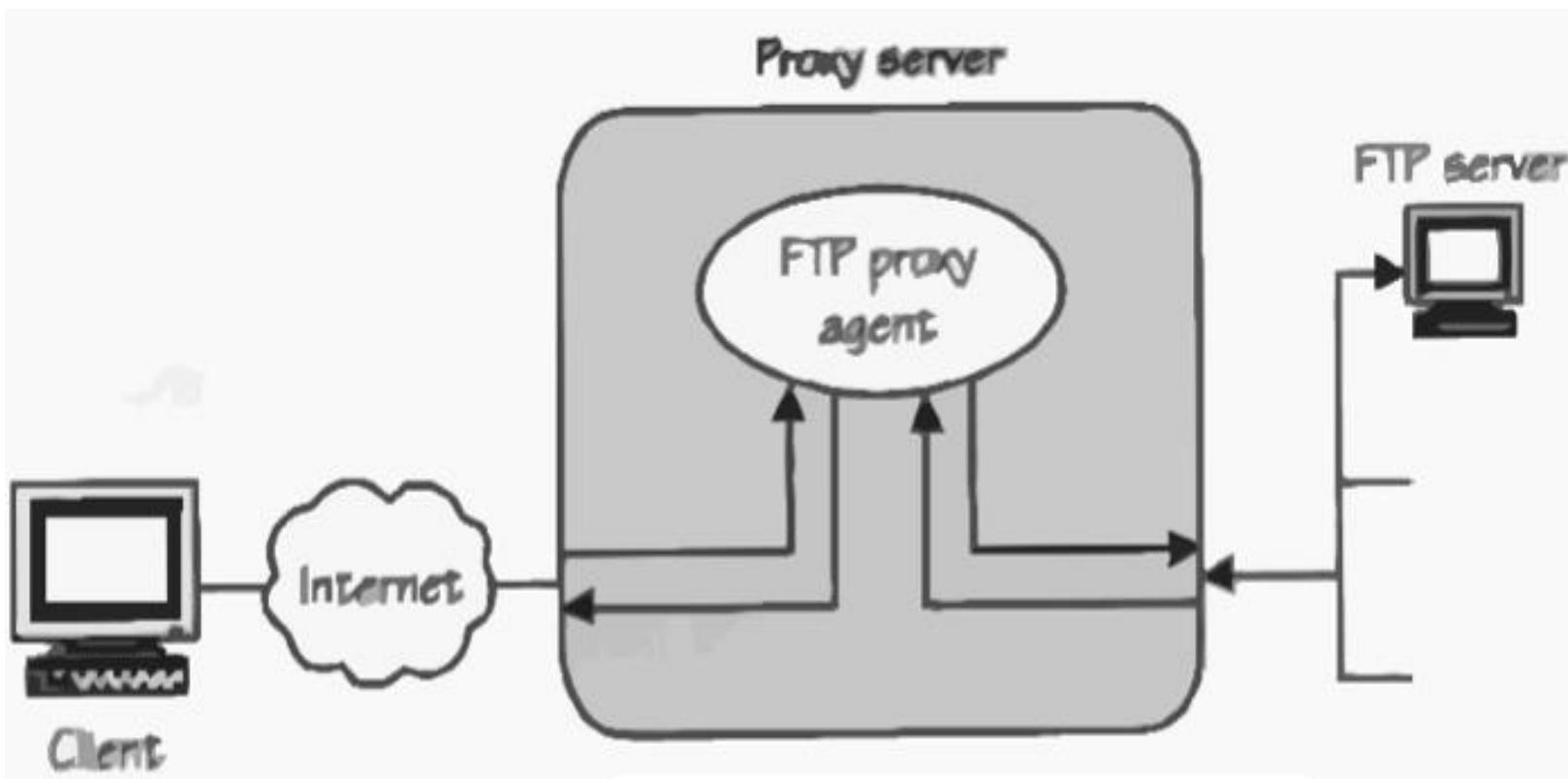
- **Advantages:** More secure than Packet Filtering Firewalls, Provide anonymity to the private network.
- **Disadvantages:** Circuit level Gateways do not filter Individual Packets. An attacker can hijack a session and take advantage of this.



3. Application Level Firewalls

- Like a circuit-level firewall, an application-level firewall runs proxies that copy and forward information across the gateway, and functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host.
- However, the proxies that an application-level firewall runs differ in two important ways from the pipe proxies that a circuit-level firewall uses:
 - a. The proxies are application specific.
 - b. The proxies can filter packets at the application layer.
- **Application-specific Proxies.** Unlike pipe proxies, application-specific proxies accept only packets generated by services they are designed to copy, forward, and filter. For example, only a Telnet proxy can copy, forward, and filter Telnet traffic. All other services would be blocked.

- **Application-level Filtering.** Application-specific proxies check each packet that passes through the firewall, verifying the contents of the individual packets. These proxies can filter particular kinds of commands or information in the application protocols the proxies are designed to handle.



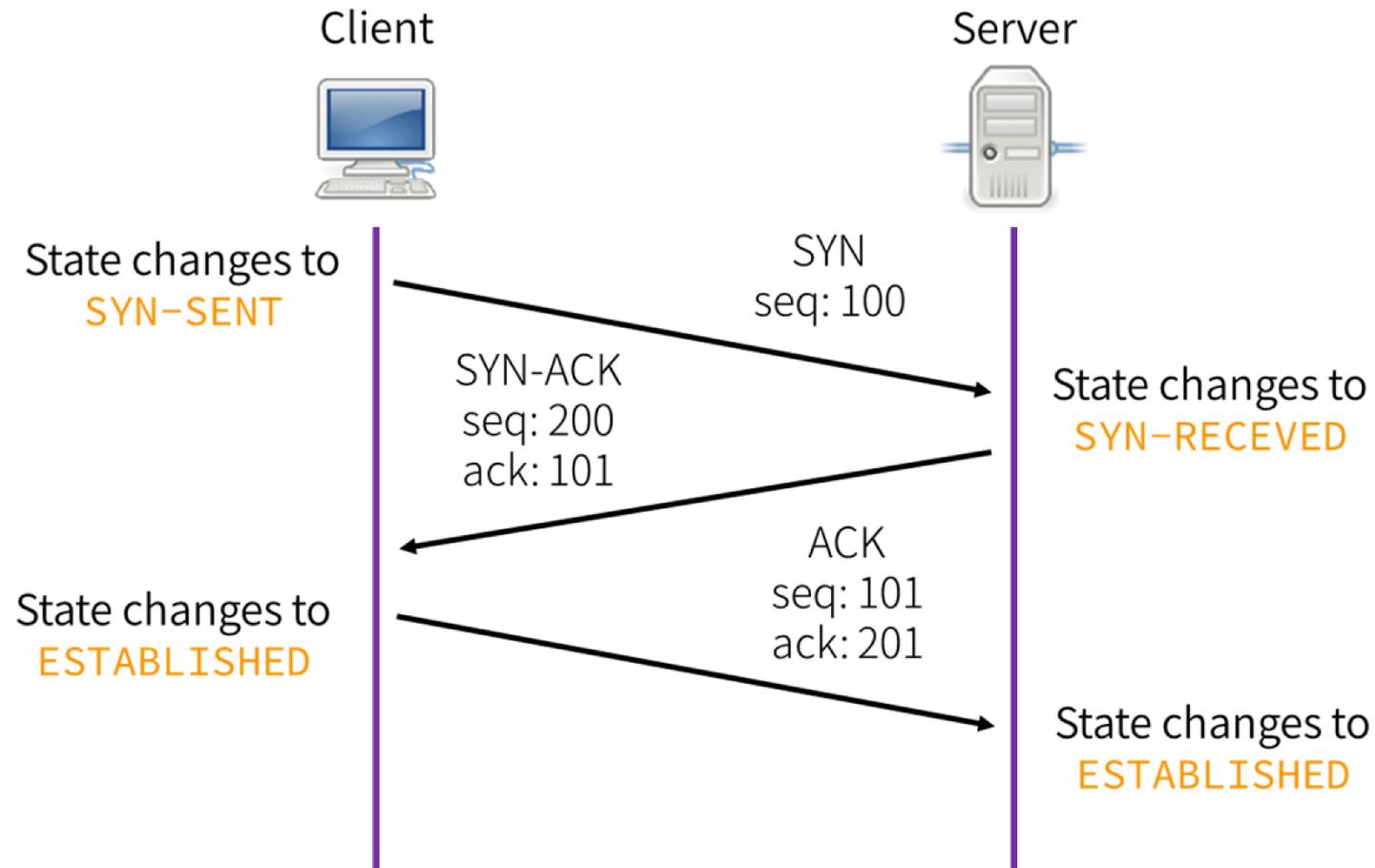
- For example, the firewall could be configured to prevent users from performing the FTP put command. This command lets users write to the FTP server. Prohibiting this action can prevent serious damage of the information stored on the server.
- ***Advantages***. More security than Circuit Level Firewalls, Filter application specific commands.
- ***Disadvantages***: Vendors must keep up with latest protocols, Require great memory and processor resources.

4. Stateful Inspection Firewalls

- A stateful inspection firewall combines aspects of a packet-filtering firewall, a circuit-level firewall, and an application-level firewall.
- Like a packet-filtering firewall, a stateful inspection firewall operates at the network layer of the OSI model, filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers.
- A stateful inspection firewall also functions as a circuit-level firewall, determining whether the packets in a session are appropriate. For example, a stateful inspection firewall verifies that SYN and ACK flags and sequence numbers are logical.
- A stateful inspection firewall mimics an application-level firewall: The firewall evaluates the contents of each packet at the application layer and ensures that these contents match the rules in a company's network security policy.

- A stateful inspection firewall does not require two connections unlike a proxy server, allowing a direct connection between a trusted client and an untrusted host.
- ***Advantages:*** More secure than packet filtering firewalls, Improved performance compared to packet filters and proxy servers
- ***Disadvantages:*** Complex, Less secure than proxy servers because it allows direct connection between trusted client and untrusted host

IMP RELATED INFO



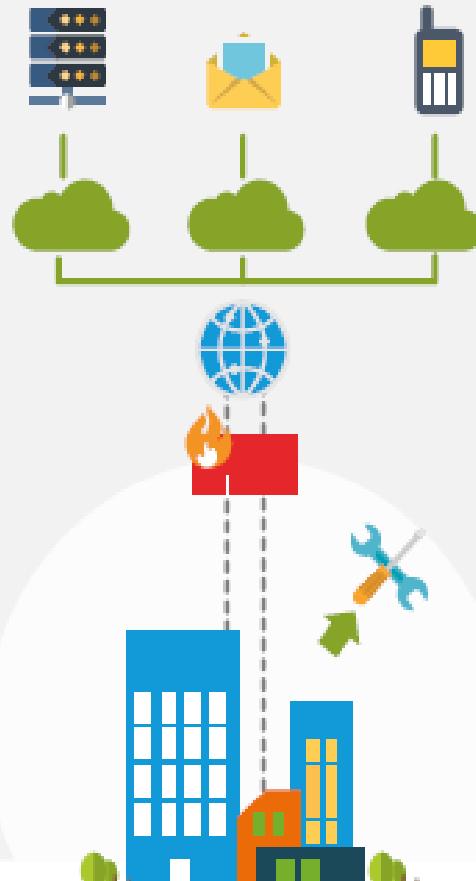
TCP 3-WAY HANDSHAKE

MODULE - 1

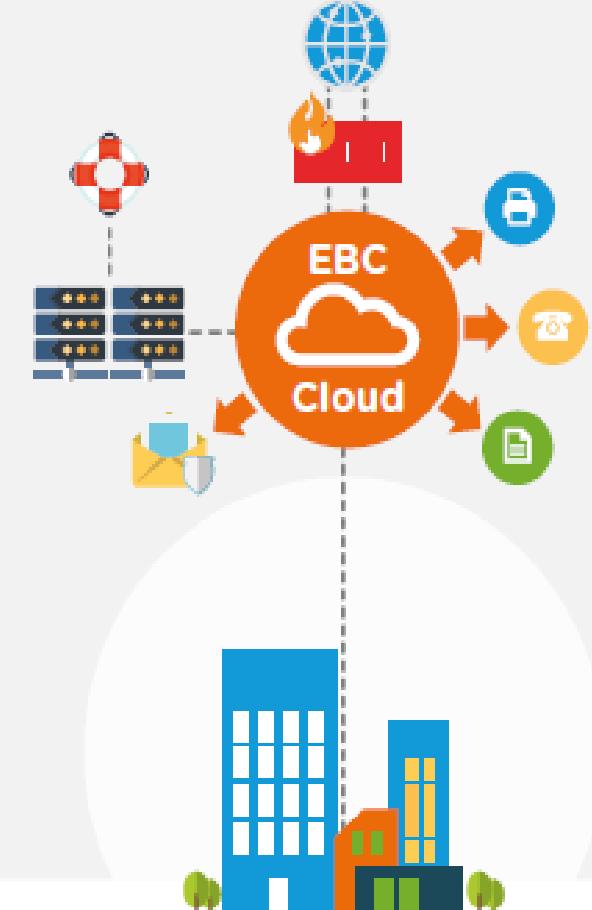
PART – 7: IDENTITY & ACCESS MGMT.



On Premise



Public Cloud



Private Cloud

Identity and Access Management

- Businesses leaders and IT departments are under increased regulatory and organizational pressure to protect access to corporate resources.
- As a result, they can no longer rely on manual and error-prone processes to assign and track user privileges.
- IAM automates these tasks and enables granular access control and auditing of all corporate assets on premises and in the cloud.
- Identity and access management (IAM) is a collective term that covers products, processes, and policies used to manage user digital identities and regulate user access within an organization.

Identity and Access Management

On a fundamental level, IAM encompasses the following components:

- how individuals are identified in a system;
- how roles are identified in a system and how they are assigned to individuals;
- adding, removing and updating individuals and their roles in a system;
- assigning levels of access to individuals or groups of individuals; and
- protecting the sensitive data within the system and securing the system itself.

Identity and Access Management

- Most IAM technology applies ***Role-Based Access Control*** (RBAC) - using predefined job roles to control access to individual systems and information.
- As users join or change roles in the enterprise, their job role is updated, which should impact their access rights.
- There are many technologies to simplify password management and other aspects of IAM. Some of them are:
 - a. **Single Sign-On:** An access and login system that allows users to authenticate themselves once and then grants them access to all the software, systems, and data they need without having to log into each of those areas individually.
 - b. **Two-Factor Authentication:** In addition to your password/username combo, you're asked to verify who you are with something that you own, such as a mobile phone. Put simply: it uses two factors to confirm it's you.

Identity and Access Management

- c. **Multi-Factor Authentication:** This system uses a combination of something the user knows (e.g. a password), something the user has (e.g. a security token), and something the user is (e.g. a fingerprint) to authenticate individuals and grant them access.
 - d. **Privileged access management:** It consists of the cybersecurity strategies and technologies for exerting control over the elevated (“privileged”) access and permissions for users across an IT environment. One of the central goals is the enforcement of *least privilege*.
- IAM technology can be provided on-premises, through a cloud-based model (i.e. identity-as-a-service, or IDaaS).
 - Practical applications of IAM, and how it is implemented, differ from organization to organization, and will also be shaped by applicable regulatory and compliance initiative.

Identity and Access Management

Sophisticated IAM technology can move beyond simply allowing or blocking access to data and systems. For example, IAM can:

- Restrict access to subsets of data: Specific roles can access only certain parts of systems, databases, and information.
- Only allow view access: Roles can only view data, they cannot add, update, or amend it.
- Only permit access on certain platforms: Users may have access to operational systems, but not development or testing platforms.
- Only allow access to create, amend, or delete data, not to transmit it: Some roles may not be able to send or receive data outside the system, meaning it cannot be exposed to other third parties and applications.

CAT 2

MODULE - 2

PART – 1: SYSTEM VULNERABILITIES

System Vulnerabilities

- **System vulnerability** is a flaw or weakness in a system or network that could be exploited to cause damage, or allow an attacker to manipulate the system in some way.
- It's important to know that vulnerabilities are present in virtually every network—there is no way to identify and address them all because of the incredibly complex nature of modern network architecture.
- However, you can significantly reduce your risk of a data breach or similar event by knowing some of the most common network vulnerabilities are and finding ways to address them.
- Computer security vulnerabilities can be divided into numerous types based on different criteria—such as where the vulnerability exists, what caused it, or how it could be used.

System Vulnerabilities

- There are many causes of vulnerabilities including:
 1. **Complexity:** Complex systems increase the probability of a flaw, misconfiguration or unintended access.
 2. **Familiarity:** Common code, software, operating systems and hardware increase the probability that an attacker can find or has information about known vulnerabilities.
 3. **Connectivity:** The more connected a device is the higher the chance of a vulnerability.
 4. **Poor password management:** Weak passwords can be broken with brute force and reusing passwords can result in one data breach becoming many.
 5. **Operating system flaws:** Like any software, operating systems can have flaws. Operating systems that are insecure by default and give all users full access can allow viruses and malware to execute commands.

System Vulnerabilities

6. **Internet usage:** The Internet is full of spyware and adware that can be installed automatically on computers.
7. **Software bugs:** Programmers can accidentally or deliberately leave an exploitable bug in software.
8. **Unchecked user input:** If your website or software assume all input is safe it may execute unintended SQL commands.
9. **People:** The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest threat to the majority of organizations.

System Vulnerabilities

- **Vulnerability management** is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.
- Vulnerability management software can help automate this process. They'll use a *vulnerability scanner* and sometimes *endpoint agents* to inventory a variety of systems on a network and find vulnerabilities on them.
- The vulnerability management process can be broken down into the following four steps as shown below.

Step 1: Identifying Vulnerabilities

- At the heart of a typical vulnerability management solution is a vulnerability scanner. The scan consists of four stages:
 1. Scan network-accessible systems by pinging them or sending them TCP/UDP packets

System Vulnerabilities

2. Identify open ports and services running on scanned systems
 3. If possible, remotely log in to systems to gather detailed system information
 4. Correlate system information with known vulnerabilities by using a vulnerability database.
- **Vulnerability scanners** can sometimes disrupt the networks and systems that they scan. If this is true in your case, then vulnerability scans should be scheduled to run during off hours.
 - **Endpoint agents** allow vulnerability management solutions to continuously gather vulnerability data from systems without performing network scans. This helps organizations maintain up-to-date system vulnerability data whether or not, for example, employees' laptops are connected to the organization's network.

A **vulnerability database** is a platform aimed at collecting, maintaining, and disseminating information about discovered computer security vulnerabilities.

System Vulnerabilities

- Vulnerability scanners aren't perfect. Their vulnerability detection false-positive rates, while low, are still greater than zero. Performing vulnerability validation with **penetration testing** tools and techniques helps weed out false-positives so organizations can focus their attention on dealing with real vulnerabilities.

Step 2: Evaluating Vulnerabilities

- After vulnerabilities are identified, they need to be evaluated so the risks posed by them are dealt with appropriately and in accordance with an organization's risk management strategy.
- Vulnerability management solutions will provide different risk ratings and scores for vulnerabilities, such as **Common Vulnerability Scoring System** (CVSS) scores. These scores are helpful in telling organizations which vulnerabilities they should focus on first.

System Vulnerabilities

Step 3: Treating Vulnerabilities

- Once a vulnerability has been validated and deemed a risk, the next step is prioritizing how to treat that vulnerability. There are different ways to treat vulnerabilities.
 - 1. Remediation:** Fully fixing or patching a vulnerability so it can't be exploited. This is the ideal treatment option that organizations strive for.
 - 2. Mitigation:** Lessening the likelihood and/or impact of a vulnerability being exploited. This is sometimes necessary when a proper fix or patch isn't yet available for an identified vulnerability.
 - 3. Acceptance:** Taking no action to fix or otherwise lessen the likelihood/impact of a vulnerability being exploited. This is typically justified when a vulnerability is deemed a low risk, and the cost of fixing the vulnerability is substantially greater than the cost of exploiting the vulnerability.

System Vulnerabilities

Step 4: Reporting vulnerabilities

- Performing regular and continuous vulnerability assessments enables organizations to understand the speed and efficiency of their vulnerability management program over time.
- Vulnerability management solutions typically have different options for exporting and visualizing vulnerability scan data with a variety of customizable reports and dashboards.
- Not only does this help IT teams easily understand which remediation techniques will help them fix the most vulnerabilities with the least amount of effort, or help security teams monitor vulnerability trends over time in different parts of their network, but it also helps support organizations' compliance and regulatory requirements.

MODULE - 2

PART – 2: NETWORK SECURITY

Network Security

- Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems.
- The most basic example of Network Security is *password protection*. You use your username and password to login into a remote system.
- There are many layers to consider when addressing network security across an organization. So your network security hardware, software and policies must be designed to address each area.
- Network security typically consists of three different controls: physical, technical and administrative. They have been explained in the next slide.

Network Security

- **Physical Network Security:** Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, switches and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.
- **Technical Network Security:** Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.
- **Administrative Network Security:** Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Network Security

- We have talked about the different types of network security controls. Now let's take a look at some of the different ways you can secure your network.
- **Firewalls:** Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both.
- **Email security:** Email gateways are the number one threat vector (path) for a security breach. Attackers use social engineering tactics to build sophisticated phishing campaigns to deceive recipients. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.
- **Anti-virus and anti-malware software:** Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Network Security

- **Network segmentation:** Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.
- **Access control:** Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control.
- **Application security:** Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Network Security

- **Behavioral analytics:** To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.
- **Data loss prevention:** Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.
- **Intrusion prevention systems:** An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.

Network Security

- **Mobile device security:** Cybercriminals are increasingly targeting mobile devices and apps. Within the next few years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.
- **Security information and event management:** SIEM is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, etc. and stores, analyzes and reports on the data to discover trends, detect threats, and enable organizations to investigate any alerts.
- **VPN:** A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Network Security

- **Web Security:** A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. Web security also refers to the steps you take to protect your own website.
- **Wireless security:** Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

MODULE - 2

PART – 3: SYSTEM SECURITY

System Security

- Security of a computer system is a crucial task. It is a process of ensuring confidentiality and integrity of the OS.
- A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of the various malicious threats and unauthorized access.
- System Security is concerned with three main areas:
 - a. **Confidentiality:** Only authorized users can access the data resources and information.
 - b. **Integrity:** Only authorized users should be able to modify the data when needed.
 - c. **Availability:** All the resources of the system must be accessible to all the authorized users.

System Security

- There are many kinds of attacks available to the dedicated hacker. These are among the most famous and frequent types of attacks.
 - a. Denial of service
 - b. Malware attack
 - c. Man in the middle
 - d. Phishing
 - e. Eavesdropping
 - f. Password attack
 - g. SQL injection

System Security

- How Do You Secure Your Computer?
 - a. **Secure passwords:** Create strong passwords so that no one will be able to hack or guess your password.
 - b. **Regular updates:** Always keep your system and all its software updated. Many updates contain additional defenses against cyber attacks.
 - c. **Antivirus:** Antivirus is a computer program used to prevent, detect, and remove malware. Examples of antivirus include Norton, Quickheal, and McAfee.
 - d. **Firewall:** A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.
 - e. **Anti-phishing tactics:** When you get an email that looks suspicious then do not click on the link in the mail or do not open the attached file(s).

System Security

- f. **Backup:** This is done by saving a copy of your existing data on an external hard-disk so that if your device is stolen or compromised, your backup data would be a savior.
- g. **Protecting Wireless Network:** Make sure that your wireless network is secured. Use a strong password for better security.
- h. **Don't disclose your personal information:** Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money.
- i. **Change passwords regularly:** Periodically change your passwords.
- j. **Give Personal Information over Encrypted Websites Only:** If you're shopping or banking online, stick to sites that use encryption to protect your information. To determine if a website is encrypted, look for https at the beginning of the web address.

MODULE - 2

PART – 4: WEB SECURITY

WEB SECURITY

- Website security is any action or application taken to ensure website data is not exposed to cybercriminals or to prevent exploitation of websites in any way.
- Website security protects your website from:
 - a. **DDoS attacks:** These attacks can slow or crash your site entirely, making it inaccessible to visitors.
 - b. **Malware:** Malware is a very common threat used to steal sensitive customer data, distribute spam, allow cybercriminals to access your site, and more.
 - c. **Blacklisting:** Your site may be removed from search engine results and flagged with a warning that turns visitors away if search engines find malware.
 - d. **Vulnerability exploits:** Cybercriminals can access a site and data stored on it by exploiting weak areas in a site, like an outdated plugin.
 - e. **Defacement:** This attack replaces your website's content with a cybercriminal's malicious content.

WEB SECURITY

- Website security protects your visitors from:
 - a. **Stolen data.** From email addresses to payment information, cybercriminals frequently go after visitor or customer data stored on a site.
 - b. **Phishing schemes.** Phishing doesn't just happen in email – some attacks take the form of web pages that look legitimate but are designed to trick the user into providing sensitive information.
 - c. **Session hijacking.** Some cyberattacks can take over a user's session by stealing the user's session key (session ID).
 - d. **Malicious redirects.** Certain attacks can redirect visitors from the site they intended to visit to a malicious website.
 - e. **SEO Spam.** Unusual links, pages, and comments can be put on a site to confuse your visitors and drive traffic to malicious websites.

WEB SECURITY

What do I need to secure my website?

An SSL certificate

- SSL certificates protect the data collected by your website, like emails and credit card numbers, as it is transferred from your site to a server.
- This is a basic website security measure, but it's so important that popular browsers and search engines are now labeling sites without SSL as "insecure," which could make visitors suspicious of your site.
- Depending on your site, you may be able to get an SSL certificate for free, but be sure to choose the SSL certificate that's best for your site.
- Remember that SSL only protects data in transit, so you'll need to take further steps for a fully secure website.

WEB SECURITY

A web application firewall (WAF)

- A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- It typically protects web applications from attacks such as cross-site-scripting (XSS) and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks.
- By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. A WAF is a type of *reverse-proxy*, protecting the server from exposure by having clients pass through the WAF before reaching the server.

WEB SECURITY

A website scanner

- A cyberattack costs more the longer it takes to be found, so time is of the essence when a site experiences an attack.
- A website scanner looks for malware, vulnerabilities and other security issues so that you can mitigate them appropriately.
- An efficient scanner not only removes known malware, it also looks for threats on a daily basis and lets you know the moment anything is found, reducing the amount of damage it can do to your site.

WEB SECURITY

Software updates

- Websites hosted on a content management system (CMS) are at a higher risk of compromise due to vulnerabilities and security issues often found in third-party plugins and applications.
- These can be prevented by installing updates to plugins and core software in a timely manner, as these updates often contain security patches – you can even use an automatic patching solution to make it easier.

IMP CONCEPTS

- **Web Application:** A web app is an application software that runs on a web server, unlike computer-based software programs that are stored locally on the Operating System (OS) of the device. Web applications are accessed by the user through a web browser with an active internet connection.
- **SEO Spam:** Ranking on Google takes a lot of effort but with it comes great benefits. Hackers let you do all the hard work of SEO and digital marketing, and then use your website to promote their product/service. This is why SEO spam is also known as spamdexing or search engine poisoning (SEP).
- **Content Management System (CMS):** CMS is a software platform that is used to manage web content, allowing multiple contributors to create, edit and publish. In simpler language, a content management system is a tool that helps you build a website without needing to write all the code from scratch (or even know how to code at all).

MODULE - 2

PART – 5: APPLICATION SECURITY

APPLICATION SECURITY

- Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.
- It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed.
- Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities.
- A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security.
- But security measures at the application level are also typically built into the software, such as an application firewall that strictly defines what activities are allowed and prohibited.
- Procedures can entail things like an application security routine that includes protocols such as regular testing.

APPLICATION SECURITY

Why Application Security is needed?

- Application security is important because today's applications are often available over various networks and connected to the cloud, increasing vulnerabilities to security threats and breaches.
- Hackers are going after apps with their attacks more today than in the past. Application security testing can reveal weaknesses at the application level, helping to prevent these attacks.

Types of application security

- ***Authentication:*** When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a user name and password when logging in to an application.

APPLICATION SECURITY

- ***Authorization:*** After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users.
- ***Encryption:*** After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. When traffic containing sensitive data travels between two devices, that traffic can be encrypted to keep the data safe.
- ***Logging:*** If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- ***Application security testing:*** A necessary process to ensure that all of these security controls work properly.

APPLICATION SECURITY

What are application security controls?

- Application security controls are techniques to enhance the security of an application at the coding level, making it less vulnerable to threats.
- Many of these controls deal with how the application responds to unexpected inputs that a cybercriminal might use to exploit a weakness.
- A programmer can write code for an application in such a way that the programmer has more control over the outcome of these unexpected inputs.
- Fuzzing is a type of application security testing where developers test the results of unexpected values or inputs to discover which ones cause the application to act in an unexpected way that might open a security hole.

IMP CONCEPTS

What is application security testing?

- Application developers perform application security testing as part of the software development process to ensure there are no security vulnerabilities in a new or updated version of a software application.
- A security audit can make sure the application is in compliance with a specific set of security criteria. After the application passes the audit, developers must ensure that only authorized users can access it.
- ***Static Application Security Testing*** (SAST) scans the application source files, accurately identifies the root cause and helps remediate the underlying security flaws. This is useful for developers to check their code as they are writing it.
- ***Dynamic Application Security Testing*** (DAST) simulates controlled attacks on a running web application or service to identify exploitable vulnerabilities in a running environment.

MODULE - 2

PART – 6: INTRUSION DETECTION SYSTEM

Intrusion Detection System

- An **Intrusion Detection System** (IDS) is a device or software application that monitors a network/system for suspicious activities and known threats. Any suspicious activity or threat is typically reported or collected centrally using a Security Information and Event Management (SIEM).
- IDS can be broken into two broad categories: network-based and host-based.

Network Intrusion Detection System (NIDS)

- A Network Intrusion Detection System (NIDS) is generally deployed or placed at strategic points throughout the network, intended to cover those places where traffic is most likely to be vulnerable to attack.
- Generally, it's applied to entire subnets, and it attempts to match any traffic passing by to a library of known attacks. It passively looks at network traffic coming through the points on the network on which it's deployed.

Intrusion Detection System

- Network-based intrusion detection system software analyzes a large amount of network traffic, which means they sometimes have low specificity.
- This means sometimes they might miss an attack or might not detect something happening in encrypted traffic. In some cases, they might need more manual involvement from an administrator to ensure they're configured correctly.
Example of NIDS: **SNORT**.

Host Intrusion Detection System (HIDS)

- The Host Intrusion Detection System (HIDS) runs on all the devices in the network with access to the internet and other parts of the enterprise network.
- HIDS have some advantages over NIDS, due to their ability to look more closely at internal traffic, as well as working as a second line of defense against malicious packets a NIDS has failed to detect.

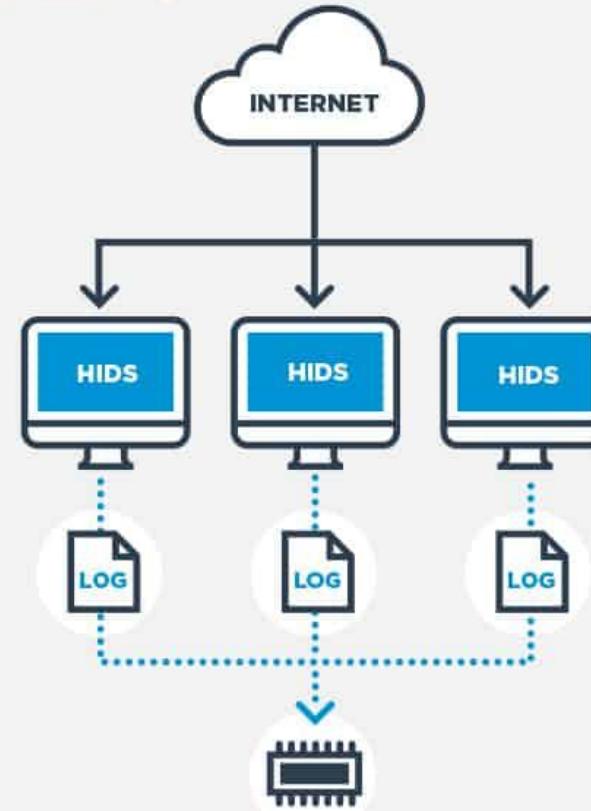
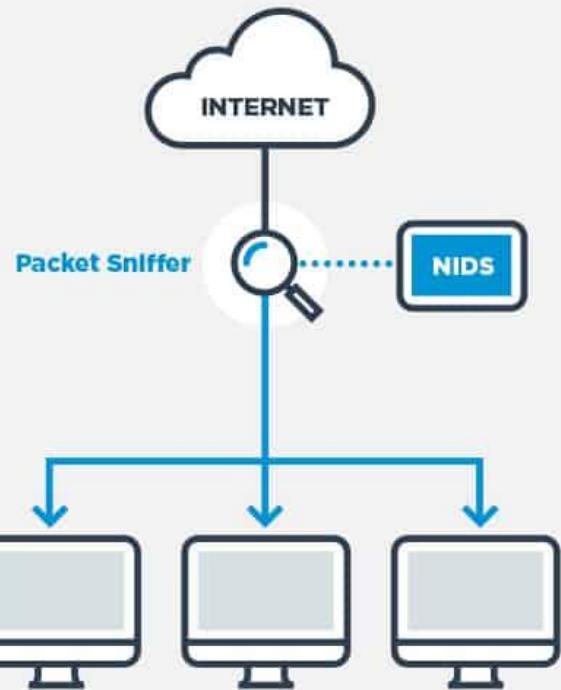
Intrusion Detection System

- It looks at the entire system's file set and compares it to its previous "snapshots" of the file set. It then looks at whether there are significant differences outside normal business use and alerts the administrator as to whether there are any missing or significantly altered files or settings.
- There are also two main approaches to detecting intrusion: signature-based IDS and anomaly-based IDS.

Signature-Based IDS

- This type of IDS is focused on searching for a "signature," patterns, or a known identity, of an intrusion or specific intrusion event. Most IDS are of this type.
- It needs regular updates of what signatures or identities are common at the moment to ensure its database of intruders is current. This means signature-based IDS is only as good as how up to date its database is at a given moment.

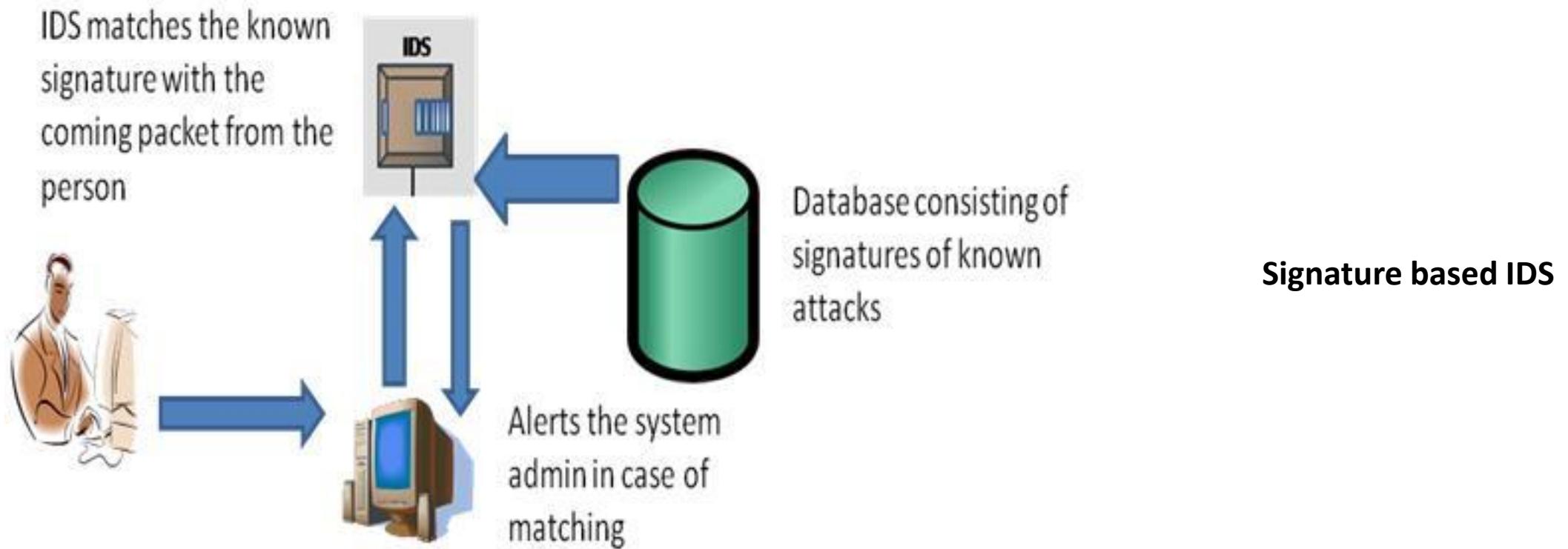
NIDS vs HIDS



NIDS vs HIDS

Intrusion Detection System

- Attackers can get around signature-based IDS by frequently changing small things about how the attack takes place, so the databases cannot keep pace.
- In addition, it means a completely new attack type may not be picked up at all by signature-based IDS because the signature doesn't exist in the database. Signature based IDSe are prone to false negatives.

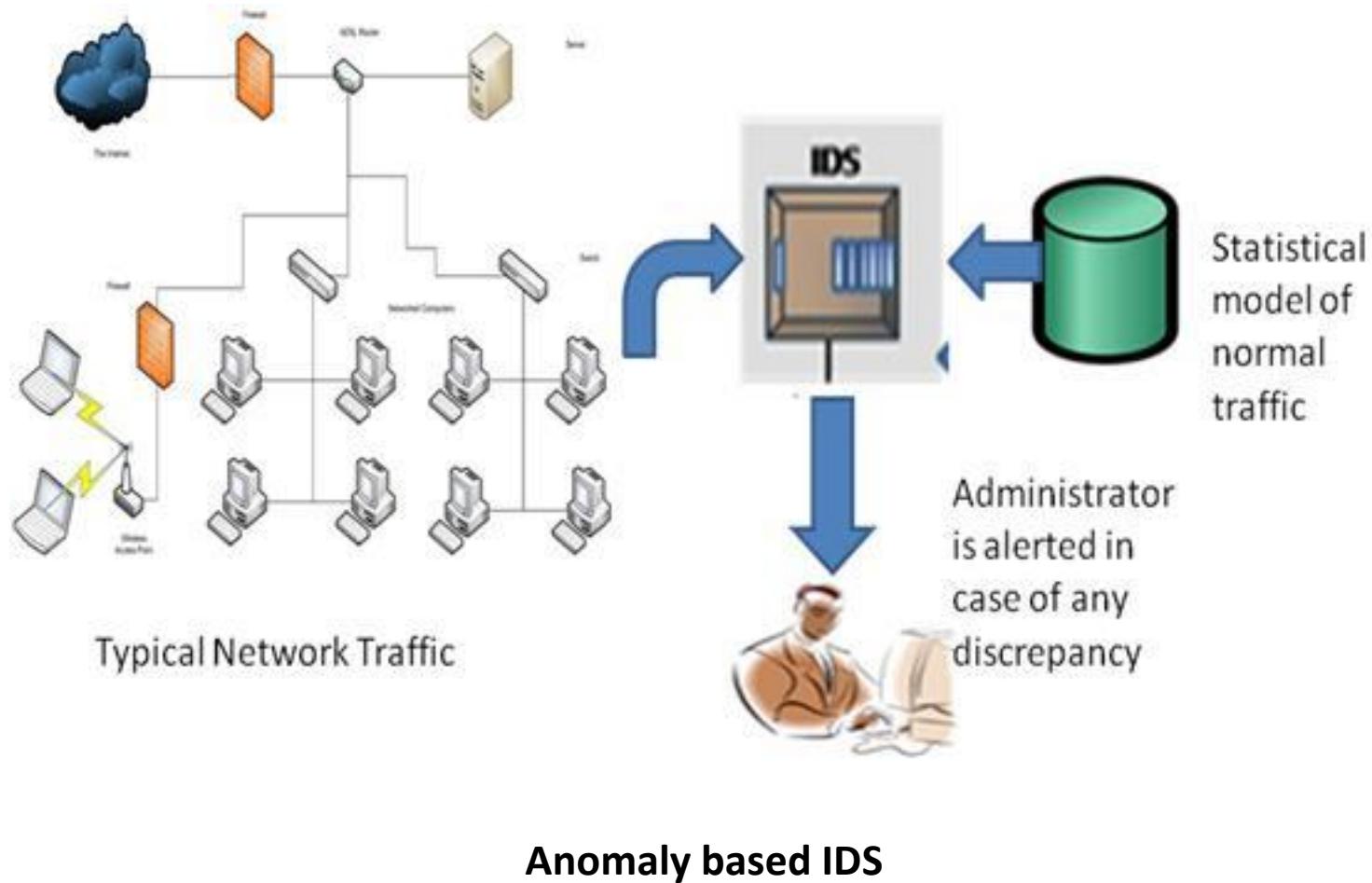


Intrusion Detection System

Anomaly-Based IDS

- Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.
- In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.
- Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.
- However, previously unknown, but legitimate, behavior can be accidentally flagged as well and depending on the response, this can cause some problems. Anomaly based IDSEs are prone to false positives.

Intrusion Detection System



Intrusion Detection System

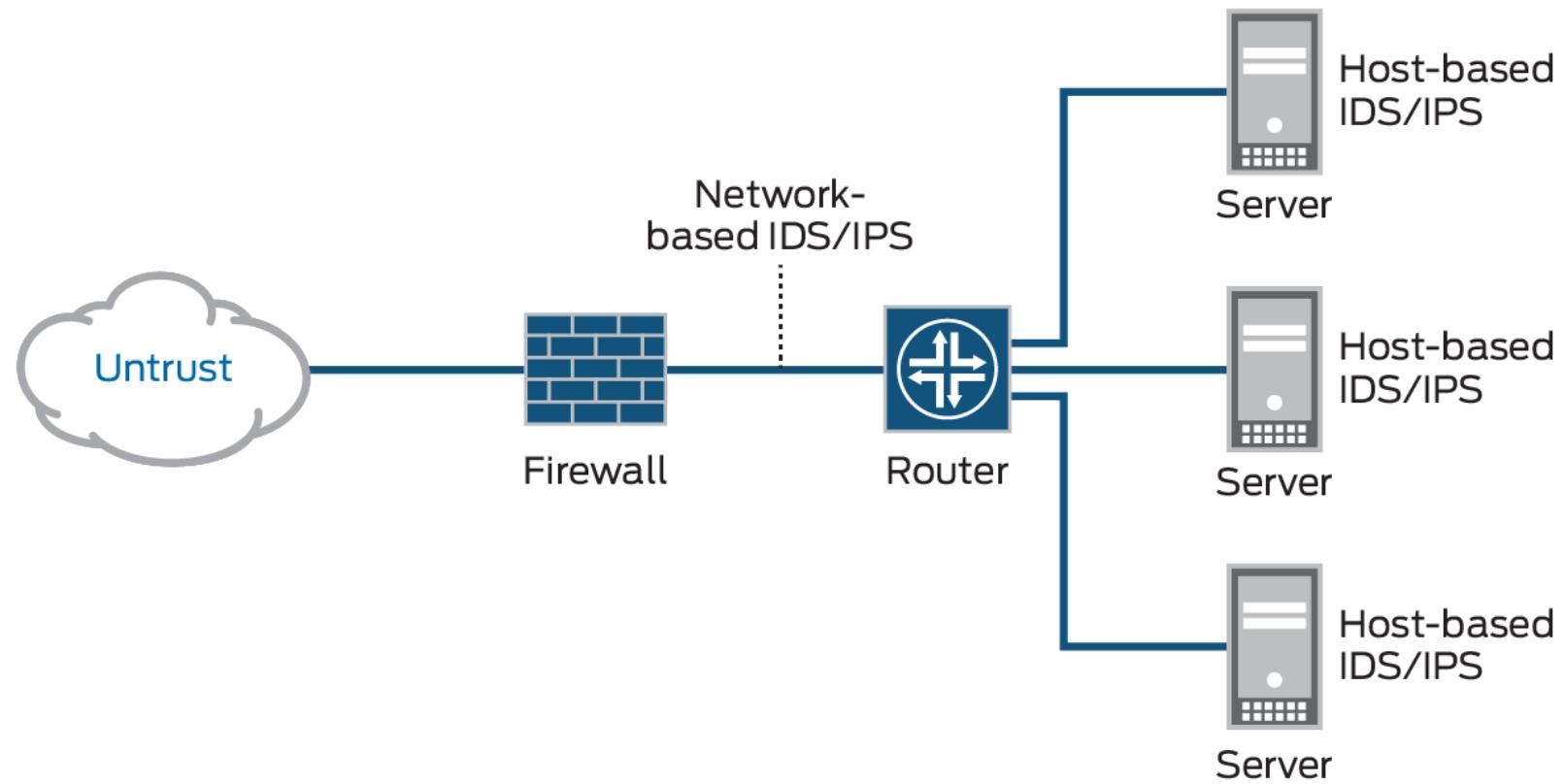
Intrusion Prevention System

- An Intrusion Prevention System (IPS) is a network security/threat prevention technology that identifies malicious activity, collects information about this activity, reports it and attempts to block or stop it.
- IPSes have two predominant methods of detecting malicious activity: signature-based detection and anomaly-based detection.
- There are a number of different threats that an IPS is designed to prevent, including:
 - a. Denial of Service (DoS) attack
 - b. Distributed Denial of Service (DDoS) attack
 - c. Various types of exploits
 - d. Worms
 - e. Viruses

Intrusion Detection System

Intrusion Prevention System

- IPS false positives are more serious than IDS false positives because legitimate traffic is stopped from entering the network in case of IPS. This could impact any part of the organization.
- The IPS performs real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out one of the following actions:
 - a. Terminate the TCP session that has been exploited and block the offending source IP address or user account from accessing any application, target hosts or other network resources unethically.
 - b. Reprogram or reconfigure the firewall to prevent a similar attack occurring in the future.
 - c. Remove or replace any malicious content that remains on the network following an attack.



IDS/IPS deployment in Network

Intrusion Detection System

How is IPS different from Firewall?

- Generally, a firewall is supposed to be configured to block all traffic, and then you set it up to allow specific types through.
- The IDS and IPS work in the opposite direction, by allowing all traffic and then flagging or blocking specific traffic only. As a result, you should use a firewall in combination with an IDS or IPS, not one or the other.
- Set up your firewall to let only specific kinds of traffic through, and then use the IDS to detect anomalies or problems in the traffic you permit. The combination of these tools provides a comprehensive security boundary for your network.

MODULE - 3

PART – 1: INFO. SECURITY MGMT.

Information Security Management

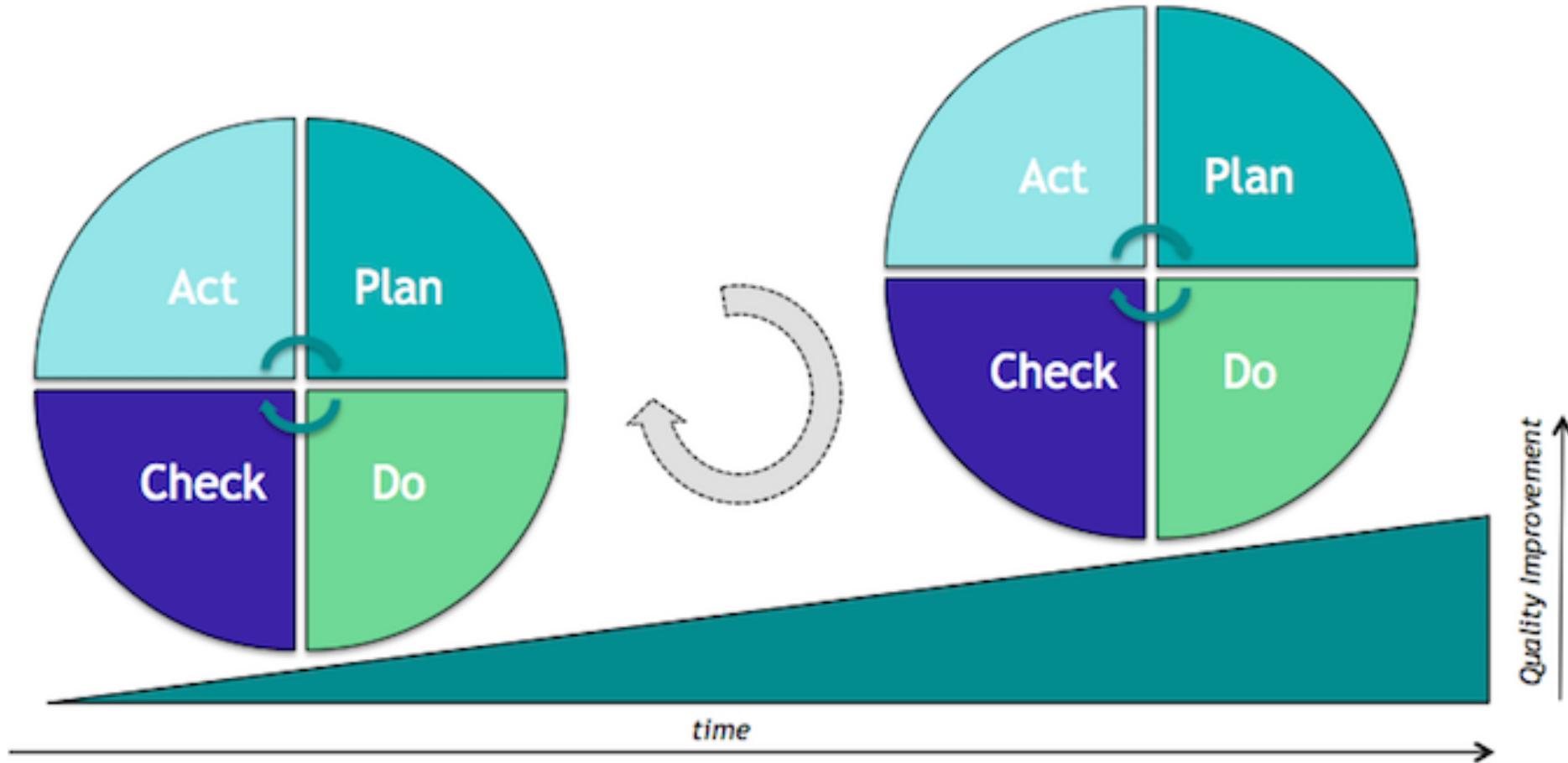
- Business organizations today create, aggregate and store massive amounts of information from their customers, including behavioral analytics, usage data, personal information, credit cards and payment data, health care information and more.
- The increase in enterprise data collection over the past decade, along with the increasing threat of cyber attacks and data breaches, has led to significant developments in the field of Information Security Management for IT organizations.
- ***Information security management*** describes the set of policies and procedural controls that IT and business organizations implement to secure their informational assets against threats and vulnerabilities.

Information Security Management

- Many organizations develop a formal, documented process for managing InfoSec - often called an ***Information Security Management System***, or ISMS.
- The security policies can follow common security standards or be more focused on your industry. For example, ***ISO 27001*** is a set of specifications detailing how to create, manage, and implement ISMS policies and controls.
- The ISO doesn't mandate specific actions; instead, it provides guideline on developing appropriate ISMS strategies.
- The structure and boundaries defined by an ISMS may apply only for a limited time frame.
- Digital transformation requires organizations to evolve their security policies and controls with time so that they don't become obsolete.

Information Security Management

- According to ISO 27001, ISMS implementation follows a ***Plan-Do-Check-Act*** (PDCA) model for continuous improvement in ISM processes:
 1. **Plan.** Identify the problems and collect useful information to evaluate security risk . Define the policies and processes that can be used to address problem root causes.
 2. **Do.** Implement the devised security policies and procedures. The implementation follows the ISO standards, but actual implementation is based on the resources available to your company.
 3. **Check.** Monitor the effectiveness of ISMS policies and controls. Evaluate tangible outcomes as well as behavioral aspects associated with the ISM processes.
 4. **Act.** Focus on continuous improvement. Document the results, share knowledge, and use a feedback loop to address future iterations of the PDCA model implementation of ISMS policies and controls.



PCDA model for continuous improvement

Information Security Management

- Information security at the organizational level is centered around the CIA triad of ***Confidentiality, Integrity and Availability***. Information security controls are put in place to ensure the confidentiality, integrity and availability of protected information.
 - **Confidentiality:** Information security management teams may classify or categorize data based on the perceived risk and anticipated impact that would result if the data was compromised.
 - **Integrity:** For data to be considered secure, the IT organization must ensure that it is properly stored and cannot be modified or deleted without the appropriate permissions.
 - **Availability:** Typical activities include hardware maintenance and repairs, installing patches and upgrades, and implementing incident response and disaster recovery processes to prevent data loss in the event of a cyber attack.

Information Security Management

- An ISO 27001-compliant ISMS does more than simply help you comply with laws and win business. It can also:
 - ***Secure your information in all its forms:*** An ISMS helps protect all forms of information, whether digital, paper-based or in the Cloud.
 - ***Increase your attack resilience:*** Implementing and maintaining an ISMS will significantly increase your organization's resilience to cyber attacks.
 - ***Manage all your information in one place:*** An ISMS provides a central framework for keeping your organization's information safe and managing it all in one place.
 - ***Respond to evolving security threats:*** Constantly adapting to changes both in the environment and inside the organization, an ISMS reduces the threat of continually evolving risks.

Information Security Management

- ***Reduce costs associated with information security:*** Thanks to the risk assessment and analysis approach of an ISMS, organizations can reduce costs spent on indiscriminately adding layers of defensive technology that might not work.
- ***Protect the confidentiality, availability and integrity of your data:*** An ISMS offers a set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of your information.
- ***Improve company culture:*** An ISMS's holistic approach covers the whole organization, not just IT. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.

Information Security Management

- To be ISO 27001 certified means that your organization has successfully passed the external audit and met all compliance criteria. This means you can now advertise your compliance to boost your cybersecurity reputation.



Information Security Management

- The ISO 27001 Standard takes a *risk-based approach* to information security. This requires organizations to identify information security risks and select appropriate controls to tackle them.
- The documentation for ISO 27001 breaks down the best practices into 14 separate controls. Certification audits will cover controls from each one during compliance checks.
 1. **Information Security Policies** – covers how policies should be written in the ISMS and reviewed for compliance.
 2. **Organization of Information Security** – describes what parts of an organization should be responsible for what tasks and actions.
 3. **Human Resource Security** – covers how employees should be informed about cybersecurity when starting, leaving, or changing positions.

ISO 27001 CONTROLS

- 1. Information Security Policies
- 2. Organization of Information Security
- 3. Human Resource Security
- 4. Asset Management
- 5. Access Control
- 6. Cryptography
- 7. Physical and Environmental Security
- 8. Operations Security
- 9. Communications Security
- 10. System Acquisition and Maintenance
- 11. Supplier Relationships
- 12. Security Incident Management
- 13. Business Continuity Management
- 14. Compliance

Information Security Management

4. **Asset Management** – describes the processes involved in managing data assets and how they should be protected and secured.
5. **Access Control** – provides guidance on how employee access should be limited to different types of data.
6. **Cryptography** – covers best practices in encryption.
7. **Physical and Environmental Security** – describes the processes for securing buildings and internal equipment.
8. **Operations Security** – provides guidance on how to collect and store data securely.
9. **Communications Security** – covers security of all transmissions within an organization's network.
10. **System Acquisition, Development and Maintenance** – details the processes for managing systems in a secure environment.

Information Security Management

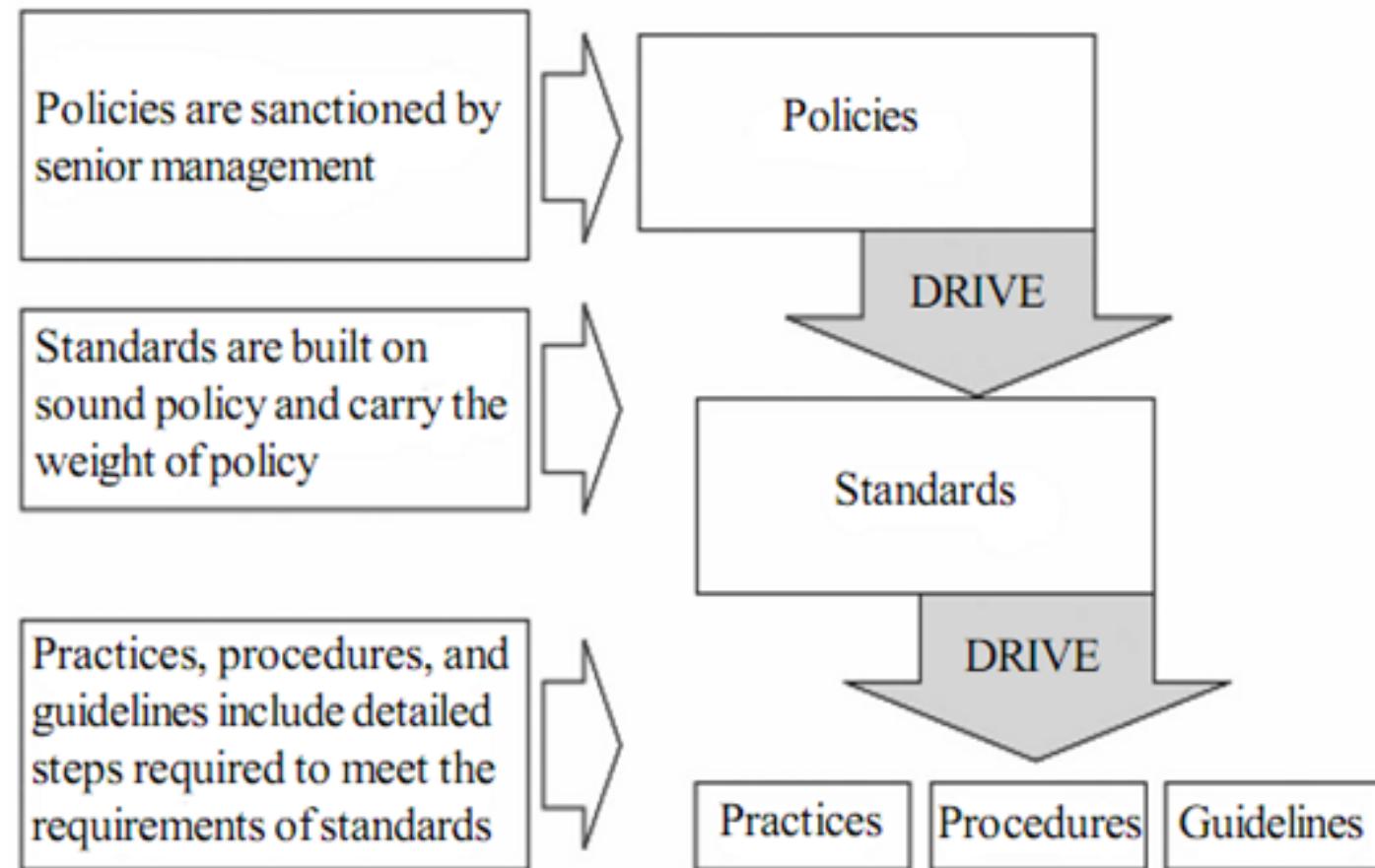
- 11. Supplier Relationships** – covers how an organization should interact with third parties while ensuring security.
- 12. Information Security Incident Management** – describes the best practices for how to respond to security issues.
- 13. Information Security Aspects of Business Continuity Management** – covers how business disruptions and major changes should be handled.
- 14. Compliance** – identifies what government or industry regulations are relevant to the organization, such as ITAR.

MODULE - 3

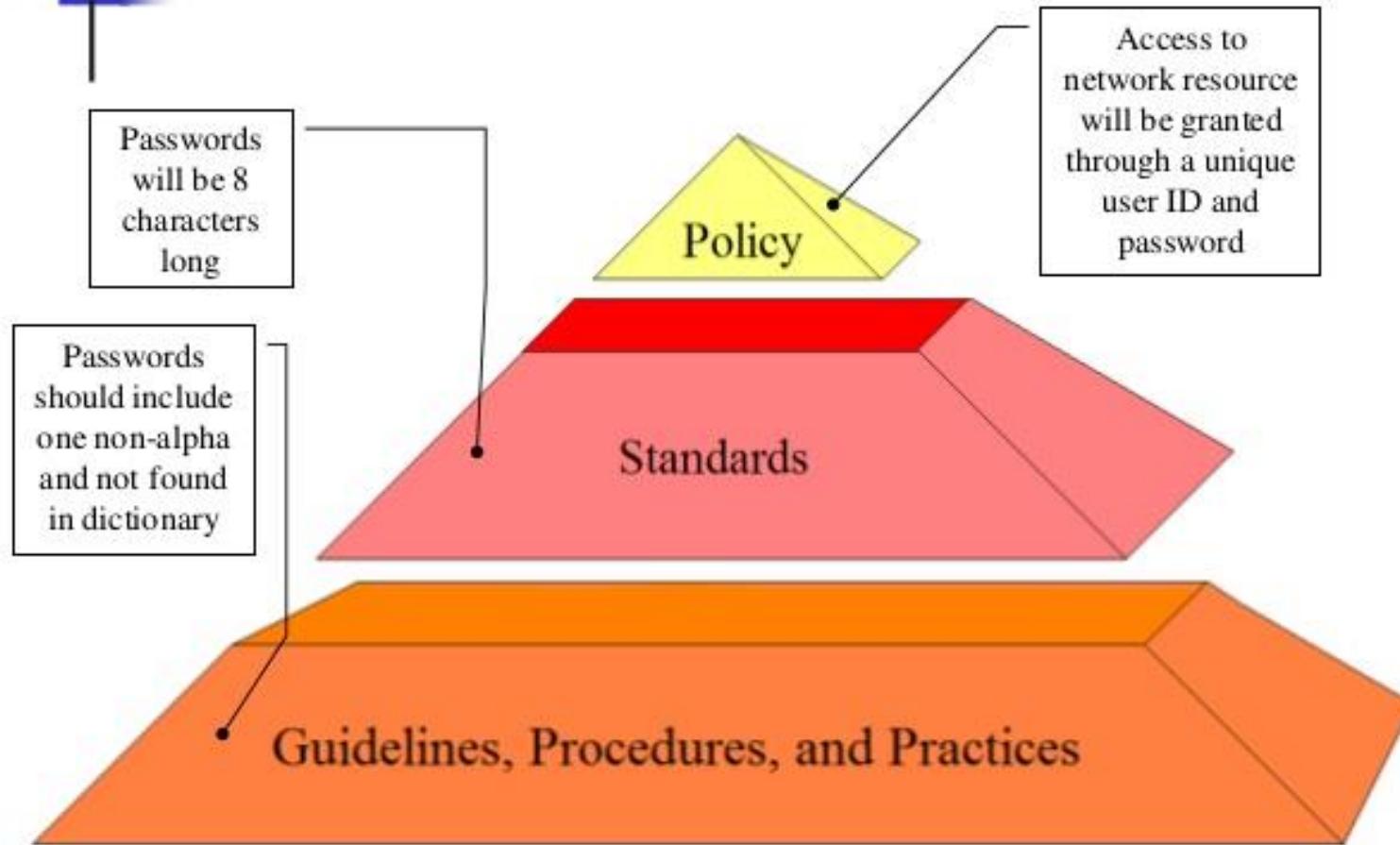
**PART – 2: POLICIES, STANDARDS, GUIDELINES &
PROCEDURES**

Policies, Standards, Guidelines, and Procedures

- Computers and information processed on them have a direct relationship with a company's missions and objectives. Because of this, it is imperative that senior management set in place a code of policies, standards, guidelines, and other procedures.



Security Policy





Policies, Standards, Guidelines, and Procedures

- A **security policy** is an overall statement produced by senior management that dictates what roles security plays within the organization. These policies need to be technology and solution-independent. It must outline the goals and missions, but not tie the organization to specific ways of accomplishing them.
- There are three types of security policies:
 1. **Organizational security policy** is one in which management establishes how a security program will be set up and lays out the programs goals, responsibilities, and enforcement.
 2. **Issue-specific policy**, also called a functional policy, addresses specific security issues that management feels need more detailed explanation and attention.
 3. **System-specific policy** presents the management's decisions that are specific to the actual computers, networks, and applications.

Policies, Standards, Guidelines, and Procedures

- **Standards** provide us with a common set of reference points to enable us to evaluate whether an organization has processes, procedures and other controls in place that meet an agreed minimum requirement.
- If an organization meets a certain standard, then it gives third parties such as customers, suppliers and partners confidence in the organization's ability to deliver to that standard.
- It can also provide an organization with a competitive advantage over other organizations.
- There are numerous standards available. These can be broken down into three main sections.
 1. Business Standards
 2. Product Standards
 3. Individual Standards

Policies, Standards, Guidelines, and Procedures

Business Standards

- Implement the standard.
- Engage a third party to audit you against the standard.
- That third party determines if you meet the standard and whether or not you achieve certification against the standard.

Product Standards

- Select the standard you wish to achieve.
- Submit your product to the company authorized to test your product against that standard.
- Have your product tested and if passed it will be certified (note that this can be a very costly exercise)

Individual Standards

- Select the standard/certification you wish to achieve.
- Study against the requirements.
- Sit an exam
- Pass the exam. Some certifications require verifiable work experience in the field on top of passing the exams.

Policies, Standards, Guidelines, and Procedures

- Standards are often standalone and referenced in policies.
- In your policy, you will find the following statement: “*We use the contract standard to review our contracts*”. In this example, the policy refers to the standard and the standard assists your partner to comply with the policy.
- Exceptions are always to Standards and never to Policies.
- If a standard cannot be met, it is generally necessary to implement a compensating control to mitigate the risk associated with that deficiency.
- However, exceptions to standards are rarely accepted.
- Example: ISO 27001 is an international standard on how to manage information security.

Policies, Standards, Guidelines, and Procedures

- A **Guideline** provides general guidance, and additional advice and support for policies, standards or procedures.
- Guidelines are recommendations to users when specific standards do not apply.
- Guidelines are designed to streamline certain processes according to what the best practices are.
- Guidelines, by nature, should open to interpretation and do not need to be followed to the letter.
- For example, your policy might require a risk analysis every year. Rather than require specific procedures to perform this audit, a guideline can specify the methodology that is to be used, leaving the audit team to work with management to fill in the details.

Policies, Standards, Guidelines, and Procedures

- The following are guidelines to access internet from the Company campus:
 1. Users must refrain from accessing websites that are not secure.
 2. Users are encouraged to verify the authenticity and accuracy of materials received via the Internet.
 3. Users must not download material from the Internet that is subject to copyright or other intellectual property right protections.
 4. When using the Internet from the campus, you are presenting yourself as a representative of the Company and should conduct yourself in accordance with all aspects of Company Policies.

Policies, Standards, Guidelines, and Procedures

- The last step before implementation is creating the **Procedures**.
- These are “*cookbook*” recipes for accomplishing specific tasks necessary to achieve a given goal or mandate. Details are written in step-by-step format from the very beginning to the end.
- These procedures can be used to describe everything from the configuration of operating systems, databases, and network hardware to how to add new users, systems, and software.
- If your organization does not perform software development, procedures for testing and quality assurance are unnecessary.
- However, some types of procedures might be common amongst networked systems:

Policies, Standards, Guidelines, and Procedures

- **Auditing**—These procedures can include what to audit, how to maintain audit logs, and the goals of what is being audited.
- **Access control**—These procedures are an extension of administrative procedures that tell administrators how to configure authentication and other access control features of the various components.
- **Configuration**—These procedures cover the firewalls, routers, switches, and operating systems.
- **Incident response**—These procedures cover everything from detection to how to respond to the incident. These procedures should discuss how to involve management in the response as well as when to involve law enforcement.
- **Physical and environmental**—These procedures cover not only the air conditioning and other environmental controls in rooms where servers and other equipment are stored, but also the shielding of Ethernet cables to prevent them from being tapped.

MODULE - 3

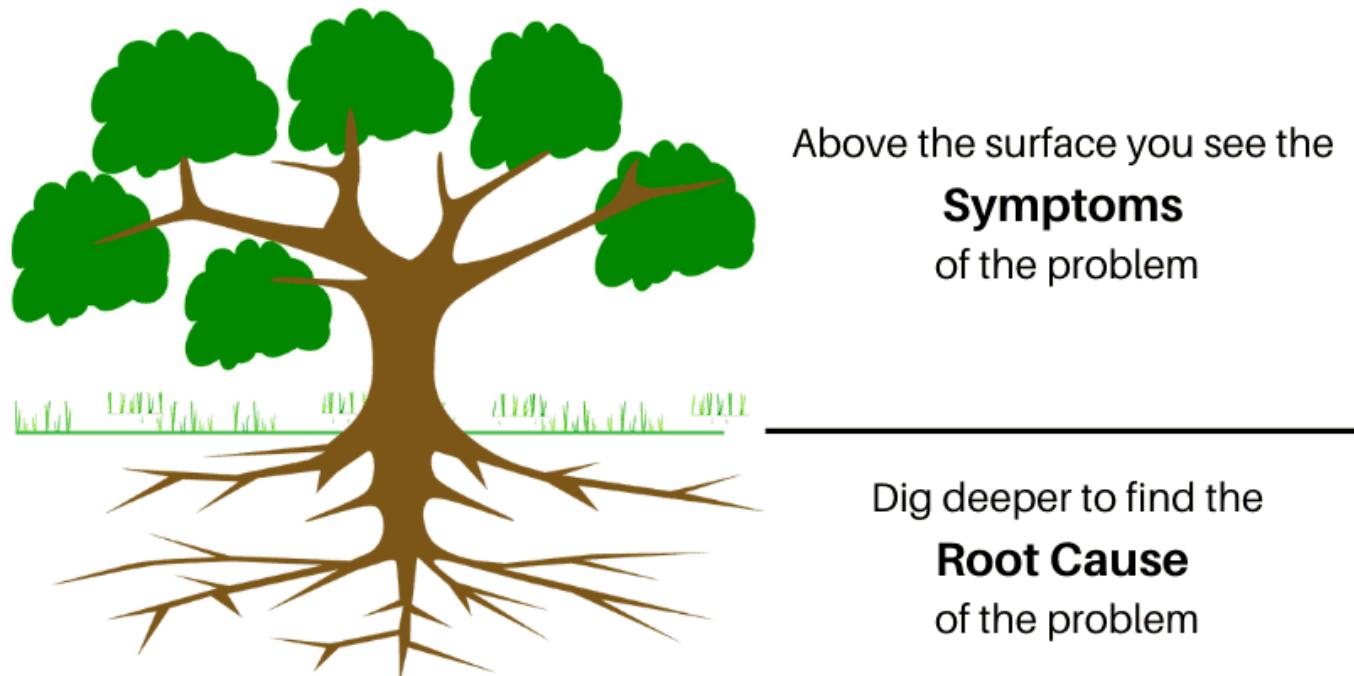
PART – 3: ROOT CAUSE ANALYSIS

What is Root Cause Analysis?

- Root cause analysis (RCA) is a systematic process for finding and identifying the root cause of a problem or event.
- While the term root cause analysis seems to imply that issues have a singular cause, this is not always the case.
- Problems may have a singular cause, or multiple causes stemming from deficiencies in products, people, processes or other factors.
- This method is applied in virtually every industry, but with particular focus and benefits in software development.
- For IT organizations, root cause analysis is a key aspect of the cyber security incident response process.

What is Root Cause Analysis?

- When a security breach occurs, SecOps teams must collaborate quickly to determine where the breach originated, isolate the vulnerability that caused the breach and initiate corrective and preventive actions to ensure the vulnerability cannot be exploited again.



Root Cause Analysis steps

- The following steps are involved in Root Cause Analysis.

1. Define the Problem

- What do you see happening?
- What are the specific symptoms?

2. Collect Data

- What proof do you have that the problem exists?
- How long has the problem existed?
- What is the impact of the problem?
- Meet with people who are familiar and understand the situation. The situation needs to be viewed from different perspectives of those involved.

Root Cause Analysis steps

3. Identify Possible Causal Factors

- What sequence of events leads to the problem?
- What conditions allow the problem to occur?
- What other problems surround the occurrence of the central problem?
- During this stage, identify as many causal factors as possible. Too often, people identify one or two factors and then stop, but that's not sufficient.

4. Identify the Root Cause(s)

- Why does the causal factor exist?
- What is the real reason the problem occurred?
- You can use a variety of RCA techniques like the *5-Whys, Fishbone or Ishikawa Diagram, Pareto Analysis, Brainstorming*.

Root Cause Analysis steps

5. Recommend and Implement Solutions

- What can you do to prevent the problem from happening again?
- How will the solution be implemented?
- Who will be responsible for it?
- What are the risks of implementing the solution?
- Analyze your cause-and-effect process, and identify the changes needed for various systems.
- It's also important that you plan ahead to predict the effects of your solution. This way, you can spot potential failures before they happen.

Root Cause Analysis Tools

- The two most important tools for RCA in cloud computing environments are *Five Whys Analysis* and *Fishbone/Ishikawa Diagram Analysis*.

Five Whys Analysis

- The "Five Whys" method of root cause analysis is an investigative technique that encourages the practitioner to repeatedly ask "Why?" to get to the deepest chain of causation that leads to an incident, event or problem.
- When a problem is observed, we can rarely get to the root cause after a single iteration of asking "Why did this happen?".
- We may have to go through several layers of questioning to understand the root cause of an event and identify an opportunity for corrective actions.

Root Cause Analysis Tools

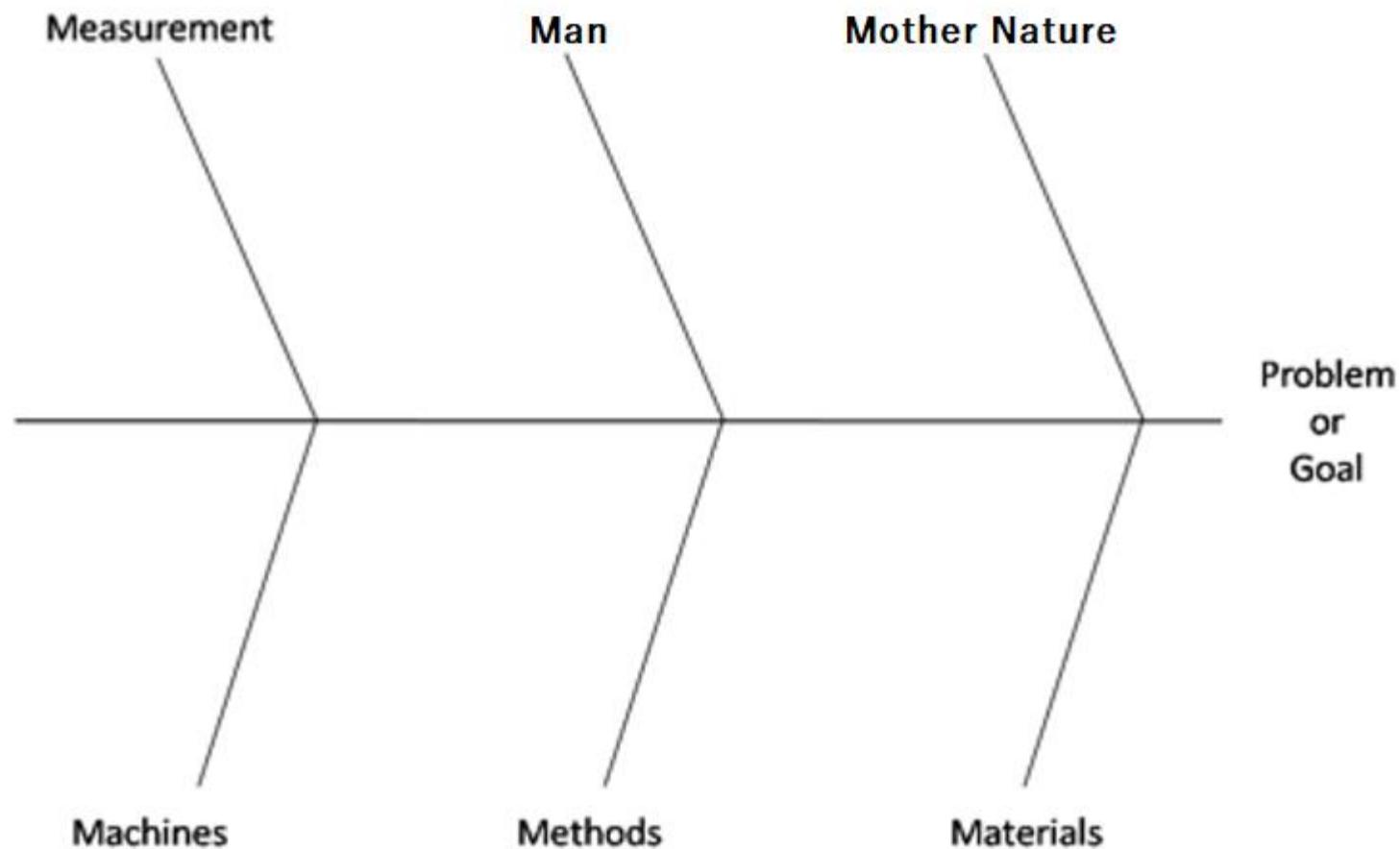
- *Problem Statement:* The company data server was infected with malware.
 1. **Why?** The server was not updated with the latest malware definitions for our anti-malware application.
 2. **Why?** The automated server that deploys the updates is not operational.
 3. **Why?** The automated server broke last month and it hasn't been repaired or replaced.
 4. **Why?** The person responsible for approving the repair or replacement is on vacation and there was inadequate communication about who should cover change approvals.
 5. **Why?** Lack of process to allocate the role to a second person.
- *Solution:* Create a process to ensure that repairs can be approved, even when the normal approving person is away.

Root Cause Analysis Tools

Fishbone/Ishikawa Diagram Analysis

- A fishbone diagram is a visual graphing tool that encourages the investigator to identify potential causes for a problem from a variety of sources.
- The leading framework for Fishbone diagrams is the 6 Ms, where investigators look at:
 1. **Man:** Human factors that could have caused the problem
 2. **Machine:** Hardware or technical causal factors
 3. **Material:** Causal factors stemming from material issues, including consumables and information
 4. **Method:** Causal factors stemming from breakdowns in process or methodology
 5. **Measurement:** Causal factors stemming from inaccuracies in measurement tools or inspections
 6. **Mother Nature:** Causal factors stemming from environmental conditions in which men and machines operate.

Root Cause Analysis Tools



Root Cause Analysis Tools

Pareto Analysis

- Pareto analysis is based on the principle that “80% of the effects come from 20% of the causes”.
- To put it differently, “20% of the work creates 80% of the results”. This is also called the “80/20” rule.
- Our energies need to focus on the “vital few” as opposed to the “trivial many” be it from a problem solving or delivery perspective.

Brainstorming

- Brainstorming is getting all the concerned team members into a room.
- Objective is to understand possible causes to the problem. Focus on solutions only once primary causes are identified.

MODULE - 4

PART – 1: SECURITY REQUIREMENTS

Security Requirements

- A requirement defining what level of security is expected from the system with respect to some type of threat or malicious attack.
- The following are the objectives of Security Requirements:
 1. To ensure that unauthorized malicious programs do not infect the application or component
 2. To ensure that communications and data are not intentionally corrupted
 3. To ensure that parties cannot repudiate interactions if they were involved
 4. To ensure that confidential communications and data are kept private
 5. To ensure that applications survive attack
 6. To ensure that system (people and application) are protected against destruction, damage, theft, or replacement
 7. To ensure that system maintenance does not unintentionally disrupt the security mechanisms

Security Requirements

- The following are the minimum security requirements for systems, applications, and data:

1. Access, Authentication, and Authorization Management:

You need to ensure that the right people have the right access to the right things at the right time, and that you apply the appropriate security controls to manage authentication, authorization, and access control.

2. Disaster Recovery Planning and Data Backup for Systems and Services:

Disaster recovery planning is the ongoing process of developing, implementing, and testing disaster recovery management procedures and processes. Data backup is an integral component of disaster recovery planning. Data backup protects against the loss of data in the event of a physical disaster, database corruption, etc.

Security Requirements

3. Security Risk Management:

Security Risk Management is the ongoing process of identifying the security risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit vulnerabilities and the impact they have on valuable assets.

4. Physical Security:

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

Security Requirements

5. Third Party Vendor Security and Compliance:

The use of external service providers can result in cost savings, efficiencies, greater security and compliance, stronger resiliency, and higher quality services. But, you should properly assess the risk associated with using a certain third party vendor's product or service.

6. Awareness, Training, and Education:

Security awareness training is the process of providing formal cybersecurity education to your workforce about a variety of information security threats and your company's policies and procedures for addressing them. Topics covered in security awareness training often expand beyond the digital world and discuss physical security and how employees can keep themselves and loved ones secure.

Security Requirements

7. Electronic Data Disposal and Media Sanitization:

When files are improperly or inadequately purged from storage media, it is often still possible to reconstruct or retrieve data. Storage media must be appropriately sanitized to prevent unauthorized access to or disclosure of sensitive data.

8. Encryption:

Encryption is the process of encoding information in order to protect the data, and can be applied to data that is stored (at-rest) or transmitted (in-transit) over networks. It reduces the risk of unauthorized access or disclosure. Encryption should be used in conjunction with other data protection controls, such as access control, strong passwords, authentication, and authorization.

Security Requirements

9. Network Security:

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

10. Secure Coding and Application Security:

Insecure software coding and web application design can leave data and IT systems vulnerable to exploitation. This requirement seeks to ensure that applications developed or administered by the organization reflect secure coding practices, which can reduce likelihood that malicious code will be inserted in software, and lessen the impact of malicious code that is already present in deployed software.

Security Requirements

- 11. Vulnerability Management:** Vulnerabilities within networks, software applications, and operating systems are an ever present threat, whether due to server or software misconfigurations, improper file settings, or outdated software versions. Vulnerability management is a critical component of an organization's information security program, and is essential to help reduce its potential financial, reputational and regulatory risks.
- 12. Security of Enterprise Application Integration:** Enterprise application integration (EAI) is the use of technologies and services across an enterprise to enable the integration of software applications and hardware systems. It is necessary to integrate security across applications and infrastructure by implementing specific privacy and security safeguards, and minimize the vulnerability of enterprise systems to external attacks and unauthorized access.

Risk Management

- Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. The risk management process involves the following steps:

Step 1: Identify the Risk

- The first step is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible.

Step 2: Analyze the Risk

- The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many business functions the risk affects.

Risk Management

Step 3: Evaluate or Rank the Risk

- Risks need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization.

Step 4: Treat the Risk

- Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs to. In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues. In a risk management solution, all the relevant stakeholders can be sent notifications from within the system.

Risk Management

Step 5: Monitor and Review the Risk

- Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. Under a digital environment, the risk management system monitors the entire risk framework of the organization. If any factor or risk changes, it is immediately visible to everyone.

Risk Management

- Response to risks usually takes one of the following forms:
 - 1. Avoidance:** While the complete elimination of all risk is rarely possible, a risk avoidance strategy is designed to deflect as many threats as possible in order to avoid the costly and disruptive consequences of a damaging event.
 - 2. Mitigation:** Companies are sometimes able to reduce the amount of damage certain risks can have on company processes. This is achieved by adjusting certain aspects of an overall project plan or company process, or by reducing its scope.
 - 3. Acceptance:** Sometimes, companies decide a risk is worth it from a business standpoint, and decide to keep the risk and deal with any potential fallout. Companies will often retain a certain level of risk if a project's anticipated profit is greater than the costs of its potential risk.

MODULE - 4

PART – 2: SECURITY INCIDENT MANAGEMENT

Security Incident Management

What is Security Incident Management?

- Security incident management is the process of identifying, analyzing, managing and recording security threats or incidents in real-time. A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach.

Why is Security Incident Management required?

- As cybersecurity threats continue to grow in volume and sophistication, organizations are adopting practices that allow them to rapidly identify, respond to, and mitigate these types of incidents while becoming more resilient and protecting against future incidents.

Security Incident Management

What are Security Incidents?

- A security incident is an isolated, undesirable and unpredictable event that can affect the company's business processes, compromise them or violate the level of information security protection. Some examples of security incidents:
 1. Violation of the procedure for interaction with Internet providers, hosting, mail services, cloud services and other providers of telecommunications services
 2. Failure of both technical and software equipment for any reasons
 3. Software bugs
 4. Violation of rules for processing, storing, transferring information, both electronic and hard copies
 5. Unauthorized access of third parties to information resources
 6. Detection of viruses or other malicious programs
 7. Any compromise of the system, for example, releasing account passwords to the public

Security Incident Management

Content of Regulatory Document

- All the incidents should be classified, described and included in the internal corporate documentation that regulate the procedure for ensuring information security.
- Moreover, regulatory documents should provide the hierarchy of incidents and divide them according to their severity.
- The structure of the document, drawn up in the form of a provision or a regulation, should include the following subsections:
 1. Definition of the incidents in relation to the security system of a particular company.
 2. The notification format (oral, memorandum, electronic message), the list of people to be notified, including those, duplicating their duties in case of absence, the list of other people, which receive information on the events (the company management), notification period after receiving information about the incident.

Security Incident Management

3. List of measures for eliminating the consequences of the incident and the procedure for their implementation.
4. Investigative procedure, which determines the officials responsible for investigation, the mechanism for evidence collection and recording, possible actions to identify a culprit.
5. The procedure for bringing the guilty persons to disciplinary responsibility.
6. Security enhancement measures to be applied after the investigation.

Security Incident Management

How Security Incident Management works?

1. The first step that most security incident management plans begin with is to start a full investigation of the incident based on how it is affecting their system, data, or user behavior.
2. The incident response team would then assess the issue to determine whether the behavior is the result of a security incident or if there is an internal software or hardware issue at hand.
3. If the issue is the result of a cyber threat, then the incident would be analyzed further with all pertinent information being collected and documented.
4. After this information is accumulated, the incident response team can identify the scope of the incident and make preparations for resolving it.
5. Following resolution, the team would then submit a detailed written report of the security incident to the appropriate department heads to be distributed amongst their teams to ensure that everyone is in the loop.

Security Incident Management

Best Practices For Security Incident Management

- Organizations of all sizes and types need to plan for the security incident management process. Implement these best practices to develop a comprehensive security incident management plan:
 1. Have a checklist ready for a set of actions based on the threat. Continuously update security incident management procedures as necessary, particularly with lessons learned from prior incidents.
 2. Establish an incident response team including clearly defined roles and responsibilities. Your incident response team should include functional roles within the IT/security department as well as representation for other departments such as legal, communications, finance, and business management or operations.

Security Incident Management

3. Develop a comprehensive training program for every activity necessary within the set of security incident management procedures. Practice your security incident management plan with test scenarios on a consistent basis and make refinements as need be.
4. After any security incident, perform a post-incident analysis to learn from your successes and failures and make adjustments to your security program and incident management process where needed.

Security Incident Management

Forensic analysis

- In some situations, collecting evidence and analyzing forensics is a necessary component of incident response. For these circumstances, you'll want the following in place:
 1. A policy for evidence collection to ensure it is correct and sufficient – or, when applicable, will be accepted in the court of law.
 2. The ability to employ forensics as needed for analysis, reporting, and investigation.
 3. Team members who have experience and training in forensics and functional techniques.

MODULE - 4

PART – 3: THIRD PARTY RISK MANAGEMENT

Third Party Risk Management

What is Third Party Risk Management?

- Third-party risk management (TPRM) is a vital part of a security program's overall risk management program. The average organization can have numerous third parties and vendors that have access to their networks or handle sensitive data on their behalf, leaving a large surface open to potential cyber-attack.
- One of the most common causes of large-scale breaches is the exploitation of third parties. Vulnerabilities in vendors or suppliers are then used to gain access into the target environment to steal or otherwise compromise sensitive information.
- The key objectives of a third-party risk management program are to reduce the ability of cyber attackers to move from a third-party environment into your own. An effective third-party risk management program should identify, measure, and manage risks surrounding the organizations.

Third Party Risk Management

Types of Risk Management

- The primary risks associated with third party/vendor risk management are:
 - a. **Cybersecurity Risk:** Cybersecurity risks include the potential for cyberattacks, third-party breaches, or other forms of system exposure that can be damaging to the technical infrastructure or operations within a company.
 - b. **Compliance Risk:** Compliance risk, or regulatory risk, occurs when laws, rules, or regulations are violated, or when business standards, internal policies, or procedures do not comply with local, regional, national, or international regulatory guidelines.
 - c. **Strategic Risk:** Strategic risk is created from failed business decisions, or the inability to implement strategies consistent with the organizational goals. Third-party vendors that are not aligned with your company's practices may threaten operations or your ability to effectively execute business strategies.

Third Party Risk Management

- d. **Reputation Risk:** Reputation risk refers to negative public opinion or customer perception that stems from irresponsible vendor practices. Dissatisfied customers will stop doing business with your organization and look for other options.
- e. **Operational Risk:** Operational risk results from internal breaches, processes, and system failures. Operational risks may be caused by employee error, system failures, failure to adhere to internal policies, internal and external fraud or criminal activity, etc.
- f. **Transaction Risk:** Transaction risk stems from issues with a service or product delivery, which can negatively impact your company or your customers. Organizations are increasingly exposed to these types of risks when a third-party vendor fails to perform due to reasons such as human error, fraud, etc.

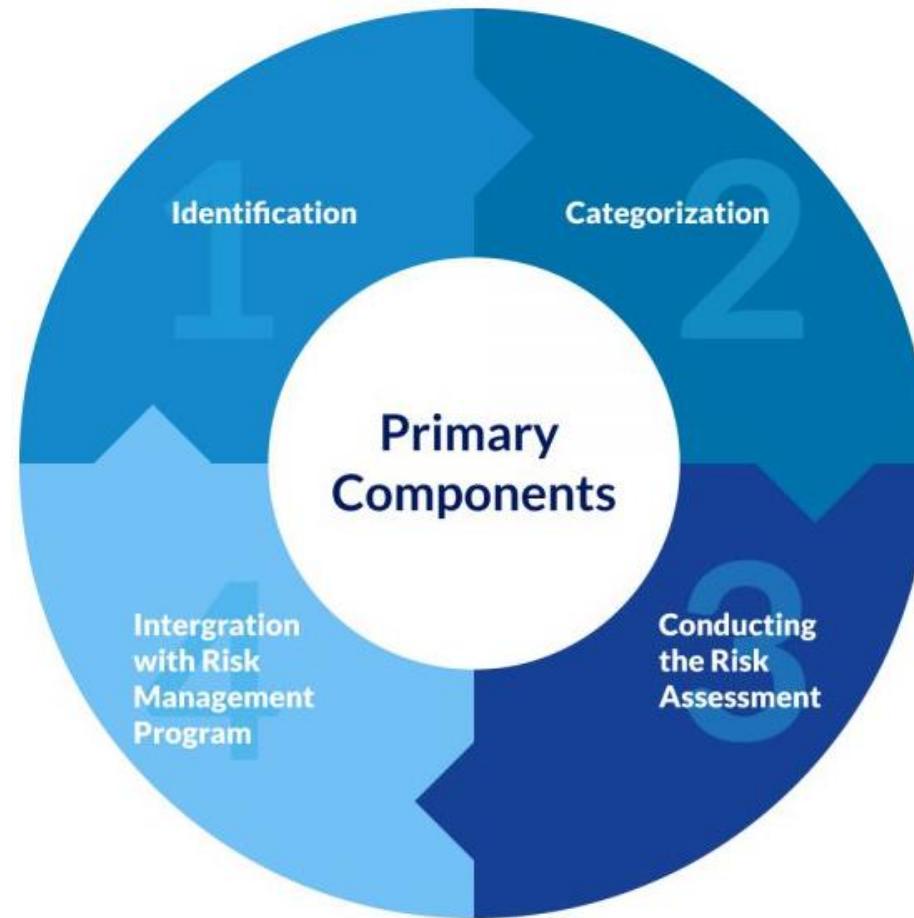
Third Party Risk Management

- g. Credit Risk:** Credit risk or financial risk occurs when a third party or any creditor tied to your third-party vendor is unable to meet the contractual terms or financial agreements. The basic form of credit risk involves the financial condition of the third party itself.

Third Party Risk Management

Third-Party Risk Management

- Every organization will have slightly different processes for third-party risk management, but the primary components can be broken down into four parts.



Third Party Risk Management

1. Identification

- Before you can start managing risk in your third parties, you need to understand who they are and how they integrate with your environment.
- Do they have direct access into your environment or do they store sensitive information of your organization?
- The best place to start the identification process is in your contracts, usually with the legal department or procurement.

2. Categorization

- The next step is to categorize these third-party companies based on the level of access they have to your systems or the types of data they handle on your behalf.
- Breaking your third parties up into appropriate categories makes it easier to prioritize the organizations that handle sensitive data or access critical systems in your environment.

Third Party Risk Management

3. Conducting Third-Party Risk Assessment

- The next step is to perform an assessment. The goal of the assessment is to measure the effectiveness of the safeguards and overall security of the organization. Typical third-party risk assessments can involve:
 - a. **Questionnaire:** These questions usually align to a security best practice framework to determine how much the third-party being assessed complies with this framework. Your organization might also ask for supporting documentation to support the answers given.
 - b. **Technical Testing:** A risk assessment might include additional testing of the third party's technical environment to validate their technical safeguards. This might include a vulnerability scan, penetration testing, or a combination of both.
 - c. **On-Site Assessment:** There may also be instances where you might visit the third party for verification of specific safeguards and overall security practices on-site.

Third Party Risk Management

4. Integration with Overall Risk Management

- Third-party risk management is usually part of your organization's overall security risk management program, which means that there are aspects of the overall risk management program that overlap.
 - i. **Reporting:** After assessing your third parties, the results of these measurement activities need to be collected into a report for presentation to stakeholders. Key decision-makers in your organization should be able to see and review the risks of both the individual vendors and supplies.
 - ii. **Risk Treatment Plan:** There are typically three ways to treat or address risks identified in the third-party assessment process: eliminate, reduce, or accept.

Third Party Risk Management

- iii. **Risk Register:** Once your organization decides how to handle the identified risks, both the risks and the resulting decisions should be documented in a centralized risk register so that your organization can keep track of them and any associated remediation activities over time.
- iv. **Remediation Planning:** For any third parties that require remediation, it's common for your organization to work with them to develop a remediation plan. Your organization should also plan on following up with third-party remediation tasks over time to ensure their execution.
- v. **Continuous Monitoring:** An organization's security program changes constantly over time. Your third parties should be monitored and re-assessed on a regular basis, usually annually.

Third Party Risk Management

Setting Up a Vendor Management Program

- Here are a few steps to help you get started on establishing a successful vendor management program:
 - a. **Create a vendor management team.** Select a few key members within your organization to manage the program. They should be tasked with finding the right vendors that are in alignment with company policies and corporate objectives.
 - b. **Utilize secure remote access tools.** Using secure remote access software can help businesses streamline and solidify their cybersecurity and IT processes to mitigate threats and identify where breaches occurred.
 - c. **Create a database of existing suppliers and vendors.** These should be classified according to services, which is also a good way to check vendor performance and compare vendors that offer similar products or services.

Third Party Risk Management

- d. **Develop policies and procedures.** Policies and procedures should be well documented and comprehensive. There should be a guide detailing how third-party vendor risk management is approached and steps that outline daily tasks and procedures.
- e. **Establish contractual standards and processes.** Contractual standards should involve a detailed negotiation, review, and approval process with your third-party vendor. There should be a complete understanding of the service provider's responsibilities before finalizing any contract draft and include security guarantees.
- f. **Institute an ongoing monitoring regimen.** A successful program includes a process for continually monitoring any changes with vendors. Changes in vendors or within a vendor relationship may present security risks and expose remote access vulnerabilities in your business.

Third Party Risk Management

- g. Create an internal audit process.** Establish an internal audit process to help you verify that your organization has the appropriate controls to mitigate any vendor liabilities.
- h. Have access to comprehensive reporting.** Create customizable, easy-to-read reports that can be accessed quickly and delivered to management and appropriate staff when necessary.

Third Party Risk Management

What to do in case of Third-Party Security Breach?

- Having a successful recovery plan is key to getting your state of business back to normal. Here are some steps to help your company recover:
 - a. **Investigate the breach.** Validate that a third-party data breach occurred and inform management and determine whether the incident needs to be reported to regulatory agencies. Gather as much information as you can to identify and resolve the breach.
 - b. **Notify affected parties.** You should notify authorities, third-party organizations, and individuals who may be affected. Businesses should cite the date of the breach, what's compromised, and how the recipients can protect themselves and control the damage.
 - c. **Identify the cause of the incident.** Find out what caused the incident, such as malware, email phishing, password attacks, or ransomware.

Third Party Risk Management

- d. **Stop the breach.** As soon as you notice a third-party data breach, try to stop or contain the breach right away. Isolate any system accessed by the cybercriminal to prevent the third-party breach from spreading. Disconnect breached user accounts or shut down the specific department targeted.
- e. **Change passwords.** Be sure to change passwords on any accounts that have been compromised (email, websites, etc.). Consider investing in a password management service that can create unique logins and control them.
- f. **Assess the damage.** Once you've eliminated the third-party data breach, you should assess the damage. As you consider your response, ask yourself questions like what data was breached, how sensitive is the data, etc.
- g. **Conduct a third-party security audit.** Use a third-party vendor security audit to assess current security systems so you can prepare for future data breaches and cyberattacks with a recovery plan.

MODULE - 5

PART – 1: INCIDENT RESPONSE

Incident Response Lifecycle

What is an Incident Response Plan?

- An incident response plan is a documented, written plan with 6 distinct phases that helps IT professionals and staff recognize and deal with a cybersecurity incident like a data breach or cyber attack.
- Properly creating and managing an incident response plan involves regular updates and training.
- An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

Incident Response Lifecycle

- The incident response phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Post Incidence Activity

Incident Response Lifecycle

1. Preparation

- This phase is the most crucial phase to protect your business. Part of this phase includes:
 - a. Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of data breach.
 - b. Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
 - c. Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance.
- Your response plan should be well documented, thoroughly explaining everyone's roles and responsibilities. Then the plan must be tested in order to assure that your employees will perform as they were trained.

Incident Response Lifecycle

2. Identification

- This is the process where you determine whether you've been breached. A breach, or incident, could originate from many different areas. The following questions need to be addressed.
 - a. When did the event happen?
 - b. How was it discovered?
 - c. Who discovered it?
 - d. Have any other areas been impacted?
 - e. What is the scope of the compromise?
 - f. Does it affect operations?
 - g. Has the source (point of entry) of the event been discovered?

Incident Response Lifecycle

3. Containment

- When a breach is first discovered, your initial instinct may be to securely delete everything so you can just get rid of it.
- However, that will likely hurt you in the long run since you'll be destroying valuable evidence that you need to determine where the breach started and devise a plan to prevent it from happening again.
- Instead, contain the breach so it doesn't spread and cause further damage to your business. If you can, disconnect affected devices from the Internet.
- Have short-term and long-term containment strategies ready. It's also good to have a redundant system back-up to help restore business operations. That way, any compromised data isn't lost forever.

Incident Response Lifecycle

4. Eradication

- Once you've contained the issue, you need to find and eliminate the root cause of the breach.
- This means all malware should be securely removed, systems should again be hardened and patched, and updates should be applied.
- Whether you do this yourself, or hire a third party to do it, you need to be thorough.
- If any trace of malware or security issues remain in your systems, you may still be losing valuable data, and your liability could increase.

Incident Response Lifecycle

5. Recovery

- This is the process of restoring and returning affected systems and devices back into your business environment.
- During this time, it's important to get your systems and business operations up and running again without the fear of another breach. The following questions need to be addressed.
 - a. When can systems be returned to production?
 - b. Have systems been patched, hardened and tested?
 - c. Can the system be restored from a trusted back-up?
 - d. What tools will ensure similar attacks will not reoccur?

Incident Response Lifecycle

6. Post Incidence Activity

- Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.
- This is where you will analyze and document everything about the breach. Determine what worked well in your response plan, and where there were some holes.
- Lessons learned from both mock and real events will help strengthen your systems against the future attacks. The following questions need to be addressed.
 - a. What changes need to be made to the security?
 - b. How should employee be trained differently?
 - c. What weakness did the breach exploit?
 - d. How will you ensure a similar breach doesn't happen again?

Incident Classification

- Classifications are determined by evaluating the likelihood and potential impact of an Incident.
- The analysis of the likelihood of occurrence and the impact of the affected resources shall result in the assignment of one of four classifications.

Likelihood - shall be determined based on the following criteria:

1. **Rare** - Highly unlikely, but may occur in exceptional circumstances.
2. **Unlikely** - Event is not expected, but a slight possibility of occurrence may exist. Identified vulnerability or issue may be legitimate; however compensating controls have been implemented and make exploitation impossible or unreasonably difficult.
3. **Possible** - The event might occur at some time as there is a history of casual occurrence of the observed behavior.
4. **Likely** - There is a strong possibility and expectation of occurrence, or there is a history of frequent occurrence.
5. **Almost Certain** - The event is expected to occur in most circumstances, there is a precedent for regular occurrence, and preventative controls are not adequate or in place.

Incident Classification

Impact - shall be determined by the associated criticality of affected resources and the following criteria for determining the current or potential severity of the Incident:

1. **Insignificant** - It impacts systems which are non-critical to business functionality, which do not contain Confidential or Restricted Data, and can be replaced with an alternative solution if made unavailable. Examples include printers, multi-function devices, and scanners.
2. **Minor** – It impacts systems which are non-critical to business functionality, which do not contain Confidential or Restricted Data, but cannot be replaced with an alternative solution if made unavailable. Examples include meeting room devices and kiosk stations.
3. **Moderate** – It impacts systems which are non-critical to business functionality but which contain a moderate amount of Confidential or Restricted Data. Examples include end-user computing devices including laptops, tablets, smartphones, and desktop computers.

Incident Classification

4. **Major** – It impacts systems which are non-critical to business functionality but contain a large volume of Confidential or Restricted Data. Major criticality may also be assigned to systems which are critical to business functionality but which do not contain Confidential or Restricted Data. Examples include file servers, development and test resources, and business analytics systems.
5. **Severe** - Identified risk impacts systems which are critical to agency functionality and contain Confidential or Restricted Data. Exposure of systems determined to be critical may result in severe consequences including loss of Confidential or Restricted Data. Removing the affected resource from production will have a negative impact to agency functionality. Examples include external service applications.

Incident Classification

Severity - Based on the likelihood of occurrence and the impact to the affected resources, the CISO will assign one of four incident severity classifications to an incident.

1. **Low** - One instance of potentially unfriendly activity (e.g., port scan, malware detection, observation of potentially malicious user activity, theft of a device, etc.)
2. **Medium** - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer infection on a non-critical system, successful unauthorized vulnerability scan, etc.) or a repeated or persistent Low Incident. Incidents classified as Medium risk may also include the incidental internal exposure of one employee record. Medium incidents may also include vulnerabilities with a rare rate of occurrence on critical systems, either due to compensating controls, network isolation, or other factors.

Incident Classification

3. **High** - Serious attempt or actual interruption in availability, or negative impact to confidentiality or integrity, or Data Breach.

For e.g., denial of service attempt, virus infection of a critical system or the network, multiple concurrent infections of systems, successful buffer/stack overflow, successful unauthorized access to systems hosting or transmitting Confidential or Restricted Data, broken lock, stolen papers, etc.) or a repeated or persistent Medium Incident.

Incidents with a high criticality may include systems with low to moderate criticalities which are affected by vulnerabilities likely to be exploited.

Incident Classification

4. **Emergency** - Incidents that involve the potential breach of Restricted or Confidential Data.

Incidents classified as Emergency risk require immediate attention including the engagement of Data Owners and SMEs to perform short-term containment including taking down potentially compromised systems and applications.

Incidents with an emergency criticality are likely to be assets with high criticality to business functionality which are affected by threats which are almost certain to occur.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Classification of Severity

Response Phase	Severity Class	Service Level Objective	Description
Acceptance	Emergency	1 hour (24x7)	Acceptance is the receipt of an incident by the IST.
	High	1 business hours	Acceptance includes assigning a criticality level to the incident and initiating the formal incident response plan.
	Medium	2 business hours	
	Low	8 business hours	
Containment	Emergency	3 hours (24x7)	Containment is the successful implementation of mitigating controls to prevent any possibility of propagation.
	High	5 hours (24x7)	
	Medium	8 business hours	
	Low	2 business days	
Recovery	Emergency	8 business hours	Resolution is the successful restoration of an affected resource to production use after implementing long-term corrective actions.
	High	1 business days	
	Medium	3 business days	
	Low	5 business days	

Service Level Agreement

IRT Roles & Responsibilities

Role	Responsibility
Team Leader	Drives and coordinates all incident response team activity, and keeps the team focused on minimizing damage, and recovering quickly.
Lead Investigator	Collects and analyzes all evidence, determines root cause, directs the other security analysts, and implements rapid system and service recovery.
Communications Lead	Leads the effort on messaging and communications for all audiences, inside and outside of the company.
Documentation & Timeline Lead	Documents all team activities, especially investigation, discovery and recovery tasks, and develops reliable timeline for each stage of the incident.
HR/Legal Representation	Just as you would guess. Since an incident may or may not develop into criminal charges, it's essential to have legal and HR guidance and participation.

MODULE - 5

PART – 2: VULNERABILITY ASSESSMENT

What is Vulnerability Assessment?

- **Vulnerability Assessment** is the process of recognizing, analyzing and ranking vulnerabilities in computers and other related systems to equip the IT personnel and management team with adequate knowledge about prevailing threats in the environment.
- The vulnerability assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.
- Some of the different types of vulnerability assessment scans include the following:
 1. **Network-based scans** are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
 2. **Host-based scans** are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans. However, it offers greater visibility into the configuration settings and patch history of scanned systems.

What is Vulnerability Assessment?

- 3. Application scans** can be used to test websites to detect known software vulnerabilities and incorrect configurations in network or web applications.
- 4. Database scans** can be used to identify the weak points in a database so as to prevent malicious attacks, such as SQL injection attacks.

Steps in Vulnerability Assessment

- The vulnerability assessment process usually consists of the following phases.
 1. **Initial Assessment:** It's important to identify at least the importance of the device that you have on your network or at least the devices that you'll test. It's also important to understand if the device (or devices) can be accessed by any member of your company (such as a public computer or a kiosk) or just administrators and authorized users.
Once you have these details at hand you will be able to predict the below-stated points:
 - a. Risk appetite*
 - b. Risk mitigation practices and policies for each device
 - c. Business impact analysis
 - d. Residual risk treatment*

Steps in Vulnerability Assessment

2. **System Baseline Definition:** Get details of installed systems before the vulnerability assessment. It is a must to know what they are, what they do, and for who – also review the device open ports, processes, and services. Besides these, get a better knowledge of the certified drivers and software that are installed on the device and the basic configuration of each device. Collect public data and vulnerabilities concerning the device platform, version, vendor and other related details.
Address questions like - Does the device send logs into a security information and event management (SIEM) platform? & Are the logs at least stored in a central repository?

Steps in Vulnerability Assessment

3. **Perform the Vulnerability Scan:** Use the right policy on your scanner to accomplish the desired results.

Prior to starting the vulnerability scan, look for any compliance requirements based on your company's posture and business, and know the best time and date to perform the scan.

It's important to recognize the client industry context and determine if the scan can be performed all at once or if a segmentation is needed.

Steps in Vulnerability Assessment

4. **Vulnerability Assessment Report Creation:** Vulnerability assessment report creation is the last and most important stage of all. It is important to pay attention to the details and combine extra value to the guidance phase. This will help you to gain true value from the report, add recommendations based on the original assessment objectives.
Based on the criticalness of the assets and results, add risk mitigation techniques. Point out the potential gap between the results and the system baseline definition.
Also, suggest measures to set right the deviations and mitigate potential vulnerabilities.

Vulnerability Assessment Benefits

- Conducting vulnerability assessments on a regular basis can put you one step ahead of the bad guys, identify holes in your security defenses yourself rather than waiting for them to be exposed by a breach, and can help you plug holes in your own security before threat actors discover them.
- Beyond *penetration testing* or a simple *vulnerability scan*, a vulnerability assessment or vulnerability analysis doesn't just assess what gaps there may be in your security defenses or how easy it may be to breach your network – it provides an overall picture of your security posture, including what data may be particularly vulnerable, and helps you prioritize the risks that need immediate attention.

MODULE - 6

PART – 1: SECURITY AUDIT

Security Audit

What is a Security Audit?

- A security audit is a comprehensive examination and assessment of an enterprise's information security system.
- Conducting regular audits can help you identify weak spots and vulnerabilities in your IT infrastructure, verify your security controls, ensure regulatory compliance, and more.

Benefits of Security Audit

- Verify that your current security strategy is adequate or not
- Check that your security training efforts are working
- Uncover any extraneous hardware or software
- Reduce cost by cancelling the use of unnecessary resources
- Uncover flaws introduced by new technology or processes
- Prove the organization is complaint with regulations

Steps in Security Audit

1. Define the Objectives

- A security audit is only as complete as its early definition. Lay out the goals that the auditing team aims to achieve by conducting the IT security audit.
- Make sure to clarify the business value of each objective so that specific goals of the audit align with the larger goals of your company.
- Use this list of questions as a starting point for brainstorming and refining your own list of objectives for the audit.
 - a. Which systems and services do you want to test and evaluate?
 - b. Do you want to audit your digital IT infrastructure, your physical equipment and facilities, or both?
 - c. Is disaster recovery on your list of concerns? What specific risks are involved?
 - d. Does the audit need to be geared towards proving compliance with a particular regulation?

Steps in Security Audit

2. Plan the Audit

- A thoughtful and well-organized plan is crucial to success in an IT security audit.
- You'll want to define the roles and responsibilities of the management team and the IT system administrators assigned to perform the auditing tasks, as well as the schedule and methodology for the process.
- Identify any monitoring, reporting and data classification tools that the team will use and any logistical issues they may face, like taking equipment offline for evaluation.
- Once you've decided on all the details, document and circulate the plan to ensure that all staff members have a common understanding of the process before the audit begins.

Steps in Security Audit

3. Perform the Auditing Work

- The auditing team should conduct the audit according to the plan and methodologies agreed upon during the planning phase.
- This will typically include running scans on IT resources like file-sharing services, database servers and SaaS applications like Office 365 to assess network security, data access levels, user access rights and other system configurations.
- It's also a good idea to physically inspect the data center for resilience to fires, floods and power surges as part of a disaster recovery evaluation.
- During this process, interview employees outside the IT team to assess their knowledge of security concerns and adherence to company security policy, so any holes in your company's security procedures can be addressed moving forward.

Steps in Security Audit

4. Report the Results

- Compile all your audit-related findings into a formal report that can be given to management stakeholders or the regulatory agency.
- The report should include a list of any security risks and vulnerabilities detected in your systems, as well as actions that IT staff recommend taking to mitigate them.

Types of Security Audits

Based on the motive of the Audit

1. ***One-time assessment:*** One-time assessments are security audits that you perform for ad-hoc or special circumstances and triggers in your operation. For example, if you are going to introduce a new software platform you have a battery of tests and audits that you run to discover any new risk you are introducing into your business.
2. ***Tollgate assessment:*** Tollgate assessments are security audits with a binary outcome. It's a go or no-go audit to determine a new process or procedure can be introduced into your environment. You aren't determining risk as much as looking for showstoppers that will prevent you from moving forward.
3. ***Portfolio assessment:*** Portfolio security audits are the annual or bi-annual regularly scheduled audit. Use these audits to verify that your security processes and procedures are being followed and that they are adequate for the current business climate and needs.

Types of Security Audits

Based on who performs the Audit

1. ***Internal Audit:*** It is performed by an organization's internal staff. Disadvantage is conflict of Interest and hidden agenda.
2. ***External Audit:*** It is Performed by third-party auditors. They are unaware of internal dynamic and politics hence they may not have any hidden agendas. Major disadvantage is the cost. Sometimes lack of internal working knowledge may translate to longer time to get oriented and be able to perform the test.

Best Practices for Security Audit

1. ***Keep Your Employees Informed:*** First and foremost, you should let your employees know that a company-wide audit is about to happen. This will help your organization remain as transparent as possible. All employees are aware of the audit and can offer potential insight. This is also advantageous because you can choose a time that works best for your team and avoid interfering with other company operations.
2. ***Gather as Much Information as Possible:*** Secondly, you should ensure that all company data is available to auditors as quickly as possible. Ask auditors what specific information they might need so that you can prepare beforehand and avoid scrambling for information at the last minute. This step is also important because you can make sure you are comfortable with the auditors, their practices and their official policies.

Best Practices for Security Audit

3. ***Hire an External Auditor:*** It's smart to hire external auditors for your security audit. The truth is that your own internal auditors might not be comfortable explaining all of your organization's vulnerabilities. Current employees may have biases with respect to company security that can lead to future issues and oversights.
4. ***Conduct Regular Audits:*** Lastly, you should make sure that your security audits are consistent. Your company might have detected and resolved major vulnerabilities last year and feel that it's excessive to conduct another one this year. But the most successful organizations are proactive when it comes to holding regular security audits. New types of cyberattacks and risks are constantly emerging.

MODULE - 6

PART – 2: SECURITY AUDIT

Security Audit

- There are a number of key questions that security audits attempt to answer which include but are not limited to:
 1. Are passwords secure and difficult to crack?
 2. Are access control lists* (ACLs) in place on network devices to control who has access to shared data?
 3. Are there audit logs to identify who accesses data?
 4. Are the audit logs reviewed effectively and how are they reviewed?
 5. How is backup media stored? What is the backup policy and is it followed? Who has access to the backup media and is it up-to-date?
 6. Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan? Does it have gaps in its construct?
 7. Are the security settings for operating systems in accordance with accepted industry security practices?

Security Audit

8. Are these operating systems and commercial applications patched? How and when did the patching take place?
9. Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
10. How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?
11. Who is allowed inside the server room? Who has the keys of the server room?
12. How are the servers, systems, network devices, etc., protected against fire? Are fire extinguishers available in all the important places?

Security Audit

Audit methodologies

- Audit methods may also be classified according to type of activity. These include three types
 1. **Testing** – Penetration tests and other testing methodologies are used to explore vulnerabilities. In other words, exercising one or more assessment objects to compare actual and expected behaviors.
 2. **Examination and Review** – This include reviewing policies, processes, logs, other documents, practices, briefings, situation handling, etc. In other words, checking, inspecting, reviewing, observing, studying, or analyzing assessment objects.
 3. **Interviews and Discussion** – This involves group discussions, individual interviews, etc.

Security Audit

Auditing Security Practices

- The first step for evaluating security controls is to examine the organization's policies, security governance structure, and security objectives because these three areas encompass the business.
- After you have identified the security audit criteria that the organization needs to comply with, the next phase is to perform assessments to determine how well they achieve their goals.
- The following are types of assessments that might be performed to test security controls:
 1. **Risk assessments:** This type of assessment examines potential threats to the organization by listing areas that could be sources of loss such as corporate espionage, service outages, disasters, and data theft. Each is prioritized by severity, matched to the identified vulnerabilities, and used to determine whether the organization has adequate controls to minimize the impact.

Security Audit

2. **Policy assessment:** This assessment reviews policy to determine whether the policy meets best practices, is unambiguous, and accomplishes the business objectives of the organization.
3. **Social engineering:** This involves penetration testing against people to identify whether security awareness training, physical security, and facilities are properly protected.
4. **Security design review:** The security design review is conducted to assess the deployment of technology for compliance with policy and best practices. These types of tests involve reviewing network architecture and design and monitoring and alerting capabilities.
5. **Security process review:** The security process review identifies weaknesses in the execution of security procedures and activities. All security activities should have written processes that are communicated and consistently followed. The two most common methods for assessing security processes are through interviews and observation.

Security Audit

- a. **Interviews:** Talking to the actual people responsible for maintaining security, from users to systems administrators, provides a wealth of evidence about the people aspect of security. Can they answer basic security policy questions? Do they feel that security is effective? The kind of information gathered helps identify any weakness in training and commitment to adhering to policy.
 - b. **Observation:** Physical security can be tested by walking around the office and observing how employees conduct themselves from a security perspective. Do they walk away without locking their workstations or have sensitive documents sitting on their desks? Do they not have a sign-out procedure for taking equipment out of the building?
6. **Document review:** Checking the effectiveness and compliance of the policy, procedure, and standards documents is one of the primary ways an auditor can gather evidence. Checking logs, incident reports, and trouble tickets can also provide data about how IT operates on a daily basis.
7. **Technical review:** This is where penetration testing and technical vulnerability testing come into play. One of the most important services an auditor offers is to evaluate the competence and effectiveness of the technologies relied upon to protect a corporation's assets.

MODULE - 6

PART – 3: INFORMATION SECURITY AUDITOR

Information Security Auditor

- An information security auditor is someone who looks at the safety and effectiveness of computer systems and their security components.
- The auditors are responsible for the following:
 - ✓ Evaluate the efficiency, effectiveness and compliance of operation processes with corporate security policies and related government regulations
 - ✓ Develop and administer risk-focused exams for IT systems
 - ✓ Interview personnel to establish security risks and complications
 - ✓ Execute and properly document the audit process
 - ✓ Assess the exposures resulting from ineffective or missing control practices
 - ✓ Accurately interpret audit results against defined criteria
 - ✓ Collaborate with management to improve security compliance, manage risk and bolster effectiveness
 - ✓ Develop rigorous “best practice” recommendations to improve security on all levels

Information Security Auditor

- The following tasks and activities are carried out by the auditor in discharging their responsibilities:
 - ✓ Auditing the information asset management process will verify that the critical assets are being managed in accordance with the company policies
 - ✓ The auditor audits the policies and standards related to access control, vendor management, vulnerability management, etc.
 - ✓ One of the important roles of audit is to verify that the policies and standards are actually being implemented by users across the enterprise.
 - ✓ Instead of focusing on the actual access of each user, the auditor focuses on the IAM* process and verify that the IAM process is working as designed.
 - ✓ During the audit of policies and standards, the auditor should understand how the policies and standards are being communicated across the enterprise.
 - ✓ The responsible auditor should determine if logging is enabled in critical systems. Where logs are enabled, the auditor verifies that there is a process for monitoring.

Information Security Auditor

- ✓ In today's business environment, Governance, Risk Management and Compliance (GRC) processes are critical to the auditor.
- ✓ The internal auditor should identify how the organization is connected to the outside (for e.g. vendors), and who on the outside is connected to the organization.
- ✓ Also, the auditor should follow the entire process within the extended enterprise where the critical data assets reside.
- ✓ The auditor verifies that a business continuity plan exists and is maintained and tested periodically. The plan should cover all the risks associated with the business.
- ✓ The auditor obtains and reviews the management reports from IT to executive management and verifies that sufficient information is provided to management.

Important Concepts

- Extended enterprise is the concept that a company does not operate in isolation because its success is dependent upon a network of partner relationships.
- Governance, risk management and compliance is the term covering an organization's approach across these three practices: Governance, risk management, and compliance.
- Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges.

Information Security Auditor

- The following things have to be borne in mind before hiring of an audit company as auditors:
 - ✓ Does the organization offer a comprehensive suite of services, tailored to specific requirements?
 - ✓ Does the organization have a quality certification?
 - ✓ Does the organization have a track record of having handled a similar assignment for security consulting?
 - ✓ Are the organization's security professional having professional certificates?
 - ✓ Does the Organization have sound methodology to follow?
 - ✓ Is the organization recognized contributor within the security industry in terms of research and publication etc.?

Information Security Auditor

- Certified Information Systems Auditor (CISA) refers to a designation issued by the Information Systems Audit and Control Association (ISACA). The designation is the global standard for professionals who have a career in information systems, in particular, auditing, control, and security.
- ISACA is a world recognized body that was founded in 1969. The CISA examination and certification was initiated by ISACA in 1978 to address industry requirements.
- To become CISA certified, you must pass the exam with a score of at least 450 while also having at least five years of professional information systems auditing, control, or security.
- The CISA exam lasts four hours and consists of 150 multiple choice questions.

Information Security Auditor

- The Information Systems Audit and Control Association (ISACA) set forth a code governing the professional conduct and ethics of all certified IS auditors and members of the association.

Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.

Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Information Security Auditor

- The benefits of a CISA certification are:
 - ✓ Validates your experience and knowledge in the field
 - ✓ Markets and quantifies expertise
 - ✓ Demonstrates tactical skills required to crack the examination
 - ✓ Global recognition as an IS audit professional
 - ✓ Increased value to organization
 - ✓ Competitive advantage over peers
 - ✓ Credibility in the job market
 - ✓ High professional standard
 - ✓ High salary

Information Security Auditor

- CISA certificate holders are likely to be hired for roles such as those listed below, just to name a few.
 - ✓ Internal Auditor
 - ✓ Public Accounting Auditor
 - ✓ Information Security Analyst
 - ✓ Network Operation Security Engineer
 - ✓ IT Audit Manager
 - ✓ Cybersecurity professional
 - ✓ IT Risk and Assurance Manager
 - ✓ IT Consulting
 - ✓ Privacy Officer
 - ✓ PCI Security Specialist

MODULE - 6

PART – 4: PENETRATION TESTING

Penetration Testing

- The main objective of penetration testing (Pen Testing or Ethical Hacking) is to test your computer system, network or web application to find security vulnerabilities that an attacker could exploit.
- Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents.
- The following are the benefits of penetration testing.
 - ✓ Identify and prioritize security risks
 - ✓ Intelligently manage vulnerabilities
 - ✓ Leverage a proactive security approach
 - ✓ Verify existing security programs are working and discover your security strengths
 - ✓ Increase confidence in your security strategy
 - ✓ Meet regulatory requirements

Penetration Testing

- The reports generated by a penetration test provide the feedback needed for an organization to prioritize the investments it plans to make in its security. These reports can also help application developers create more secure apps.
- In addition to conducting regulatory-mandated analysis and assessments, penetration tests may also be run whenever an organization:
 - ✓ adds new network infrastructure or applications
 - ✓ makes significant upgrades or modifications to its applications or infrastructure
 - ✓ establishes offices in new locations
 - ✓ applies security patches
 - ✓ modifies end-user policies

Asset x Vulnerability x Threat = Risk

Common Security Vulnerabilities

- Some common security vulnerabilities are:
 - 1. Insecure configurations:** Open ports, use of weak password credentials and unsafe user privileges, as well as deep configuration issues can be exploited to achieve network access.
 - 2. Flaws in encryption:** Encryption methods being used to protect and transmit data may not be secure enough to prevent tampering and eavesdropping.
 - 3. Programming weakness:** A bug in software source code can lead to code injection and memory flaws that can again lead to the exposure of data.
 - 4. Session management flaws:** Cookies and tokens used by software applications can be exploited to hijack sessions and escalate privileges.

Types of Penetration Testing

- The following are the different types of Penetration Testing.
 1. **Network Infrastructure Testing:** Network penetration testing, also known as Infrastructure penetration testing, can be performed from two perspectives: inside and outside your organization's network perimeter.
 - a. ***Internal network penetration testing:*** An internal network pen test is performed to help gauge what an attacker could achieve with initial access to a network. An internal network pen test can mirror insider threats, such as employees intentionally or unintentionally performing malicious actions.
 - b. ***External network penetration testing:*** An external network pen test is designed to test the effectiveness of perimeter security controls to prevent and detect attacks as well as identifying weaknesses in internet-facing assets such as web, mail and FTP servers.

Types of Penetration Testing

2. **Wireless Penetration Testing:** Wireless penetration testing is the assessment of wireless local area networks (WLANs) and use of associated wireless protocols and technologies, including Bluetooth, ZigBee, etc., to identify and address vulnerabilities that could lead to unauthorized network access and data leakage.
3. **Application and API security review:** Vulnerabilities contained within software are commonly exploited by cybercriminals and are easily introduced by under-pressure programmers. Ethical hackers can conduct automated and manual penetration tests to assess backend application logic and software and API source code.
4. **Remote Working Assessment:** A remote working security assessment is a type of penetration test designed to help organizations identify and address security risks that result as a consequence of employees working outside of the office. An assessment can uncover a range of security risks, such as misconfigured infrastructure, systems and applications.

Types of Penetration Testing

5. **Web Application Security Testing:** Web applications play a vital role in business success and are an attractive target for cybercriminals. Ethical hacking services include website and web app penetration testing to identify vulnerabilities including SQL injection and cross-site scripting problems plus flaws in application logic and session management flows.
6. **Social Engineering:** People continue to be one of the weakest links in an organization's cyber security. Social engineering pen test service includes a range of email phishing engagements designed to assess the ability of your systems and personnel to detect and respond to a simulated attack exercise.
7. **Mobile Security Testing:** Mobile app usage is on the rise, with more and more companies enabling customers to conveniently access their services via tablets and smartphones. Ethical hackers can carry out in-depth mobile application assessments based on the latest development frameworks and security testing tools.

Types of Penetration Testing

8. **Firewall configuration review:** Firewall rule sets can quickly become outdated. Penetration testers can detect unsafe configurations and recommend changes to optimize security and throughput.

What is Teaming?

- Teaming exercises simulate real-life attack scenarios with one team attacking, and another defending.
 1. **Red Team:** The red team is formed with the intention of identifying and assessing vulnerabilities, testing assumptions, viewing alternate options for attack, and revealing the limitations and security risks for that organization.
 2. **Blue Team:** The blue team is tasked with defending the organization. Blue teams are in charge of building up an organization's protective measures, and taking action when needed.
 3. **Purple Team:** The purple team ensures that the efforts of both teams are utilized to their maximum by combining the defensive tactics and controls from the Blue Team with the threats and weaknesses exposed by the Red Team into a single narrative.

MODULE - 7

PART – 1: SECURITY AUDIT PREPARATION

Security Audit Preparation

- It is important to make sure that your data is secured from attackers. A security audit is one of the best ways to check your organization's security level.
- Security audits can help to identify security vulnerabilities in your system, and find out if your business practices are complaint with various standards.
- Sometimes your customers want to audit your organization security. They want to make sure that their data is secured from attackers.
- Thus, it is important to make sure that you are ready for a security audit. These are some tips that you can use for preparing for a security audit.
 1. **Always Stay Informed:** Hackers are coming up with new complex attacks. Thus, the government is also changing security compliance regulations every year. They have to make sure that your client's data is secured from new attacks. You should always know about the new compliance regulations and standards. This will help your organization in preparing for a security audit.

Security Audit Preparation

2. **Assess your security policy:** Every organization must have a security policy. It must contain all the operating procedures for protecting your company from a data breach. Most of the security audit questions are going to apply to your security policy document. Thus, you must ensure that your security policy is updated.
3. **Create an asset inventory:** A security audit will also check your IT infrastructure. Thus, you must create an inventory of your technology assets. You don't want a security auditor to find out that your IT team forgot to create an asset inventory.
4. **Create a Timeline:** It is difficult to prepare for a security audit. Thus, you must first establish a timeline for your preparation phase. There are many things that you need to check. Hence, you must have a proper strategy. This will help your security team on focusing on important things only.

Security Audit Preparation

5. **Assign Roles and Responsibilities:** It is important to assign roles to your security team. If you want to prepare for the security audit quickly, then you should distribute tasks during the planning phase. This will ensure that everyone knows their responsibility. If everyone already knows their roles, then they can focus on their assigned tasks. This will help you in speeding up the preparation phase.
6. **Review your previous security audit results:** Most of the companies have already gone through at least one security audit. Thus, it is always the best idea to review your previous security audit results. This will ensure that you have already addressed all the recommendations. Also, you must implement recommendations that you have ignored in the past.
7. **Time for a self-assessment:** Test your security policies. This test will help you in fixing all the security errors in your company and identifying security gaps and risks in your company. It will also help you in reducing the stress and anxiety of a real security audit. Your team will already know what to do. Also, you can fix all the security gaps before a real security audit.

Security Audit Preparation

8. **Address security gaps:** If you have done a self-assessment security audit, then you must have found some security gaps in your infrastructure. There can be some deficiencies in your security policy. It is important to address all the security gaps. This will help you in saving your money and time. Also, it will improve your security procedures. Thus, it will reduce the risk of data breaches.

MODULE - 8

PART – 1: SELF AND WORK MANAGEMENT

Self and Work Management

- It is important to understand the scope of the work and work within the limits of the authority.

Scope of Work

- Scope of work refers to the range of tasks and activities to be performed or expected to be performed by someone or within a project or contract, as agreed.
- It is important to understand clearly one's own and others' scope of work and responsibilities clearly and commonly between co-workers for the following reasons:
 - ✓ Helps in planning and organizing work better
 - ✓ Builds trust and reliability
 - ✓ Reduces scope of conflict and confusion
 - ✓ Helps optimize effort through reducing omissions and overlaps
 - ✓ Helps secure the right level of support from the right people

Self and Work Management

- Ways to clarify scope of work
 - ✓ Job descriptions
 - ✓ Seniors (Supervisors or managers)
 - ✓ Job or duty assignment sheet/document/roster
 - ✓ Colleagues
 - ✓ Policy and procedure documents

Seeking/Providing Clarity, Assistance and Support

- When working in an organization, very often, work dependencies means executing work that involves or impacts different departments, co-workers and other stakeholders.
- Executing the work well may require people to:
 - ✓ collaborate, assist and support each other
 - ✓ Stay and keep others informed
 - ✓ participate in planning and decision making, etc.

Self and Work Management

- It is important to know one's own limits of decision making. When one is unclear about it or needs to execute or make decisions about work that extends beyond one's remit and authority, it is important to secure formal permissions, advice and assistance from those designated for the same.
- All tasks at work must be performed accurately as per instructions and within the time limit while demonstrating the following principles:
 - ✓ Work in line with your organization's policies and procedures
 - ✓ Work within the limits of your job role
 - ✓ Obtain guidance from appropriate people, where necessary
 - ✓ Ensure your work meets the agreed requirements
 - ✓ Provide feedback in the end that can be used to identify and address the issues

Self and Work Management

- It is important in many contexts to inform others of work related issues, problems and progress.
- Any work being assigned also comes with a set of expectations of customers, co-workers, supervisors or managers, other departments, etc. These expectations are around:
 - ✓ Volume of work
 - ✓ Quality of work
 - ✓ Time within which the work needs to be completed

Seeking Feedback and Approvals

- Seeking feedback and getting work quality checked by appropriate persons is important for various reasons including:
 - ✓ Ensuring internal and external customer satisfaction
 - ✓ Identifying areas of strength and improvement
 - ✓ Gathering evidence of satisfactory performance
 - ✓ Compliance with set procedures and organization guidelines

Self and Work Management



Self and Work Management

- Feedback must be analyzed and used to improve our work and achieve better. Feedback sought and not worked on is wasted feedback and often can cause disappointment to the person providing the feedback.
- Usually once feedback is used to improve or change work processes and performance, the person providing the feedback must be informed of the same.
- This gets greater support, generates positivity in the mind of the person providing the feedback and usually gets greater buy-in from them.

Self and Work Management

Change and flexibility

- While scope of work, limits of authority, remit of work, policies, processes and procedures define what one must do, it is also important to balance this with flexibility and willingness to change.
- This is important because of the dynamic environment that we work within and the ever-evolving nature of our work, work environment, customer expectations and related policies and procedures.
- Flexibility to change is required to:
 - ✓ incorporate new and improved methods of working
 - ✓ adjusting to environmental changes
 - ✓ supporting others
 - ✓ refining goals and objectives

Self and Work Management

- However, it is important to follow protocol and go through the right channels and procedures. This is particularly important as any change has many facets of impact and in organizations it usually impacts others.
- Those people and organizations which are not willing to change often fail to improve and adapt to newer conditions and environments, which may make them redundant.
- Change must be communicated to all those who are impacted by it and often their views must be collected regarding the same in a timely manner, in order to ensure that the change is not causing undesired impact that can escalate into larger problems.

Self and Work Management

- Planning work and work environment can have a substantial impact on the quality and quantity of work and contributes towards efficiency and productivity.

Work Planning

- Work planning involves many things including:
 - ✓ Defining goals and sub goals
 - ✓ Sequencing activities
 - ✓ Time allocation
 - ✓ Resource planning
 - ✓ Anticipating events and issues impacting work
 - ✓ Mechanisms for checking accuracy and quality of work

Self and Work Management

Work Environment Planning

- One can contribute effectively towards making one's work environment conducive for efficient working. Some of the key requirements for this are:
 - ✓ Cleanliness and tidiness
 - ✓ Organizing the space layout for efficient working
 - ✓ Ergonomic design
 - ✓ Right ambient conditions (lighting, ventilation, etc.).

Self and Work Management

Maintaining Confidentiality

- Confidential information refers to items that should be kept private. This can include documents, images, audio materials, etc.
- In today's world, confidentiality is important for a host of reasons:
 - ✓ Sharing confidential information is often a professional violation and a legal violation. There are a wide range of consequences including financial damages, loss of reputation, litigation, etc.
 - ✓ Failure to properly secure and protect confidential business information can lead to the loss of business/clients.
 - ✓ In the wrong hands, confidential information can be misused to commit illegal activity (e.g., fraud or discrimination), which can in turn result in costly lawsuits for the employer.
 - ✓ The disclosure of sensitive employee and management information can lead to a loss of trust.

Self and Work Management

Effective Communication

- Communication can be verbal, non-verbal communication and written communication.
 - ✓ Be clear about what you want to say before communicating.
 - ✓ Modify your message according to the recipient, if required. The background and need of the recipient should be kept in mind.
 - ✓ Be careful about the language, tone and content of the message.
 - ✓ Take cues from the non-verbal messages that the receiver may be sending that may help you understand whether he is getting your message, or is still interested.
 - ✓ The message being sent out should be consistent and not self-contradictory.
 - ✓ Listen to the other person's point of view during a communication.
 - ✓ Follow-up after the communication to ensure the message has gone across.
 - ✓ Choose the medium of communication carefully.
 - ✓ Do not let your personal biases creep in.

Self and Work Management

Working effectively

- The following are some benefits of developing productive relationships with colleagues:
 - ✓ Getting tasks done gets easier.
 - ✓ Colleagues are more likely to go along with the changes that you recommend.
 - ✓ Instead of spending time and energy on negative relationships, you can focus on opportunities.
 - ✓ You can get ideas and feedback from others.
 - ✓ You can take help in hours of need, if required.
 - ✓ Your productivity increases.
 - ✓ Your performance gets appraised better.
 - ✓ You can learn from others and add to your existing skill-set.

Self and Work Management

Self Development

- Self-development is a continual process throughout one's career. The benefits of continual learning and self-development are also as follows:
 - ✓ It helps to stay relevant and up to date of the changing trends and directions in one's profession.
 - ✓ It helps in becoming more effective in the workplace
 - ✓ Builds a knowledge base that helps identify different types of problems and generate solutions.
 - ✓ This assists in advancing one's career and move into new positions
 - ✓ Can deliver a deeper understanding of what it means to be a professional, along with a greater appreciation of the implications and impacts of your work.
 - ✓ Leads to increased self confidence

Network Security Challenges

Challenges

- “Increase in threats from third-party networks and IoT devices.”
- “Hackers are using more complex and comprehensive tools and internal users seemingly are less aware of what they do to reduce protection.”
- “More things keep getting added to the network, with more vulnerabilities.”

List of well-defined problems in network security (top challenges)

- 1) Insider threats – 44%
- 2) IT infrastructure complexity – 42%
- 3) Absence of leader support – 40%
- 4) Lack of data interoperability – 37%
- 5) Shadow IT – 31%
- 6) Weak controls for privileged access – 29%
- 7) Cloud visibility – 28%
- 8) BYOD – 26%
- 9) Too many alerts – 22%
- 10) Too many tools – 18%

- **Shadow IT** is the use of information technology systems, devices, software, applications, and services without explicit IT department approval. It has grown exponentially in recent years with the adoption of cloud-based applications and services.
- **Bring your own device (BYOD)** refers to the trend of employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data. Personal devices could include smartphones, personal computers, tablets, or USB drives.

3 Ways to Address Some of the Network Security Challenges

Segment your network.

- Insider threats are a good reason to segment your network and protect sensitive data from both malicious and accidental events.
- Instrument those segments with comprehensive threat detection deployed at a central point. Look for modern technologies that include stateful anomaly detection to identify suspicious behaviors.
- In addition, be sure to adjust detection rules and policies to accommodate for the variations in traffic behavior you are likely to see from internal vs. external threats.

- Bring context to alerts

- A key challenge with security alerts is the overwhelming volume. The survey showed the deluge of alerts can exceed the capacity of security teams: they can't investigate them all.
- A solution is to look for tools that provide ways to filter and prioritize alerts based on your unique environment.
- Tools that enable security to correlate network metadata directly with alerts brings to bear context that reduces time-to-detection and minimizes false positives.

- Cybersecurity integration and data interoperability.

- The fourth and tenth challenge on the list – too many tools and data interoperability – are closely related.
- Our analysis of the data suggests it's not so much that organizations have too many tools, it's that some tools make it difficult to share data.
- This requires security analysts to switch from one console to the next to detect threats, which is a manual and time-consuming task.
- More importantly, manual efforts invite human error and gaps for adversaries to exploit. Look for cybersecurity tools that openly embrace integration and provide ways for analysts to share data and get greater visibility of the network and potential threats.

Network Security Problems and Solutions

Unknown Assets on the Network

- There are many businesses that don't have a complete inventory of all the IT assets that they have tied into their network.
- This is a massive problem. If you don't know what assets are on your network, how can you be sure your network is secure?
- The easiest fix for this is to conduct a review of all the devices on your network and identify all the various platforms they run on.
- By doing this, you can know what are the different access points are on your network and which ones are most in need of security updates.

Abuse of User Account Privileges

- According to data cited by the [Harvard Business Review](#), for the year of 2017, "65% of all attacks were carried out by insiders." Whether it's because of honest mistakes (accidentally sending info to the wrong email address or losing a work device), intentional leaks and misuse of account privileges, or identity theft arising from a phishing campaign or other social engineering attack that compromises their user account data, the people inside your business represent one of the biggest security problems you'll ever face.

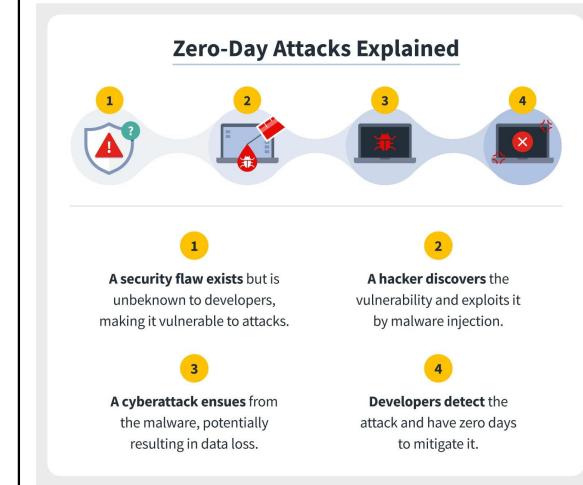
- Because these threats come from trusted users and systems, they're also among the hardest to identify and stop.
- However, there are ways to minimize your risk in case of an insider attack. For example, if your company uses a policy of least privilege (POLP) when it comes to user access, you can limit the damage that a misused user account can do. In a POLP, every user's access to the various systems and databases on your network is restricted to just those things that they need to do their jobs.

Unpatched Security Vulnerabilities

- A zero-day is a computer-software vulnerability either unknown to those who should be interested in its mitigation or known and without a patch to correct it. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network

Vulnerability timeline

- A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence “zero-day.” Let’s break down the steps of the window of vulnerability:
 1. A company’s developers create software, but without their knowledge it contains a vulnerability.
 2. The threat actor spots that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
 3. The attacker writes and implements exploit code while the vulnerability is still open and available
 4. After releasing the exploit, either the public recognizes it in the form of identity or information theft or the developer catches it and creates a patch to fix the issue.



Zero Day Vulnerability Timeline



A Lack of Defense in Depth

- Eventually, despite all of your best efforts, there will be a day where an attacker succeeds in breaching your network security. However, just how much damage this attacker will be capable of depends on how the network is structured.
- The problem is that some businesses have an open network structure where once an attacker is in a trusted system, they have unrestricted access to all systems on the network.
- If the network is structured with strong segmentation to keep all of its discrete parts separate, then it's possible to slow down the attacker enough to keep them out of vital systems while your security team works to identify, contain, and eliminate the breach.

Not Enough IT Security Management

- Another common issue for many companies is that even when they have all of the best cybersecurity solutions in place, they might not have enough people in place to properly manage those solutions.
- When this happens, critical cybersecurity alerts may get missed, and successful attacks may not be eliminated in time to minimize damage.
- However, finding a large enough internal IT security team to manage all of your needs can be an expensive and time-consuming process. Qualified professionals are in demand, and they know it.
- To build up IT security staff quickly, many businesses use the services of a dedicated partner such as **Compuquip Cybersecurity**. This allows these businesses to access a full team of experienced cybersecurity professionals for a fraction of the cost of hiring them full-time internally.

MODULE 4- INFORMATION SECURITY AUDITOR

Information Security Auditor

- An information security auditor is someone who looks at the safety and effectiveness of computer systems and their security components.
- The auditors are responsible for the following:
 - ✓ Evaluate the efficiency, effectiveness and compliance of operation processes with corporate security policies and related government regulations
 - ✓ Develop and administer risk-focused exams for IT systems
 - ✓ Interview personnel to establish security risks and complications
 - ✓ Execute and properly document the audit process
 - ✓ Assess the exposures resulting from ineffective or missing control practices
 - ✓ Accurately interpret audit results against defined criteria
 - ✓ Collaborate with management to improve security compliance, manage risk and bolster effectiveness
 - ✓ Develop rigorous "best practice" recommendations to improve security on all levels

Information Security Auditor

- The following tasks and activities are carried out by the auditor in discharging their responsibilities:
 - ✓ Auditing the information asset management process will verify that the critical assets are being managed in accordance with the company policies
 - ✓ The auditor audits the policies and standards related to access control, vendor management, vulnerability management, etc.
 - ✓ One of the important roles of audit is to verify that the policies and standards are actually being implemented by users across the enterprise.
 - ✓ Instead of focusing on the actual access of each user, the auditor focuses on the IAM* process and verify that the IAM process is working as designed.
 - ✓ During the audit of policies and standards, the auditor should understand how the policies and standards are being communicated across the enterprise.
 - ✓ The responsible auditor should determine if logging is enabled in critical systems. Where logs are enabled, the auditor verifies that there is a process for monitoring.

Information Security Auditor

- ✓ In today's business environment, Governance, Risk Management and Compliance (GRC) processes are critical to the auditor.
- ✓ The auditor should identify how the organization is connected to the outside (for e.g. vendors), and who on the outside is connected to the organization.
- ✓ Also, the auditor should follow the entire process within the extended enterprise where the critical data assets reside.
- ✓ The auditor verifies that a business continuity plan exists and is maintained and tested periodically. The plan should cover all the risks associated with the business.
- ✓ The auditor obtains and reviews the management reports from IT to executive management and verifies that sufficient information is provided to management.

Important Concepts

- Extended enterprise is the concept that a company does not operate in isolation because its success is dependent upon a network of partner relationships.
- Governance, risk management and compliance is the term covering an organization's approach across these three practices: Governance, risk management, and compliance.
- Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges.

Information Security Auditor

- The following things have to be borne in mind before hiring of an audit company as auditors:
 - ✓ Does the organization offer a comprehensive suite of services, tailored to specific requirements?
 - ✓ Does the organization have a quality certification?
 - ✓ Does the organization have a track record of having handled a similar assignment for security consulting?
 - ✓ Are the organization's security professional having professional certificates?
 - ✓ Does the Organization have sound methodology to follow?
 - ✓ Is the organization recognized contributor within the security industry in terms of research and publication etc.?

Information Security Auditor

- Certified Information Systems Auditor (CISA) refers to a designation issued by the Information Systems Audit and Control Association (ISACA). The designation is the global standard for professionals who have a career in information systems, in particular, auditing, control, and security.
- ISACA is a world recognized body that was founded in 1969. The CISA examination and certification was initiated by ISACA in 1978 to address industry requirements.
- To become CISA certified, you must pass the exam with a score of at least 450 while also having at least five years of professional information systems auditing, control, or security.
- The CISA exam lasts four hours and consists of 150 multiple choice questions.

Information Security Auditor

- The Information Systems Audit and Control Association (ISACA) set forth a code governing the professional conduct and ethics of all certified IS auditors and members of the association.

Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.

Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Information Security Auditor

- The benefits of a CISA certification are:

- ✓ Validates your experience and knowledge in the field
- ✓ Markets and quantifies expertise
- ✓ Demonstrates tactical skills required to crack the examination
- ✓ Global recognition as an IS audit professional
- ✓ Increased value to organization
- ✓ Competitive advantage over peers
- ✓ Credibility in the job market
- ✓ High professional standard
- ✓ High salary

Information Security Auditor

- CISA certificate holders are likely to be hired for roles such as those listed below, just to name a few.

- ✓ Internal Auditor
- ✓ Public Accounting Auditor
- ✓ Information Security Analyst
- ✓ Network Operation Security Engineer
- ✓ IT Audit Manager
- ✓ Cybersecurity professional
- ✓ IT Risk and Assurance Manager
- ✓ IT Consulting
- ✓ Privacy Officer
- ✓ PCI Security Specialist

MODULE – 4 SECURITY AUDIT - I

Security Audit

What is a Security Audit?

- A security audit is a comprehensive examination and assessment of an enterprise's information security system.
- Conducting regular audits can help you identify weak spots and vulnerabilities in your IT infrastructure, verify your security controls, ensure regulatory compliance, and more.



Steps in Security Audit

1. Define the Objectives

- A security audit is only as complete as its early definition. Lay out the goals that the auditing team aims to achieve by conducting the IT security audit.
- Make sure to clarify the business value of each objective so that specific goals of the audit align with the larger goals of your company.
- Use this list of questions as a starting point for brainstorming and refining your own list of objectives for the audit.
 - a. Which systems and services do you want to test and evaluate?
 - b. Do you want to audit your digital IT infrastructure, your physical equipment and facilities, or both?
 - c. Is disaster recovery on your list of concerns? What specific risks are involved?
 - d. Does the audit need to be geared towards proving compliance with a particular regulation?

Steps in Security Audit

2. Plan the Audit

- A thoughtful and well-organized plan is crucial to success in an IT security audit.
- You'll want to define the roles and responsibilities of the management team and the IT system administrators assigned to perform the auditing tasks, as well as the schedule and methodology for the process.
- Identify any monitoring, reporting and data classification tools that the team will use and any logistical issues they may face, like taking equipment offline for evaluation.
- Once you've decided on all the details, document and circulate the plan to ensure that all staff members have a common understanding of the process before the audit begins.

Steps in Security Audit

3. Perform the Auditing Work

- The auditing team should conduct the audit according to the plan and methodologies agreed upon during the planning phase.
- This will typically include running scans on IT resources like file-sharing services, database servers and SaaS applications like Office 365 to assess network security, data access levels, user access rights and other system configurations.
- It's also a good idea to physically inspect the data center for resilience to fires, floods and power surges as part of a disaster recovery evaluation.
- During this process, interview employees outside the IT team to assess their knowledge of security concerns and adherence to company security policy, so any holes in your company's security procedures can be addressed moving forward.

Steps in Security Audit

4. Report the Results

- Compile all your audit-related findings into a formal report that can be given to management stakeholders or the regulatory agency.
- The report should include a list of any security risks and vulnerabilities detected in your systems, as well as actions that IT staff recommend taking to mitigate them.

Types of Security Audits

Based on the motive of the Audit

1. **One-time assessment:** One-time assessments are security audits that you perform for ad-hoc or special circumstances and triggers in your operation. For example, if you are going to introduce a new software platform you have a battery of tests and audits that you run to discover any new risk you are introducing into your business.
2. **Tollgate assessment:** Tollgate assessments are security audits with a binary outcome. It's a go or no-go audit to determine a new process or procedure can be introduced into your environment. You aren't determining risk as much as looking for showstoppers that will prevent you from moving forward.
3. **Portfolio assessment:** Portfolio security audits are the annual or bi-annual regularly scheduled audit. Use these audits to verify that your security processes and procedures are being followed and that they are adequate for the current business climate and needs.

Types of Security Audits

Based on who performs the Audit

1. **Internal Audit:** It is performed by an organization's internal staff. Disadvantage is conflict of Interest and hidden agenda.
2. **External Audit:** It is Performed by third-party auditors. They are unaware of internal dynamic and politics hence they may not have any hidden agendas. Major disadvantage is the cost. Sometimes lack of internal working knowledge may translate to longer time to get oriented and be able to perform the test.

Best Practices for Security Audit

1. **Keep Your Employees Informed:** First and foremost, you should let your employees know that a company-wide audit is about to happen. This will help your organization remain as transparent as possible. All employees are aware of the audit and can offer potential insight. This is also advantageous because you can choose a time that works best for your team and avoid interfering with other company operations.
2. **Gather as Much Information as Possible:** Secondly, you should ensure that all company data is available to auditors as quickly as possible. Ask auditors what specific information they might need so that you can prepare beforehand and avoid scrambling for information at the last minute. This step is also important because you can make sure you are comfortable with the auditors, their practices and their official policies.

Best Practices for Security Audit

3. **Hire an External Auditor:** It's smart to hire external auditors for your security audit. The truth is that your own internal auditors might not be comfortable explaining all of your organization's vulnerabilities. Current employees may have biases with respect to company security that can lead to future issues and oversights.
4. **Conduct Regular Audits:** Lastly, you should make sure that your security audits are consistent. Your company might have detected and resolved major vulnerabilities last year and feel that it's excessive to conduct another one this year. But the most successful organizations are proactive when it comes to holding regular security audits. New types of cyberattacks and risks are constantly emerging.

MODULE - 4: SECURITY AUDIT - II

Security Audit

- There are a number of key questions that security audits attempt to answer which include but are not limited to:
 1. Are passwords secure and difficult to crack?
 2. Are access control lists* (ACLs) in place on network devices to control who has access to shared data?
 3. Are there audit logs to identify who accesses data?
 4. Are the audit logs reviewed effectively and how are they reviewed?
 5. How is backup media stored? What is the backup policy and is it followed? Who has access to the backup media and is it up-to-date?
 6. Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan? Does it have gaps in its construct?
 7. Are the security settings for operating systems in accordance with accepted industry security practices?

Security Audit

8. Are these operating systems and commercial applications patched? How and when did the patching take place?
9. Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
10. How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?
11. Who is allowed inside the server room? Who has the keys of the server room?
12. How are the servers, systems, network devices, etc., protected against fire? Are fire extinguishers available in all the important places?

Security Audit

Audit methodologies

- Audit methods may also be classified according to type of activity. These include three types
 1. **Testing** – Penetration tests and other testing methodologies are used to explore vulnerabilities. In other words, exercising one or more assessment objects to compare actual and expected behaviors.
 2. **Examination and Review** – This include reviewing policies, processes, logs, other documents, practices, briefings, situation handling, etc. In other words, checking, inspecting, reviewing, observing, studying, or analyzing assessment objects.
 3. **Interviews and Discussion** – This involves group discussions, individual interviews, etc.

Security Audit

Auditing Security Practices

- The first step for evaluating security controls is to examine the organization's policies, security governance structure, and security objectives because these three areas encompass the business.
- After you have identified the security audit criteria that the organization needs to comply with, the next phase is to perform assessments to determine how well they achieve their goals.
- The following are types of assessments that might be performed to test security controls:
 1. **Risk assessments:** This type of assessment examines potential threats to the organization by listing areas that could be sources of loss such as corporate espionage, service outages, disasters, and data theft. Each is prioritized by severity, matched to the identified vulnerabilities, and used to determine whether the organization has adequate controls to minimize the impact.

Security Audit

2. **Policy assessment:** This assessment reviews policy to determine whether the policy meets best practices, is unambiguous, and accomplishes the business objectives of the organization.
3. **Social engineering:** This involves penetration testing against people to identify whether security awareness training, physical security, and facilities are properly protected.
4. **Security design review:** The security design review is conducted to assess the deployment of technology for compliance with policy and best practices. These types of tests involve reviewing network architecture and design and monitoring and alerting capabilities.
5. **Security process review:** The security process review identifies weaknesses in the execution of security procedures and activities. All security activities should have written processes that are communicated and consistently followed. The two most common methods for assessing security processes are through interviews and observation.

Security Audit

- a. **Interviews:** Talking to the actual people responsible for maintaining security, from users to systems administrators, provides a wealth of evidence about the people aspect of security. Can they answer basic security policy questions? Do they feel that security is effective? The kind of information gathered helps identify any weakness in training and commitment to adhering to policy.
- b. **Observation:** Physical security can be tested by walking around the office and observing how employees conduct themselves from a security perspective. Do they walk away without locking their workstations or have sensitive documents sitting on their desks? Do they not have a sign-out procedure for taking equipment out of the building?
7. **Document review:** Checking the effectiveness and compliance of the policy, procedure, and standards documents is one of the primary ways an auditor can gather evidence. Checking logs, incident reports, and trouble tickets can also provide data about how IT operates on a daily basis.
8. **Technical review:** This is where penetration testing and technical vulnerability testing come into play. One of the most important services an auditor offers is to evaluate the competence and effectiveness of the technologies relied upon to protect a corporation's assets.

MODULE 4- SECURITY AUDIT PREPARATION

Security Audit Preparation

- It is important to make sure that your data is secured from attackers. A security audit is one of the best ways to check your organization's security level.
- Security audits can help to identify security vulnerabilities in your system, and find out if your business practices are compliant with various standards.
- Sometimes your customers want to audit your organization security. They want to make sure that their data is secured from attackers.
- Thus, it is important to make sure that you are ready for a security audit. These are some tips that you can use for preparing for a security audit.
 1. **Always Stay Informed:** Hackers are coming up with new complex attacks. Thus, the government is also changing security compliance regulations every year. They have to make sure that your client's data is secured from new attacks. You should always know about the new compliance regulations and standards. This will help your organization in preparing for a security audit.

Security Audit Preparation

2. **Assess your security policy:** Every organization must have a security policy. It must contain all the operating procedures for protecting your company from a data breach. Most of the security audit questions are going to apply to your security policy document. Thus, you must ensure that your security policy is updated.
3. **Create an asset inventory:** A security audit will also check your IT infrastructure. Thus, you must create an inventory of your technology assets. You don't want a security auditor to find out that your IT team forgot to create an asset inventory.
4. **Create a Timeline:** It is difficult to prepare for a security audit. Thus, you must first establish a timeline for your preparation phase. There are many things that you need to check. Hence, you must have a proper strategy. This will help your security team focus on important things only.

Security Audit Preparation

5. **Assign Roles and Responsibilities:** It is important to assign roles to your security team. If you want to prepare for the security audit quickly, then you should distribute tasks during the planning phase. This will ensure that everyone knows their responsibility. If everyone already knows their roles, then they can focus on their assigned tasks. This will help you in speeding up the preparation phase.
6. **Review your previous security audit results:** Most of the companies have already gone through at least one security audit. Thus, it is always the best idea to review your previous security audit results. This will ensure that you have already addressed all the recommendations. Also, you must implement recommendations that you have ignored in the past.
7. **Time for a self-assessment:** Test your security policies. This test will help you in fixing all the security errors in your company and identifying security gaps and risks in your company. It will also help you in reducing the stress and anxiety of a real security audit. Your team will already know what to do. Also, you can fix all the security gaps before a real security audit.

Security Audit Preparation

8. **Address security gaps:** If you have done a self-assessment security audit, then you must have found some security gaps in your infrastructure. There can be some deficiencies in your security policy. It is important to address all the security gaps. This will help you in saving your money and time. Also, it will improve your security procedures. Thus, it will reduce the risk of data breaches.

IT System Security Audit Checklist

- Record audit procedure
- Document current policies
- Evaluate IT security measures
- Ensure employee training
- Update security patches
- Test system for vulnerabilities



- Search for firewall holes
- Configure data access
- Implement encryption
- Verify wireless security
- Scan network access points
- Review event logs

Team Work and Communication

Problem-Solving Skills

- When employers talk about problem-solving skills, they are often referring to the ability to handle difficult or unexpected situations in the workplace as well as complex business challenges.
- Organizations rely on people who can assess both kinds of situations and calmly identify solutions. Problem-solving skills are traits that enable you to do that.
- While problem-solving skills are valued by employers, they are also highly useful in other areas of life like relationship building and day-to-day decision making.

What are problem-solving skills

- Active listening
- Analysis
- Research
- Creativity
- Communication
- Dependability
- Decision making
- Team-building

Research

- Researching is an essential skill related to problem solving. As a problem solver, you need to be able to identify the cause of the issue and understand it fully.
- You can begin to gather more information about a problem by brainstorming with other team members, consulting more experienced colleagues or acquiring knowledge through online research or courses.

Analysis

- The first step to solving any problem is to analyze the situation. Your analytical skills will help you understand problems and effectively develop solutions. You will also need analytical skills during research to help distinguish between effective and ineffective solutions.

Decision-making

- Ultimately, you will need to make a decision about how to solve problems that arise. With industry experience—you may be able to make a decision quickly.
- Solid research and analytical skills can help those who have less experience in their field. There may also be times when it is appropriate to take some time to craft a solution or escalate the issue to someone more capable of solving it.

Communication

- When identifying possible solutions, you will need to know how to communicate the problem to others. You will also need to know what communication channels are the most appropriate when seeking assistance. Once you find a solution, communicating it clearly will help reduce any confusion and make implementing a solution easier.

Dependability

- Dependability is one of the most important skills for problem-solvers. Solving problems in a timely manner is essential. Employers highly value individuals they can trust to both identify and then implement solutions as fast and effectively as possible.

Tips for team building with problem-solving activities

Here are some strategies you can use to ensure productive team building sessions:

- **Be realistic about participant abilities:** When developing your own problem-solving activities for team building, be realistic about participant abilities. Everyone brings a specific set of skills to the group, so utilizing everyone's unique traits can ensure the most effective team-building sessions. For instance, if you have a team member who is stronger at motivating others, assign them to a leadership role in the activity.
- **Evaluate your team-building budget:** If you are planning team-building activities, evaluate your team-building budget. The overall costs of team building depend on the activities. For example, off-site activities cost more. However, these activities do not need to be expensive to be effective. There are many free team-building activities you can try in-house or off-site based on your team's needs and preferences.

Keep team-building sessions short:

- Try to keep team-building sessions short for several reasons. Primarily, short team-building sessions are less intrusive to the work schedule.
- A session that is 30 minutes long takes away less time than a longer session and is much easier to schedule. That way, you can incorporate it into your routine.

1) Identify the problem that needs to be solved

One of the easiest ways to identify a problem is to ask questions. A good place to start is to ask journalistic questions, like:

- **Who:** Who is involved with this problem? Who caused the problem? Who is most affected by this issue?
- **What:** What is happening? What is the extent of the issue? What does this problem prevent from moving forward?
- **Where:** Where did this problem take place? Does this problem affect anything else in the immediate area?
- **When:** When did this problem happen? When does this problem take effect? Is this an urgent issue that needs to be solved within a certain timeframe?
- **Why:** Why is it happening? Why does it impact workflows?
- **How:** How did this problem occur? How is it affecting workflows and team members from being productive?

Asking journalistic questions can help you define a strong problem statement so you can highlight the current situation objectively, and create a plan around that situation.

Here's an example of how a design team uses journalistic questions to identify their problem:

Overarching problem: Design requests are being missed

- **Who:** Design team, digital marketing team, web development team
- **What:** Design requests are forgotten, lost, or being created ad hoc.
- **Where:** Email requests, design request spreadsheet
- **When:** Missed requests on January 20th, January 31st, February 4th, February 6th
- **How:** Email request was lost in inbox and the intake spreadsheet was not updated correctly. The digital marketing team had to delay launching ads for a few days while design requests were bottlenecked. Designers had to work extra hours to ensure all requests were completed.

2) Brainstorm multiple solutions

When you and your team are brainstorming different possible solutions, it's important to consider who the problem affects. Go back to the journalistic questions you're asking: Who is involved in this problem? Make sure these individuals (often referred to as [project stakeholders](#)) are involved in the decision making process.

If at all possible, bring in a facilitator who doesn't have a major stake in the solution. Bringing an individual who has little-to-no stake in the matter can help keep your team on track and encourage good problem-solving skills.

Here are a few [brainstorming techniques](#) to encourage creative thinking:

- **Brainstorm alone before hand:** Before you come together as a group, provide some context to your team on what exactly the issue is that you're brainstorming. This will give time for you and your teammates to have some ideas ready by the time you meet.

Say yes to everything (at first): When you first start brainstorming, don't say no to any ideas just yet—try to get as many ideas down as possible. Having as many ideas as possible ensures that you'll get a variety of solutions. Save the trimming for the next step of the strategy.

- **Talk to team members one-on-one:** Some people may be less comfortable sharing their ideas in a group setting. Discuss the issue with team members individually and encourage them to share their opinions without restrictions—you might find some more detailed insights than originally anticipated.

Break out of your routine: If you're used to brainstorming in a conference room or over Zoom calls, do something a little different! Take your brainstorming meeting to a coffee shop or have your Zoom call while you're taking a walk. Getting out of your routine can force your brain out of its usual rut and increase critical thinking.

3) Define the solution

After you brainstorm with team members to get their unique perspectives on a problem, it's time to look at the different strategies and decide which option is the best solution for the problem at hand. When defining the solution, consider these main two questions: What is the desired outcome of this solution and who stands to benefit from this solution?

Set a deadline for when this decision needs to be made and update stakeholders accordingly. Sometimes there's too many people who need to make a decision. Use your best judgement based on the limitations provided to do great things fast.

4) Implement the solution

To implement your solution, start by working with the individuals who are closest to the problem. This can help those most affected by the problem get unblocked. Then move farther out to those who are less affected, and so on and so forth. Some solutions are simple enough that you don't need to work through multiple teams.

After you prioritize implementation with the right teams, assign out the ongoing work that needs to be completed by the rest of the team. This can prevent people from becoming overburdened during the [implementation phase](#). Once your solution is in place, schedule check-ins to see how the solution is working and course-correct if necessary.

What is problem solving?

Problem solving is the process of finding a resolution for a specific issue or conflict. There are many possible solutions for solving a problem, which is why it's important to go through a problem-solving process to find the best solution. You could use a flathead screwdriver to unscrew a Phillips head screw, but there is a better tool for the situation. Utilizing common problem-solving techniques helps you find the best solution to fit the needs of the specific situation, much like using the right tools.

4 steps to effective problem solving

While it might be tempting to dive into a problem head first, take the time to move step by step. Here's how you can effectively break down the problem-solving process with your team:

- 1) **Identify the problem that needs to be solved**
- 2) **Brainstorm multiple solutions**
- 3) **Define the solution**
- 4) **Implement the solution**

Common problem-solving strategies

There are a few ways to go about identifying problems (and solutions). Here are some strategies you can try, as well as common ways to apply them:

Trial and error

Trial and error problem solving doesn't usually require a whole team of people to solve. To use trial and error problem solving, identify the cause of the problem, and then rapidly test possible solutions to see if anything changes.

This problem-solving method is often used in tech support teams through troubleshooting.

SWOT analysis

A [SWOT analysis](#) can help you highlight the strengths and weaknesses of a specific solution. SWOT stands for:

- **Strength:** Why is this specific solution a good fit for this problem?
- **Weaknesses:** What are the weak points of this solution? Is there anything that you can do to strengthen those weaknesses?
- **Opportunities:** What other benefits could arise from implementing this solution?
- **Threats:** Is there anything about this decision that can detrimentally impact your team?

As you identify specific solutions, you can highlight the different strengths, weaknesses, opportunities, and threats of each solution.

This particular problem-solving strategy is good to use when you're narrowing down the answers and need to compare and contrast the differences between different solutions.

5 whys

The 5 whys problem-solving method helps get to the root cause of an issue. You start by asking once, "Why did this issue happen?" After answering the first why, ask again, "Why did that happen?" You'll do this five times until you can attribute the problem to a root cause.

This technique can help you dig in and find the human error that caused something to go wrong. More importantly, it also helps you and your team develop an actionable plan so that you can prevent the issue from happening again.

Here's an example:

Problem: The email marketing campaign was accidentally sent to the wrong audience.

1. "Why did this happen?" Because the audience name was not updated in our email platform.
2. "Why were the audience names not changed?" Because the audience segment was not renamed after editing.
3. "Why was the audience segment not renamed?" Because everybody has an individual way of creating an audience segment.
4. "Why does everybody have an individual way of creating an audience segment?" Because there is no standardized process for creating audience segments.
5. "Why is there no standardized process for creating audience segments?" Because the team hasn't decided on a way to standardize the process as the team introduced new members.

In this example, we can see a few areas that could be optimized to prevent this mistake from happening again. When working through these questions, make sure that everyone who was involved in the situation is present so that you can co-create next steps to avoid the same problem.

Types of Policies and Procedures Every Workplace Needs

Policies and Procedures for Attendance

- These documents can include guidelines on tardiness, vacation time, sick leave, appointments and paid volunteer hours. You can also include the amount of notice required before booking time off. Take your corporate culture into consideration when developing these rules.

Policies and Procedures for Employee Conduct

- This is a broad topic and may require multiple, separate policies. Including guidelines on drugs and alcohol use, smoking, performance management and discipline helps employees know what is and is not acceptable behavior at work.

Policies and Procedures for Use of Company Property

- Employees have to use company property in order to do their jobs. Depending on your industry, this could include electronics, medical equipment, vehicles, tools and uniforms. Include guidelines on how to care for company property, as well as how much (if any) and what types of personal use are permitted using company property.

Policies and Procedures for Harassment and Discrimination

- Harassment and discrimination affect workplace culture. Keep employees safe and treat them fairly by developing policies and procedures that prohibit behaviors such as:
- sexual harassment
- bullying
- verbal and physical harassment
- stalking
- hiring discrimination
- workplace discrimination
- Include information on how to report harassment and discrimination and explain that the company will not retaliate for reporting.

Policies and Procedures for Internet and Social Media Use

- Make employees aware that any internet use at work is not private. Urge employees to limit personal internet use and ensure everything they do online in the **workplace is legal, ethical and appropriate** (and explain what these mean). Add guidelines about what is and is not appropriate to post on social media regarding your organization as well.

Policies and Procedures for Health and Safety

- Protecting employees' safety and well-being should be every organization's top priority. When writing your health and safety policies, include information about how to **deal with illness or injury at work**, equipment safety guidelines and how to report a health or safety concern. Also include procedures to follow in the event of a fire or natural disaster.

Policies and Procedures for Expenses

- If your employees travel or purchase things for work, having an expense reimbursement policy in place is essential. Explain what types of expenses are acceptable for reimbursement (**airfare class, transportation, meals, etc.**). Include procedures on how to submit a reimbursement claim.

MANAGING HEALTH AND SAFETY

- Employers have a responsibility to ensure the health and safety of employees in the workplace. They set the protocols and make sure the workplace is in compliance with standards.
- However, regardless of how many risks and hazards employers minimize, accidents will continue to happen if workers don't take responsibility for their actions.
- Safety is a team effort. One employee acting irresponsibly cannot only hurt themselves, but other employees as well. Consider that employee collisions are one of the top causes of injury in the workplace: one person running into another or an employee running into an object. This is largely a result of someone being distracted or just not paying attention.

- Another common cause of workplace accidents is a trip and fall. Two primary reasons this happens are, again, someone not paying attention, or poor housekeeping: people tripping over objects that haven't been put in their proper place.
- These and most all other common causes of injuries at work are readily avoided simply by workers being more mindful and diligent about keeping the workplace safe.
- Workers must understand their role in creating a safe and healthy working environment and always take that responsibility seriously. Safety is always the top priority.

What Is Employee Safety?

- Employees have a legal right to be safe at work. An employer must ensure that the workplace is free from as many hazards as possible. Some hazards cannot be completely eliminated, in which case every precaution should be taken to reduce the chances of injury.
- Employee safety involves the following:
 - Adequate and ongoing safety training
 - Machinery that is well maintained and has adequate protective guards
 - Being provided with the required safety gear
 - Protection from toxic chemicals
 - The ability to report any injury

Your Employees' Role in Health and Safety in the Workplace

- Although employers have a legal responsibility to ensure worker safety, as noted, responsibilities for health and safety in the workplace also fall on the employees.
- Employees are required to comply with the standards, rules, and regulations put in place by the employer. Employees are required to use safety equipment, PPE, and other safety devices made available by the employer that are necessary for their protection.
- It is critical that all workers feel empowered to carry out their role in the health and safety regime. This includes not only following protocols themselves, but encouraging others to do the same and having a trusted superior who will listen to suggestions or complaints.

How to Motivate Employees to Create a Safety Culture

Provide Health and Safety Training for All Staff

- Just as business owners and CEOs are aware of their obligations toward their employees, workers must be aware of their own responsibilities when it comes to ensuring safety at work.
- Teaching employees effective personal strategies they can implement themselves is one effective way of motivating staff. Emphasize that employee safety is a priority by providing new trainees with health and safety training in their first week of work.

How to Motivate Employees to Create a Safety Culture

Promote Engagement and Participation from Workers

- Encouraging employee engagement and participation are key aspects in promoting and growing a positive safety culture in your workplace. A healthier and safer workplace increases employee job satisfaction, productivity, and business performance.
- Employee-suggested solutions are often straightforward, effective, cost-efficient, and easy for employers to implement. Urge workers to get involved and speak up about workplace safety issues. Ask that they tell you what's working and what isn't. Emphasize that, by reporting hazards, employees are making their workplace safer.

How to Motivate Employees to Create a Safety Culture

Designate Health and Safety Representatives

- CEOs and business owners are not always present in the workplace, so don't know firsthand about new hazards that may arise. Information on safety issues needs to be passed to those in charge, which, for various reasons, some workers are reluctant to do.
- By designating a health and safety representative, employees can confidently and discreetly (and, if necessary, anonymously) discuss their concerns with this person. The representative, who acts as a trusted intermediary between CEO or owner and employee, can relay these matters to the employer at regular meetings.

Key Components of a Health and Safety Plan

1. **A reporting system:** A simple, clear, well-communicated procedure to report accidents (including near misses), injuries and illness, as well as potential hazards in the workplace.
2. **Training programs:** Some aspects may be legal requirements, such as dangerous goods handling, while other components may deal with the facility, and specific aspects of the health and safety plan.
3. **Inspections:** Employee and management teams regularly inspect the workplace to identify changing conditions or activities that may compromise safety.
4. **Emergency planning:** Foreseeable emergencies such as fires and flooding have developed action plans that are well-communicated with all staff through meetings and workplace postings.
5. **Continuous improvement:** Management seeks staff input before implementing changes to the workplace, and regular meetings address not only current health and safety issues, but also improvements to the health and safety plan.

- The World Day for Safety and Health at Work is celebrated every year on 28 April and aims to prevent occupational accidents and diseases. The day focuses on promoting a culture of safety and health.
- It coincides with the April 28 International Commemoration Day for Dead and Injured Workers.
- By far the greatest proportion of current work-related deaths, 86 percent, come from disease.
- An estimated 6,500 people a day die from occupational diseases, compared to 1,000 a day from fatal occupational accidents.

Work-related diseases include:

- Musculoskeletal disorders.
- Stress and mental health disorders.
- Work-related cancer.
- Skin diseases.
- Work-related diseases from biological agents.

Data and Information management

Data	Information
<ul style="list-style-type: none">• Data refers to raw facts that have no specific meaning.	<ul style="list-style-type: none">• Information refers to processed data that has a purpose and meaning.
<ul style="list-style-type: none">• The word 'data' is derived from the Latin word 'datum', which means 'something that is given'.	<ul style="list-style-type: none">• The word 'information' is derived from the Latin word 'informatiō', which means 'formation or conception'.
<ul style="list-style-type: none">• The data is independent of the information.	<ul style="list-style-type: none">• Information is dependent on data.
<ul style="list-style-type: none">• Data or raw data is not enough to make a decision.	<ul style="list-style-type: none">• The information is sufficient to help make a decision in the respective context.

- **Data management** is the practice of collecting, organizing, protecting, and storing an organization's data so it can be analyzed for business decisions.

- As organizations create and consume data at unprecedented rates, data management solutions become essential for making sense of the vast quantities of data.

What Is Data Management? Importance & Challenges

Data management continues to evolve to address challenges

Because data management plays a crucial role in today's digital economy, it's important that systems continue to evolve to meet your organization's data needs. Traditional data management processes make it difficult to scale capabilities without compromising governance or security. Modern data management software must address several challenges to ensure trusted data can be found.

Challenge 1: Increased data volumes

Every department within your organization has access to diverse types of data and specific needs to maximize its value. Traditional models require IT to prepare the data for each use case and then maintain the databases or files. As more data accumulates, it's easy for an organization to become unaware of what data it has, where the data is, and how to use it.

Challenge 2: New roles for analytics

As your organization increasingly relies on data-driven decision-making, more of your people are asked to access and analyze data. When analytics falls outside a person's skill set, understanding naming conventions, complex data structures, and databases can be a challenge. If it takes too much time or effort to convert the data, analysis won't happen and the potential value of that data is diminished or lost.

Challenge 3: Compliance requirements

Constantly changing compliance requirements make it a challenge to ensure people are using the right data. An organization needs its people to quickly understand what data they should or should not be using—including how and what personally identifiable information (PII) is ingested, tracked, and monitored for compliance and privacy regulations.

Establish data management best practices

Implementing best practices can help your organization address some data management challenges and reap the benefits. Get the most out of your data with an effective data management strategy.

1. Clearly identify your business goals

Just like in every business practice, the first step is identifying your organization's goals. Setting goals will help determine the process for collecting, storing, managing, cleaning, and analyzing data. Clearly defined business objectives ensure you're only keeping and organizing data relevant for decision-making and prevent your data management software from becoming overcrowded and unmanageable.

2. Focus on the quality of data

You set up a data management system to provide your organization with reliable data, so put the processes in place to improve the quality of that data. First create goals to streamline your data collection and storage, but make sure to complete regular checks for accuracy so data does not become outdated or stale in any way that can negatively impact analytics. These processes should also identify incorrect or inconsistent formatting, spelling errors, and other errors that will impact results. Training team members on the proper process for inputting data and setting up data prep automation is another way to ensure data is correct from the beginning.

3. Allow the right people to access the data

Having quality data is half the battle. You also need to make sure the right people can access that data when and where they need it. Instead of issuing blanket rules for everyone in the company, it is often smart to set up different levels of permissions so each person can access the relevant data to do their jobs. It can be difficult to find the right balance between convenience and security, but if your team cannot access the data they need efficiently, it can lead to a loss of time and money.

4. Prioritize data security

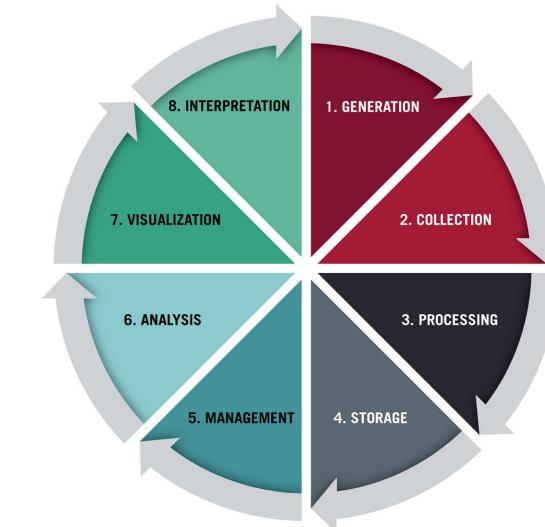
Data should be appropriately accessible inside your organization, but you must put protections in place to keep your data secure from outsiders. Train your team members on how to handle data properly, and ensure your processes meet compliance requirements. Be prepared for the worst-case scenario and have a strategy in place for handling a potential breach. Finding the right data management software can help keep your data secure and safe.

Find effective data management platform

An effective data management solution can help you achieve each of these best practices. Tableau's approach to data management is unique from traditional solutions in that it surfaces metadata and integrates management processes into the Tableau analytics platform where people are already spending their time in analysis. With the [Tableau Data Management Add-on](#), you get a solution that's designed with multiple people in mind. It also remains heavily focused on analytics so people get the information they need when and where they need it—directly in the flow of their analysis. Plus, the visual interface provides a better way to interact with your data, making the process faster and easier. Learn more about [Tableau's approach to data management](#) and how you can increase visibility, reliability, security, and scalability in your data management processes.

Data management techniques include the following:

- **Data preparation** is used to clean and transform raw data into the right shape and format for analysis, including making corrections and combining data sets.
- **Data pipelines** enable the automated transfer of data from one system to another.
- **ETLs** (Extract, Transform, Load) are built to take the data from one system, transform it, and load it into the organization's data warehouse.
- **Data catalogs** help manage metadata to create a complete picture of the data, providing a summary of its changes, locations, and quality while also making the data easy to find.
- **Data warehouses** are designed for data analytics, which involves reading large amounts of data to understand relationships and trends across the data.
- **Data governance** is a set of principles and practices that ensure high quality through the complete lifecycle of your data.
- **Data architecture** is the process of standardizing how organizations collect, store, transform, distribute, and use data.
- **Data security** protects data from unauthorized access and corruption.
- **Data modeling** is the process of creating data models by which data associations and constraints are described and eventually coded to reuse.



DATA LIFE CYCLE

Steps in Data Life Cycle:

- **Generation** occurs regardless of whether you're aware of it, especially in our increasingly online world. Some of this data is generated by your organization, some by your customers, and some by third parties you may or may not be aware of.
- **Collection** Not all the data that's generated every day is collected or used. It's up to your data team to identify what information should be captured and the best means for doing so, and what data is unnecessary or irrelevant to the project at hand.
- **Processing** Once data has been collected, it must be processed. Data processing can refer to various activities, including data cleaning, data compression, and data encryption
- **Storage** After data has been collected and processed, it must be stored for future use. This is commonly achieved through the creation of databases. These databases are stored in the cloud, on servers, or using another form of physical storage like a hard drive, CD, cassette, or floppy disk.

- **Management** involves organizing, storing, and retrieving data as necessary over the life of a data project. While referred to here as a "step," it's an ongoing process that takes place from the beginning through the end of a project.
- **Analysis** refers to processes that attempt to glean meaningful insights from raw data. Analysts and data scientists use different tools and strategies to conduct these analyses
- **Visualization** refers to the process of creating graphical representations of your information, typically using one or more visualization tools. Visualizing data makes it easier to quickly communicate your analysis to a wider audience both inside and outside your organization.
- **Interpretation** provides the opportunity to make sense of your analysis and visualization. Beyond simply presenting the data, this is when you investigate it through the lens of your expertise and understanding.

PRODUCTIVITY
With good data management, your company will be more organized and productive. Employees will have an easier time finding, understanding, and relaying information.

COST EFFICIENCY
Data management can help your organization avoid unnecessary extra costs such as unneeded duplication. When data is easily accessible, You won't have to worry about employees conducting the same research over and over again.

OPERATIONAL NIMBLENESS
Great data management makes it easy for companies to respond quickly to the world around them. This means companies can respond efficiently to market changes and react appropriately to competitors.

SECURITY RISKS
Proper data management helps ensure that your information stays secure and never ends up in the wrong hands. A strong data management system will help protect your information from theft and attacks.

REDUCED DATA LOSS
With a data management plan in place, you greatly reduce the risk of losing vital company information. It also ensures your important information is backed up and retrievable in case something happens to the original copies.

ACCURATE DECISIONS
Proper data management helps ensure all employees and workers view and analyze the same, most recent information. This helps ensure that your company will be making the most accurate decisions based on the most accurate information.

WHY IS DATA MANAGEMENT IMPORTANT?

Source: <http://www.blue-pencil.ca/what-is-data-management-and-why-it-is-important/>

blue-pencil
Information Security

Who's Using Data Management?

Retail



Understanding customers and responding appropriately to expectations requires having an accurate, up-to-date view of all the data - whether it's streaming, cloud based, or stored in a data lake or warehouse. From marketing to merchandising to sales, trusted data management is essential to taking charge of retail data.

More retail solutions ➔

Manufacturing



In the manufacturing industry, nothing speaks success like quality. With solid data management and data quality technologies, manufacturers can efficiently manage product inventory, and integrate structured and unstructured data from all sources to get an enterprise view of performance, drive better outcomes and make well-informed business decisions.

More manufacturing solutions ➔

Banking



More than ever, issues around data privacy, compliance and digitization require banks to have a trusted data foundation. Only with a complete, integrated view of all their data - and sound techniques for quality, governance and personal data protection - can banks gain customers' trust and pursue forward-looking digital transformation efforts.

More banking solutions ➔

Health Care



Enterprise data management is a must-have in the health care industry. The industry counts on being able to integrate data from all formats and sources - including data from outside of the organization - all while spotting duplicate data, fixing data quality issues, and adhering to strict regulatory and compliance requirements for protecting personal data and privacy.

More health care solutions ➔

Government



Local and national governments are responsible for a vast range of services and programs. Reliable data management technologies support all those efforts - from fighting fraud and improper payments to ensuring citizen safety to overseeing population health outcomes, economic development and smart city initiatives.

More government solutions ➔

Small and midsize business



As small and midsize businesses work toward digital transformation, they need to implement data-driven business models and modernize legacy IT so they can be competitive with their larger counterparts. One way to get there is with reliable data management technology that can be catered to the needs of smaller businesses.

More SMB solutions ➔

Learning and Self-Development

Learning on the job, recipe for the best results.

- **70%** of what we learn, comes from our daily work. For example, we get new assignments and challenging jobs, of which we do not exactly know how to do them. By doing them anyway, we learn. Sometimes by trial and error.
- **20%** of our new knowledge and skills, we develop through feedback and tips from colleagues and by watching how other people do it.
- **10%** of what we learn, we extract from formal learning contexts, such as training, e-learning and workshops.
- That's what we call **70:20:10**.

Learning at work

- Workplace learning helps people build the skills and knowledge they need to do their jobs. That could be picking up something in the flow of work or developing to advance their careers.
- Short or long-term, learning motivates people – and provides organizations with the workforce needed to perform better and adapt to future challenges.

Indisputable benefits of personal development at work

- It helps you get realistic picture of your skills and knowledge If you weren't concerned with your personal development that much before, you probably don't realize your competencies objectively. Personal growth starts with accessing where you are at the moment, i.e. keeping track of your skills and behaviors. By controlling them, you'll understand your areas for growth, both professionally and personally. It applies for all types of jobs, even those outside of the office (to find out more about the world's weirdest and curious jobs, continue reading here: <http://resumeperk.com/blog/top-weirdest-jobs-youll-be-curious-to-discover>)
- It will boost your motivation Becoming totally aware of your strengths, weaknesses and level of skills can increase your motivation levels in the long run. How does that work? As you understand your positive and negative attitudes, their consequences and how they affect others, you learn to act differently and more productively. If you are persistent enough, you and the other team members will see the result. And observing the results of your own personal growth will give you a boost of confidence and motivation for even bigger achievements. If you experience loss of motivation at the moment, read here what may cause it and how to regain motivation for work: LINK. Is it your resume that you're unmotivated to write on your own? Our expert resume writers know how to assist you with this.

• It helps you advance your skills

Personal development at the workplace is closely connected to developing skills needed in your role. Since you've realized your areas for improvement, you will know which skills to focus on to achieve your long-term career goals. And, by developing them, you'll be seen as a more dynamic and proactive to your colleagues and management and maybe will get the desired promotion faster. Sounds attractive, doesn't it? Moreover, knowing that you develop your personality, not just perform the duties assigned to you, you'll find it more pleasant to grow and learn more.

There are a plenty of skills in the modern world of work that can predetermine your successful career. Learn more about these skills and how to develop them here: <http://resumeperk.com/blog/10-skills-for-career-success-from-cv-proofreading-service>.

• It will enable you to master goal-setting

Most people get it wrong how to [set either professional or personal goals](#). We tend to dream of something bad that is hard to achieve or, in contrary, focus on minor, day-to-day responsibilities that aren't taking us anywhere. When you start working on developing your personality, it will require you to create a plan and set smart goals. These goals will be based on the assessment of your current professional level, your professional goals within the organization and your personal objectives and preferences. It's hard to commit to goals imposed on you; however, when you set goals which are truly yours, you understand how to set goals right and how to break major ones into small, achievable steps.

Getting an outlook of your past career record is helpful for understanding your future direction, career experts say. Your resume is a great tool to do this. If your resume is inconsistent and lacks structure, you can get [your resume done at an affordable price](#).

• It helps you develop positive attitude to work

The job that doesn't contribute to our growth and doesn't allow us to learn and develop ourselves eventually starts to depress us and destroy our motivation. Even though some employers say that you should care of your personal development outside of work, it's indisputable that work is the perfect site to develop all attributes of your personality. When your work allows you to do so, it helps you feel more inspired and motivated, which results in your success at work.

Do you feel uninspired at work and can't figure out the reason of this? Learn about the methods to restore your inspiration and inner drive: <http://resumeperk.com/blog/10-ways-to-find-lost-desire-and-inspiration>

• It focuses you on discovering your life purpose

Are you one of those personalities who can say for sure what their life purpose is? Then, you'll be surprised to find out that finding your calling is one of key topics in personal development. In other words, people often start developing themselves just to identify their goal in life and stick to it.

If you're still searching, by focusing on accessing your current state both in personal and private life and taking steps for the sake of personal growth will streamline this process. By following your passion and advancing your skills you'll find your true calling faster. And, as soon as you've defined your major goal, you'll be astonished at how rewarding your professional life can be.

If finding your true calling is the primary focus of your interest right now, see what you can do about it:

<http://resumeperk.com/blog/discover-your-true-calling-tips-from-resume-services-online>. For those in the middle of career change, it's important to make sure your resume reflects this change properly. [Consider contacting resume professionals](#) for assistance.

Personal development at work: where to start

Historically, the success has been measured by academic and professional achievements. The matter of personal growth has been downplayed; nevertheless, millennials are more concerned about this issue than their parents. Moreover, if personal and organizational developments are integrated, we tend to achieve better results and feel more satisfied than if we achieved some goal that doesn't ring true to us.

One way or another, your personal development is up to you. Here are a few working approaches and tips if you want to advance your life but don't know where to begin:

Collect the feedback

As we've mentioned above, your personal and professional growth starts with understanding of your current state. In other words, to understand the areas for improvement, you need to know both the areas of your strength and the skills you lack in. Collecting feedback from management and coworkers can be a good start.

- **Ask for feedback with examples** – everyone at work, even clients, can provide you with a piece of valuable information regarding your work. So, don't be shy to ask to evaluate your work and analyze the feedback.

- **Value the constructive criticism** – [criticism at work is inevitable](#); so, take it in your stride and use to develop your skills and attitude.

Ask for mentorship/coaching

Coaching is necessary to provide you [support and advice for your personal development](#). It will help you to stay on track when the things get complicated and show the way out when you feel stuck. Moreover, a quality coaching will speed up the process of your development.

- **Consult your manager or supervisor**. Your direct boss is the perfect mentor candidacy as he observes your work day to day. Make sure he/she understands your career goals and aspiration, as well as personal preferences. In this case, they'll assign you the tasks which will help you develop faster and better, helping you develop according to your long-term goals in context of organizational goals.

- **Partner with a colleague**. If you don't get on well with your boss, try finding a colleague with the same need for personal growth and coach each other. You don't need to have the same goal in mind; what you'll need to do is to check in on a weekly basis and report your progress to each other.

Not every subject is okay to discuss with the coworkers. Remember than some [topics for conversation don't belong to workplace](#), so it's better to avoid them.

- **Find an outside mentor**. The company doesn't allow much space for growth or mentorship opportunities? Try hiring an outside career coach. Having someone by your side will keep you motivated.

Put your hierarchy of needs in order

According to Maslow, a [personal development occurs through the process of self-actualization](#). He suggested that human needs form a pyramid where each need is based on the previous ones. Only when the needs of a lower level are satisfied, you become capable of developing higher ones. At the top of this pyramid he placed **self-actualization** – the process of individual's becoming the best he is capable of becoming.

The basic human needs such as food, drink, temperature regulation, sex and sleep are placed at the bottom of this pyramid. Safety, both physical and economical, forms the next level. Third, there goes a need of love and belongingness to some group and society and higher up to self-actualization.

The matter is if your personal development at work isn't effective enough, maybe, some of your lower-level needs are dissatisfied. Just like it's impossible to look for a new job without a [well-written professional resume](#), it's tough to pay all of your attention to developing yourself when you are bothered by poor relationships with family members or cannot trust others. In this case, you'll need to go back to those needs and resolve any pending issues to fully focus on your personal growth.

Develop yourself through enhancing your skills

As soon as you have defined your areas for growth and aligned your goals with the employer's expectations from you, it's time to create a plan for your development. There's a vast array of possible future goals from you; however, most of the goals people set will require a few skills from the list below. They all help you [achieve huge work success](#) and get more satisfied in all areas of your private life.

Time management skills

Ability to organize tasks, prioritize them, schedule into to-do list and complete on time (or just with insufficient delays) – all these skills can be grouped under **time management** term. Managing tasks and priorities are critical for developing, successful personality. It's impossible to imagine a respected individual who can't get work done according to deadlines.

- **Eat the frog** – time management experts suggest that you start your working day with the most critical or unpleasant task instead of delaying it. This will contribute to your willpower and relieve you from stress for the rest of the day.
- **Start planning by scheduling important tasks** – put critical tasks into your to-do list first and then add secondary, minor tasks that can be delayed without damage.
- **Tight schedule isn't your friend** – it's impossible to plan every factor that can possibly arise. That's why it's important to allocate blank spaces into your schedule, so you will have extra time to complete the task if it happens to require more time than you estimated.

Unitasking

As opposed to multitasking, unitasking is the process of focusing on one activity at a time. And this is considered to be a healthier approach to work than multitasking. The latter isn't the effective approach to work, except just a few roles (i.e. a manager of a busy store who needs to resolve lots of customer issues on the go). In fact, the habit of [multitasking lowers your IQ, boosts stress levels](#) and causes mistakes at work.

Unitasking enables you to focus entirely on the same task for a long time, boosting your concentration and ensuring high quality of work you produce. Moreover, it helps you enter a flow state in which you can work faster and more productively than usual. Mastering work in a flow state will be a huge step for your personal development.

Stress management

An accomplished career requires physical and mental stamina. Nevertheless, things don't always go smooth at work, and we all are subjected to workplace stress. Short-time stress isn't dangerous and can even facilitate your development at work. However, if accumulated, stress can pose a major risk for your mental, physical and emotional health. In the extreme cases it can even lead to clinical anxiety which is actually a disorder requiring professional help.

That's why it's critical to manage your levels of stress timely. If this is the routine that prevents you from personal development and causes stress, learn how to [get rid from routine at work](#). Here are a few more techniques for your perusal:

- meditation makes multiple positive effects on our body and mind, and stress reduction is just one of them. It lets you to relax your body and get away from annoying thoughts, thus helping you get away from stressful obstacles at work.
- **Take your time for hobbies** – if there's some activity that you truly enjoy, don't put it aside to focus on work. Personal development implies that you focus on doing things that bring you satisfaction and joy. So, be sure to allocate some time for your hobby every day (or every other day) – it will help you remain stress-resistant.
- **Talk it out** – if you feel depressed or anxious, don't keep the things bothering you within. Talk to your friends, colleagues, family or even therapist – it can reduce your stress levels. Surprisingly, when we speak about our problems aloud, we can unexpectedly come across the solution.

If it's your resume writing that won't let you stress out, it's time to learn more about [our services and prices](#) for resume help.

Conflict resolution

Workplace conflicts aren't rare. Conflict is defined as difference in opinion, approaches to work or disagreements of any kind, and may lead to hurt feelings and drop of productivity in the department or company. In any case, if conflict isn't resolved and handled properly, it will destroy the relationships within the team and lead to a plenty of other unpleasant consequences. That's why a person with conflict resolution skills is valued in any organization.

Moreover, mastering this skill will develop a plenty of valuable personal qualities in you, such as the ability to make unbiased decisions, be more patient towards other people's opinions and views and come up with win-win solutions. Basically, conflict resolution involves the following skills:

- **Active listening** – as the conflict arbitrator, you'll need to ask open-ended questions and listen carefully to the answers to understand the nature of conflicts and every point of view objectively.
- **Empathy** – this skill is about having a look at the situation from different perspective. This will enable you to realize how each party feels about this conflict and encourage them to do the same, helping to evaluate the conflict and its influence in full.
- **Creative problem solving** – if the conflict exists, this is the sign that a situation couldn't be resolved using traditional methods. Creativity is the must to offer the solution that will leave both parties satisfied; if creativity isn't your biggest strength, learn how to [get your creative juices flowing](#).

Interviewing

Surprised? Well, you shouldn't be. Since an average worker changes job approximately once in 3 years, passing interviews with brilliance will help your career a lot. Moreover, only the top companies offer lucrative opportunities for personal development, which results in fierce competition for these roles. The more seasoned you are at impressing interviewers and selling yourself as the top candidate for the role, the faster you'll be getting jobs you like at any stage of your career. This is what you should pay specific attention to:

- **Master the basic rules of interviewing** – make sure that such trifles as not knowing details of the company or showing up late won't break it. Learn the key [tips for passing interview successfully](#) to get started.
- **Practice different interview types** – online interview, group interview, phone interview... There are lots of interview types, each with its own peculiarities and recipes for success. Getting accustomed to each type of interview through [personal interview preparation](#) and practice will make your personality flexible in any circumstances, and you'll go a long way.
- **End on a good note** – how you end the interview determines whether you'll be remembered or not. The [catchy questions for the end of interview](#) will help you stand out from the pool of candidates.

Confidence and emotional intelligence

There's a strong correlation between your confidence levels and success. Why? Confident individuals at work are perceived as more competent, more easy-going and they are assigned complex projects more often than their coworkers who are shy about their knowledge and skills. That's why gaining confidence should become one of top priorities for your personal development. Since [self-esteem is what you think about yourself](#), it can – and should – be trained, and the others will see you as a more confident personality.

Emotional intelligence, in its turn, determines how well you communicate with others, your perseverance and self-control. These qualities make you pleasant to work with in a team.

Good written communication

Written communication such as business letters, e-mails, contracts, etc. is not going anywhere and valued in majority of office roles. Mastering clear, concise and accurate writing will help you express your thoughts better and faster and ensure effective communication with teams and stakeholders. Moreover, strong writing skills are the sign of a developed individual.

- **E-mail writing**: [good e-mail writing](#) can be learned, so put mastering this skill into your personal development plan. Grammar, structure, word choice and even signature – everything matters when it comes to writing effective emails.
- **E-mail title**: When composing an e-mail, it's important to think of a short yet informative subject line. It's the subject line that often determines whether the letter will be read or not.
- **Business letter writing**: during your professional career you'll have to deal with business letters a lot. This is especially true for [cover letters which need to be customized](#) for jobs you apply. Ability to author excellent letters will contribute a lot to your professional image.

Why learning in the workplace is important?

- With the rise of technology such as artificial intelligence and automation, many organizations sense an urgent need to up- or re-skill their workforces.
- But learning doesn't just build skills, it motivates people too. The opportunity to learn and develop is the most important driver in employee happiness after the nature of their job.
- It is worth hearing your learners out. Organizations with engaged learners are 12% more likely to increase on-the-job productivity and 28% more likely to respond faster to changing market conditions.

Workplace Learning Types?

- **Formal or structured learning** such as classroom teaching, e-learning or MOOCs which guide the learner.
- **Informal or unstructured learning** that enables people to learn what they want, when they want to. Like online resources such as articles, videos and podcasts.
- But the two types of learning often overlap. A formal course, for example, may include a video that learners can watch on their own time.
- Today, many organizations favor a blend of formal and informal, synchronous (real-time) and asynchronous (any time) learning.
- Studies show employees with access to a blend of activities are more motivated to learn than those with access to one approach. What's more, blended approaches prove more effective at putting learning into practice.

Workplace learning opportunities, programs and strategies

- **Apprenticeships**. Highly specialized leaders at your organization can directly train employees, or apprentices, on hard or soft skills related to their area of expertise.
- **Mentorships**. One-on-one instruction opportunities between junior and senior staff members can help nurture a mutually beneficial relationship that cultivates professional and skills development.
- **Workforce education programs**. Invest in an education program that provides employees the ability to earn degrees, credentials or certificates from an academic institution.
- **Independent learning**. Encourage employees to seek out ways to learn informally outside of the workplace. This can include access to volunteering opportunities or industry-relevant events and conferences.
- **Training**. Leverage internal or external experts to host workshops, lectures or seminars around relevant skills-based topics to support learning and knowledge sharing.

How to create a learning culture in the workplace?

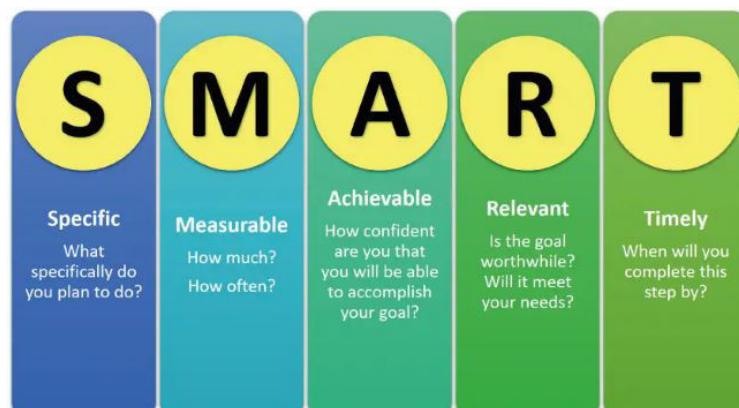
- **Celebrate success.** Keep your employees motivated by acknowledging their accomplishments.
- **View learning as a business strategy.** Align employee development with the larger goals of your company to ensure your efforts drive growth and deliver a ROI.
- **Start with the C-suite.** Company culture starts at the top of an organization — this means upper management should prioritize their own learning and development alongside everyone else.
- **Prioritize skill building.** Boost employee confidence by committing to skill building programs that can help them get to the next level in their career. Be transparent and provide team members with tangible outcomes to encourage participation.
- **Encourage communication.** Empower employees at all levels to share their learning experiences and support one another in their mutual growth.

How to measure your workplace learning strategy?

Here are some of the most important key performance indicators (KPIs) to track:

- **Skills retention.** How long after training do employees keep acquired knowledge and skills? Do they require additional training to maintain information and abilities?
- **Time to proficiency.** How long does it take your employees to integrate training? How quickly are new skills being learned? How well are these skills being performed?
- **Knowledge transfer.** How effectively are your employees applying learning to on-the-job activities? Is their understanding of the training purely theoretical or are they successfully using these skills in their respective roles?
- **Engagement.** What percentage of your employees are taking advantage of your education initiatives? What is the return-on-investment (ROI) on your learning investments?

Goals for personal development in workplace



Benefits of personal development at work

- It helps you get realistic picture of your skills and knowledge
- It will boost your motivation
- It helps you advance your skills
- It will enable you to master goal-setting
- It helps you develop positive attitude to work
- It focuses you on discovering your life purpose

Personal development at work: where to start

- Collect the feedback
- Ask for mentorship/coaching
- Put your hierarchy of needs in order
- Develop yourself through enhancing your skills
- Learn Time Management
- Unitasking
- Stress management
- Conflict resolution
- Confidence and emotional intelligence

What is a cyber crisis & how can a small business stay prepared?

Ransomware attacks against small businesses are running rampant. Nearly half (43%) of all cyber attacks now target organizations with 250 employees or fewer. Reports also suggest there's a one-in-two chance your small business will be hit with some form of cyberattack in the next 12 months. In fact, one in five small businesses have already been hit with ransomware.

What is a cyber crisis?

A cyber crisis is when a cybercriminal places ransomware on your website or files and holds your information and data until you pay a ransom. When ransomware hits, the average small business experiences two full days of downtime. They pay anywhere from a few thousand to tens of thousands of dollars to get their data back. One-third of them lose actual revenue, and all of them experience brand and loyalty damage that's much harder to quantify and recover from.

Unfortunately, while most small businesses end up paying the ransom, that doesn't guarantee anything. Plenty of businesses have fully complied with the ransom demands, only to have the hacker increase the ransom request—or simply take off with the ransom and your data. It's no wonder, then, that 41% of surveyed small business customers find that ransomware, phishing attacks, and other viruses are the top threat to their business data.

Why does my small business need a cybersecurity and disaster recovery plan?

Cyberattacks increasingly target small businesses. Cybercriminals know smaller organizations have fewer resources to dedicate to data security, making them an easier target. Compromising just one user often grants the hacker the "keys to the castle."

With a seemingly harmless click on a link or email attachment, ransomware quickly and silently installs on a victim's device and mounts an extortion attack, demanding a ransom in return for access to their data. And if that user is connected to a cloud collaboration tool, such as Google Drive, OneDrive or Dropbox, the virus can spread to the rest of the organization in minutes. Now the whole company is in trouble.

What do I need to start cyber recovery planning for my small business?

Don't wait for a disaster to happen – start a cyberattack recovery plan

Many small businesses may not see the importance of a disaster recovery plan until it's too late. Their data gets compromised, their customers are now vulnerable, and money goes down the drain – next thing you know, their doors may be closing.

Protect your business and its critical data by starting a disaster recovery plan that:

- Has a clear owner
- Involves many partners from across the business
- Is simple to execute
- Leverages a comprehensive, multilayered approach
- Is regularly practiced and continuously updated

Steps to creating a disaster recovery plan

If you're still wondering about cyber crisis management plans, or how disaster recovery ties into it, use our 10 guidelines below. These steps will help you establish a disaster recovery and cybersecurity plan while taking into account the key points bulleted above.

1. Establish an owner

While the expectation of protecting the business from cyberattacks often falls on the IT department. In a small business, however, this department may already be contracted out or too busy with other issues to take this head-on.

This means it will be important for you to identify someone in the organization who can own the development of the disaster recovery and cybersecurity planning. This person should be organized, comfortable collaborating with people across the organization, and able to add creation, review, and maintenance of the plan as a core responsibility of their job. Business leaders and managers must also support this person's work in order for it to get the attention it needs from the rest of the organization.

2. Identify representatives from each area of the business

Creating a plan that impacts the entire business will require input from every area of the business. Here's how to put this step into action:

As a group, identify which tools and data are most critical for each team to do their work, and then document who has access to those tools and data.

These documents will need to be updated as employees come and go, or move within the organization. This will require clear and crucial communication between team leads.

These people will also participate in table-top exercises that will allow your business to practice "what if" scenarios and will test your plan before you actually need it. Make sure to include off-hour contact information for everyone on the team in case an incident occurs outside of normal working hours.

3. Document your risks

Small business risks could include a multitude of events: natural disasters, a vendor or business partner shutting down, a ransomware attack, or simply an unfortunate user error.

This is where the full team can help brainstorm the possibilities:

What if a supplier goes out of business?

What if a disgruntled employee deletes a bunch of data before walking out the door?

What if our office closed down after a hurricane?

Talking through what steps you would need to take to recover from each of these will quickly identify actions to mitigate those risks and what the priority should be.

4. Specify which data, technologies, and tools are most critical

Each department has data and systems they need to function.

Accounting needs access to payroll data, developers need their code repository, sales needs their customer lists, fulfillment needs order information, etc.

While all of these systems and technologies are important, in the event of a disaster, you can't fix everything at once. The disaster recovery team should determine the amount of time the business can reasonably survive without that system or technology, who "owns" that system, and who will be responsible for restoring it. All of this information should be added to your disaster recovery document in step 3.

5. Maintain an inventory of physical assets

Ensure that you keep an updated list of all of the equipment your business uses on a day-to-day basis. This includes not only computers, servers, printers, phones, and network hardware, but other equipment such as office furniture, product inventory, shipping supplies, etc.

As you are creating this list, ask yourself: What would I need to go buy if I had to rapidly set up a new office location somewhere else? And don't forget to contact your insurance company as you are developing your list. They will help you understand what specifically you need to track and how they can help you get up and running post-disaster.

6. Determine where and how critical business information will be backed up

Around 60 percent of all small business data lives on desktops and laptops. If you want to ensure every important file is covered, then you need a backup solution that includes the following features:

Protection for every computer – Around 60 percent of all small business data lives on desktops and laptops. If you want to ensure critical data is

covered, then you need a solution that automatically protects data on every laptop and desktop.

Taps the benefits of cloud backup – The cloud enables leading data backup providers to offer unlimited protection. It also provides fast and simple user-driven recovery of important information.

Runs automatically – Your data backup solution should run silently and automatically in the background without requiring any action by users or impeding their productivity.

Prioritizes easy recovery – You should be able to specify a point-in-time for your restore and recover your files to any device, without needing a VPN connection.

7. Create a communication plan

When disaster strikes during off-hours, how will you notify employees? Should they report to the office that day? Should they work remotely or an alternate office location? How will customers and vendor partners be notified? Who should handle questions from the media? Where will you store/update contact information for each of these groups?

Not every disaster will merit communication with every constituency, but you should make a plan for identifying how and when these communications will occur as well as who owns that work.

8. Practice! Practice! Practice!

Have you heard the term "table top exercise" before? It simply refers to your disaster recovery team sitting around a table and discussing, in detail, how the company will respond to various given scenarios from your list of possible risks.

Here's an example:

Imagine an employee clicked on a link in an email that appeared to be legitimate — it turns out it was a phishing attack, and now every computer in your company is locked. And no surprise — the hackers are demanding a ransom. Let the team then talk through what they would do!

There will inevitably be questions that come up about which systems are available, who needs to be involved in addressing it, and who needs to be notified. All of these questions will give you an opportunity to put plans and answers in place so that you aren't left scrambling when the incident occurs. The more you practice, the better the team gets and the more prepared you will be.

Cybersecurity and Disaster Recovery Plans

While the primary role of disaster recovery plans is to ensure business continuity, cybersecurity protects IT assets from numerous threats that digital environments face. Cybersecurity disaster recovery plans aim to reduce the impact of unexpected attacks and incidents. A lack of these proper plans means businesses are not prepared to deal with any cyberattack which leaves its whole infrastructure vulnerable. As a recovery strategy, these plans exhibit enough activities to enable the restoration of business operations as quickly as possible. These plans are designed to provide limitless resilience power to reduce the occurrence of any such attack in the future. As such, there are different cybersecurity disaster recovery plans that businesses can take advantage of, as highlighted below:

Types of Cybersecurity Disaster Recovery Plans :

Data Center Disaster Recovery Plan

This plan covers the whole infrastructure that houses the data center and not just the computing facility it is housed in. The tools and characteristics within the infrastructure like support personnel, physical security, utility providers, HVAC, backup power, and even fire suppression — all have an impact on the data center. If any type of outage occurs, these features and tools within the infrastructure are expected to work efficiently. This ensures that the business' data has a very low risk against cybercriminals and intruders.

Cloud-Based Disaster Recovery

When applying a cloud-based approach, businesses can cut on costs by utilizing a cloud provider's data center as a recovery site, instead of spending more on its own data center's facilities, systems, and personnel. Businesses can also benefit from the competition among cloud providers as they offer competitive deals, allowing them to save money. Before adopting this approach, businesses should determine the issues that the cloud providers may have, especially with recovery and back-up. This is because the cloud provider serves a critical role in fixing problems, therefore gaining an understanding of them before making them part of the disaster recovery plan is crucial.

Virtualization Disaster Recovery

Virtualization disaster recovery is a way of data recovery that mainly involves replication, therefore allowing a business to failover to virtualized workloads. This approach avoids the need to rebuild a physical server if a disaster occurs. Businesses can achieve their targeted recovery time objectives (RTO) more easily and efficiently by having a virtual server on cloud or reserve capacity. Virtualization helps simplify disaster recovery when integrated into a business properly. This automation of disaster recovery tasks through virtualization helps save time while providing businesses with a reprieve from human error,

which is vital. Virtualization also helps businesses decrease the amount of time required to undertake a full restoration. For the most effective and efficient virtual disaster recovery, a business is expected to copy virtual machine workloads off-site regularly, to help minimize loss when an attack or problem occurs.

Disaster Recovery as a Service

While Disaster Recovery as a Service (DRaaS) is mainly based on the cloud, it is not a strictly cloud-based service. Some DRaaS providers provide their solutions to businesses as a site-to-site service where they can host and run a secondary hot site. Moreover, service providers can reconstruct and ship servers to an organization's site as a server replacement service. Cloud-based DRaaS allow businesses to failover applications, reconnect users through Remote Desktop Protocol or VPN, and also effectively undertake fallback to rebuilt servers. Businesses must understand that some DRaaS solutions own their providers while others partner with other vendors. This helps ensure that what the vendor is offering works with the business' products.

A comprehensive cybersecurity disaster recovery plan is difficult to create, but this does not mean that businesses need to struggle. Cybersecurity disaster recovery plans offer different features and tools that ensure businesses are better placed when attacks do occur. Businesses are, however, required to make sure they understand what products are offered by vendors and how they assimilate with their products. Ensuring this helps guarantee that a business' data is safer from natural disasters, cyberattacks, and even simple human errors.

Understanding different recovery plans is essential to becoming a disaster recovery professional. There are a diverse number of cyber disaster recovery training for employees that your organization can

register for. One of the most popular business continuity planning (BCP) training courses is the EC-Council Disaster Recovery Professional (EDRP) program, which offers IT professionals, CISOs, cybersecurity professionals, and other cybersecurity lovers an extensive knowledge of business continuity and disaster recovery ideologies.

Cybersecurity Audit Checklist

Today's network and data security environments are complex and diverse. There are hundreds of pieces to a security system and all of those pieces need to be looked at individually and as a whole to make sure they are not only working properly for your organization, but also safe and not posing a security threat to your company and your data or the data of your customers.

Risk management and risk assessments are important parts of this process. Data loss and data breaches are detrimental to your organization and can make or break a company, especially if a breach causes other organizations to lose confidence in your ability to keep yours and their data secure. For this reason, it is absolutely critical for you to perform regular audits of your environment.

There are hundreds of items that could be on a cybersecurity audit checklist. Here are some broad categories and ideas that cover many of the crucial cybersecurity threats:

1. Management

- 1. Company security policies in place**
- 2. Security policies written and enforced through training**
- 3. Computer software and hardware asset list**
- 4. Data classified by usage and sensitivity**
- 5. Established chain of data ownership**

2. Employees

- 1.** Training on phishing, handling suspicious emails, social engineering hackers
- 2.** Password training and enforcement
- 3.** Training on dealing with strangers in the workplace
- 4.** Training on carrying data on laptops and other devices and ensuring the security of this data
- 5.** All security awareness training passed and signed off ensuring that all employees not only understand the importance of security but are active guardians for security
- 6.** Ensure that Secure Bring Your Own Device (BYOD) plans are in place

3. Business practices

- 1.** Emergency and cybersecurity response plans
- 2.** Determine all possible sources of business disruption cybersecurity risk
- 3.** Plans in place to lessen business disruptions and security breaches
- 4.** Emergency disaster recovery plans in place
- 5.** Alternative locations for running business in case of emergencies or disruptions
- 6.** Redundancy and restoration paths for all critical business operations
- 7.** Have you tested your restoration and redundancy plans?

4. IT staff

- 1.** System hardening plans
- 2.** Automated system hardening on all operating systems on servers, routers, workstations, and gateways
- 3.** Software patch management automated
- 4.** Security mailing lists?
- 5.** Regular security audits and penetration testing
- 6.** Anti-virus software installed on all devices with auto-updates
- 7.** Systematic review of log files and backup logs to make sure there are no errors
- 8.** Remote plans in place, as well as policies regarding remote access

5. Physical security

- 1.** Lock servers and network equipment
- 2.** Have a secure and remote backup solution
- 3.** Make sure keys for the network are in a secure location
- 4.** Keep computers visible
- 5.** Use locks on computer cases
- 6.** Perform regular inspections
- 7.** Prevent unauthorized users from entering the server room or even in the workstation areas
- 8.** Security camera monitoring system
- 9.** Key Card system required for secure areas

- 10.** Secure Data Policy in place and ensure users understand the policy through training
 - 11.** Secure trash dumpsters and paper shredders to prevent dumpster diving
- 6. Secure data**
- 1.** Encryption enabled wherever required
 - 2.** Secure laptops, mobile devices, and storage devices
 - 3.** Enable automatic wiping of lost or stolen devices
 - 4.** Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers
 - 5.** Secure email gateways ensuring data is emailed securely

7. Active monitoring and testing

- 1.** Regular monitoring of all aspects of security
- 2.** Regularly scheduled security testing
- 3.** External penetration testing to ensure your staff hasn't missed something
- 4.** Scanning for data types to make sure they are secure and properly stored

There are three levels of security in an organization. Information Security or InfoSec encompasses everything and refers to the processes and information technology designed to protect any kind of sensitive data and information whether in print or electronic form from unauthorized access.

Cybersecurity is a subset of InfoSec and deals with protecting internet-connected systems including hardware, software, programs,

and data from potential cyberattacks. It protects the integrity of networks from unauthorized electronic access.

Cybersecurity is the practice of defending your organization's networks, computers and data from unauthorized digital access, attack or damage by implementing processes, technologies and practices. There are many sophisticated threats targeting many organizations and it is critical that your infrastructure is secured at all times to prevent a full-scale attack on your network and risk exposing your company' data and reputation.

Network Security is a subset of cybersecurity and deals with protecting the integrity of any network and data that is being sent through devices in that network. We discussed Network Security in another blog entry. This blog also includes the Network Security Audit Checklist.

Governance Framework

When creating an information systems security program, start with proper governance structure and management systems software. There are many articles on this website about what governance frameworks are, but it is the framework established to ensure that the security strategies align with your business objectives. Governance aligns business and information security, so the teams can efficiently work together. It also defines the roles, responsibilities and accountabilities of each person and ensures that you are meeting compliance.

CIA Model

When security experts are creating policies and procedures for effective information security programs, they use the CIA (confidentiality, integrity and availability) Model as a guide. The components of the CIA Model are Confidentiality, Integrity, and Availability.

Confidentiality: Ensures that information isn't accessible to unauthorized people—usually by enabling encryption—which is available in many forms.

Integrity: Protects data and systems from being modified by unauthorized people; making sure that data has integrity and wasn't changed between the time you created it and the time it arrives at its intended party.

Availability: Ensures that authorized people can access the information when needed and that all hardware and software is maintained and updated when necessary.

The CIA Model has become the standard model for keeping your organization secure. The three principles help build a set of security controls to preserve and protect your data.

About Other Cybersecurity Audit Checklists

There are many sources of cybersecurity checklists you can find on the Internet. Some companies are happy to give away their checklists and others charge for them. Some are just the cost of a subscription email in hopes of selling you other products and services down the road.

It really doesn't hurt to start grabbing some of these security checklists as they are a great place to start developing your own, because you really need to make a checklist of your own. Nobody else has the same configuration of networks, devices, and software that you have.

Those canned lists are merely ballpark ideas of how you should be checking your security, as will the one included in this document.

For your checklist to be effective, you need to take a basic checklist or collection of checklists, put them together, and then add specifics for your environment. Also, because an organization is constantly changing, you will be making changes to it as time goes by. ZenGRC can help

streamline the process of creating and updating your information security controls, related objects such as risks, threats, and vulnerabilities, as well as audit and assessment tasks.

You may attend a new class about security that will give you ideas to add to your checklist. Or you may purchase a new firewall or some new anti-virus software that will make you rethink how you do a certain aspect of your checklist. You may also decide that you want to outsource your security checks, although even if you do that, you'll want to have your own checklist and compare it against what your outsourced consultants use to make sure that they have covered all the bases as well as add things from their checklist to yours.

Module 5 - Work related Problem

Common Work-Related Problems Among New Businesses

Problem 1: Making quality time to communicate with your employees.

Solve this problem by setting the bar of communication high. Whenever you can, communicate face-to-face. Phone calls, emails and texts are OK in a pinch, but they are a poor substitute for a fully present exchange.

Problem 2: Setting appropriate goals and expectations.

Solve it by referring to job descriptions to ensure that your employees understand the basics. Then, for special projects and ancillary goals, convene a brainstorming session, and set goals as a team. Your employees may surprise you by setting tougher goals for themselves than you would.

Problem 3: Proving yourself to a new team – and maybe even yourself.

Solve it by sharing your own job description with your employees. Seriously; and if you don't have one, draft one. It could be a wake-up

call like no other. Communicate your priorities, and above all else: do what you say you're going to do.

Problem 4: Encouraging productivity and creativity.

Solve it by finding out how your employees work best: starting work at the crack of dawn, working in teams, working from home occasionally or coming in on weekends to work when nobody else is in the office. They're all different, so they're bound to have different preferences. Accommodate those you can, and that accommodation should repay you tenfold.

Problem 5: Managing your time.

Solve it by stopping the juxtaposition in its tracks (i.e., letting time manage you). This will undoubtedly be one of the most vexing "work-related problems" you will face – and you'll probably swing back and forth like a pendulum between successes and setbacks. Several proactive steps will buttress the former: keeping track of appointments in a calendar, creating a daily to-do list to stay focused, setting aside certain blocks of time to read and reply to emails and freeing yourself from work for at least 15 minutes a day for private "think time."

Problem 6: Creating brand awareness.

Solve it by hitting the ground running, with exhaustive outreach efforts, creative public relations and promotional events, active blogging and an inbound marketing program that's second to none. Amidst such fertile ground – "watered" by discipline and persistence – your brand should grow in no time.

Problem 7: Generating leads.

Solve it by optimizing your website – your most important and potent sales tool. Each page should be built around a keyword (or two), steering visitors to landing pages and nudging visitors to take action – such as providing their email address. And your published blogs should always include a call to action. Generating leads is another of those

ongoing "work-related problems." But it should provide some semblance of consolation so that readers will believe that when it's optimized right, your website can generate leads while you sleep.

Problem 8: Balancing growth and quality.

Solve it by deciding which is more important: product (or service) perfection or customer service perfection. Of course, there's arguably no such thing as "perfection." And of course it's a lousy choice to have to make. But as a new small-business owner, you can bet that you will face this tough choice, whether you're reviewing a core product (or service) or an ancillary feature, such as your marketing content. If it helps, many "big business types" say it's more important to focus on customers, no matter what. Growth should spring from putting their priorities first.

Problem 9: Hiring talented people.

Solve it by refusing to settle for anything less than great – not merely good – employees. You probably have "ideal personas" for your target customers. Why not create personas for each position on your team to ensure a good culture and role fit? Your employees represent your biggest investment, and replacing them is costly.

Problem 10: Asking for help.

Solve it by identifying a mentor whom you can consult for advice. The sooner you do this as a new business owner, the better; the mentor will be in a better position to get a broad opinion of you and your fledgling business. If nobody immediately comes to mind, turn to your local chamber of commerce, a community college or to local business groups for potential candidates.

Common Work-Related Problems Among More Experienced Business Owners

Problem 1: Complying with laws and regulations.

Solve it by subscribing to relevant news feeds, reading the U.S. Department of Labor's Employment Law Guide and, perhaps above all else, hiring a competent business attorney.

Problem 2: Attending training and development sessions, including for you.

Solve it by making it a priority, incorporating benchmarks on employee evaluations and perhaps by offering incentives. But you may not have to. Challenged employees are usually the ones who stay on the job the longest and are the most loyal and productive.

Problem 3: Developing leaders.

Solve this problem by constantly looking for opportunities to give employees special assignments that challenge them. Also, enrolling them in regular leadership development programs will do volumes to ingrain a company culture that prizes creative leadership.

Problem 4: Delegating.

Solve this problem by forcing yourself to isolate tasks that don't require your higher level thinking and problem-solving skills, as well as your other talents. After all, you bring distinctive skills to your business – and the more time you spend on tasks that only you can perform – the more productive your business will become. If you can't delegate in-house – then outsource tasks that you can.

Problem 5: Responding to changing marketing tactics.

Solve it, while also remaining true to your marketing plan – the plan that outlines your overall strategy. Any new tactics should complement and advance your strategy. It can be too easy to become swept up in "knee-jerk" or "follow-the-pack" marketing. Nobody likes to miss out on a hot, profitable trend – but trends fade – and tactics aren't what drives marketing. If a tactic suits your strategy, use it. In addition to "firefighter," you'll become another small-business owner adjective – "risk-taker."