**1.Who are hackers? Explain different types of hackers? Illustrate different hacking Methodology?**

Hackers can be classified into three different categories:

* **Black Hat Hacker**
* **White Hat Hacker**
* **Grey Hat Hacker**

**Black Hat Hackers:**They are often called *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious action

**White Hat Hackers:**White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cybercrimes. They work under the rules and regulations provided by the government, that’s why they are called *Ethical hackers* or *Cybersecurity experts*

**Grey Hat Hackers:**Grey hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a grey hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers

**Hacker’s Methodology:**

**Foot printing**: This is a method that conducts a target analysis, identification and discovery typically through the use of open-source tools. This include dumpster diving, social engineering and the use of utility such as website hacking, treasurers, pings, network lookups etc.

**Scanning**: This step extracts information from foot printing and explores more data from it. This step includes pore scanning, operating system identification and determining whether or not a machine is accessible.

**Enumeration**: This is a phase where the hacker further interrogates a specific server to determine an operating system’s software. It includes searching for network shared information, the specific version of the application running, user account, traffic and more.

***Network Mapping***: This step is exactly as the name implies. Laying out an illustration of the target network includes taking all the resources, logs, target surveys, etc. to create a visualization of the target environment, this often looks different from the exploitative perspective.

***Gaining Access***: This step is the exploitation process. This is about gaining access to a machine or network by the client’s side, insider threat, supply interdiction or remote exploitation opportunity. Hackers use spear phishing, device exploitation and many more methods to conduct the exploitation.

***Privilege Escalation***: Depending on the exploitation opportunity, hackers decide the intensity of the exploitation, what kind of privileges he wants to escalate. They conduct it through local exploit opportunity in order to gain system-level privileges, the highest possible user.

***Post Exploitation***: This step is a compilation of many steps and is dependent upon the objective of the mission. It includes any combination of target surveys and remote forensic analysis, cover track (cleaners), data collection, backdoor implant resistance, computer network attacks, delay target survey and more.

***Forensic Analysis***: This step is to conduct analysis on the target machine for potential security mechanisms, fires or users which could either assist in obtaining the objective or harmed assessment. It basically analyses the target’s operating environment.

***Cover Tracks***: This is the process of removing any forensic relevant residue that was left behind as a result of exploitation. This is one of the most important steps that the hacker can perform.

***Data Collection:*** The attacker is in the present to perform some activity, which involves extracting as much data as possible. Network traffic analysis is the key to this phase.

**2. Elaborate the three dimensions of MC Cumber Cube?**

The Three Dimensions principles are:-

* **Confidentiality**
* **integrity**
* **availability**.

Confidentiality:-

Confidentiality is **the principle and practice of keeping sensitive information private unless the owner or custodian of the data gives explicit consent for it to be shared with another party**. Confidentiality may also refer to the request to honour the principle and practice.

Confidentiality means respecting someone's privacy, and abstaining from sharing personal or potentially sensitive information about an individual, especially if that information has been shared in confidence.

Confidential information includes **non-public information disclosed or made available to the receiving party, directly or indirectly, through any means of communication or observation**. Examples of confidential information are: Medical information.

Integrity:-

Integrity means **being honest and having strong moral principles**. A person with integrity behaves ethically and does the right thing, even behind closed doors.

It is defined as having strong moral principles and being honest. In other words, a person with integrity is someone who is truthful and can be trusted. Integrity is a very important virtue to have in life because **it helps you to be a good person**.

Availability:-

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.

Availability is one of the five pillars of Information Assurance (IA). The other four are integrity, authentication, confidentiality and nonrepudiation.

**3. How do you apply secure SDLC in each stage of software development?**

**Secure your SDLC to secure your business:-**

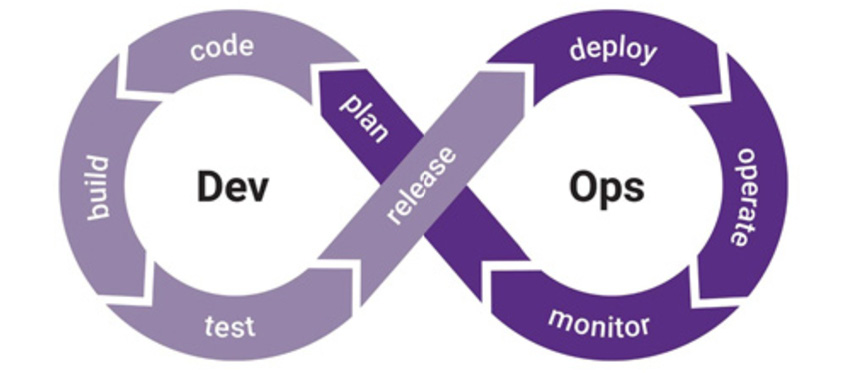
* Planning and requirements.
* Architecture and design.
* Test planning.
* Coding.
* Testing and results.
* Release and maintenance.

1.Planning and requirements:-

The most important phase of the SDLC is the requirement gathering and analysis phase because this is **when the project team begins to understand what the customer wants from the project**. During the requirements gathering sessions, the project team meets with the customer to outline each requirement in detail

2.Architecture and design:-

Architectural design is **a process for identifying the sub-systems making up a system and the framework for sub-system control and communication**. The output of this design process is a description of the software architecture. Architectural design is an early stage of the system design process.



3.Testing planning:-

This strategy includes tools needed, testing steps, and roles and responsibilities. Part of determining this strategy is a risk and cost analysis and an estimated timeline for testing.

**Creating an effective Test Plan involves the following steps:**

* Product Analysis.
* Designing Test Strategy.
* Defining Objectives.
* Establish Test Criteria.
* Planning Resource Allocation.
* Planning Setup of Test Environment.
* Determine test schedule and estimation.
* Establish Test Deliverables.

4.Coding:-

In this phase, **developers start build the entire system by writing code using the chosen programming language**. In the coding phase, tasks are divided into units or modules and assigned to the various developers. It is the longest phase of the Software Development Life Cycle process

5.Testing and Results:-

The testing phase of the software development lifecycle (SDLC) is where you focus on investigation and discovery. During the testing phase, **developers find whether their code and programming work according to customer requirements**

Test result means any document that contains a result of testing including all original test measures, all subsequent test measures that are not identical to the original test measure, and all worksheets on which calculations are performed.

6.Release and maintenance:-

The release phase of the Software Development Life Cycle (SDLC) is **traditionally associated with production, deployment, and post-production activities**. Which generally include maintenance and support of the software that has been developed

The maintenance phase of the SDLC **occurs after the product is in full operation**. Maintenance of software can include software upgrades, repairs, and fixes of the software if it breaks. Software applications often need to be upgraded or integrated with new systems the customer deploys.

**4. Illustrate the importance of a). Hashing b).Digital Signature.**

Hashing:-

Hashing **gives a more secure and adjustable method of retrieving data compared to any other data structure**. It is quicker than searching for lists and arrays. In the very range, Hashing can recover data in 1.5 probes, anything that is saved in a tree. Hashing, unlike other data structures, doesn't define the speed A balance between time and space has to be maintained while hashing.

There are two ways of maintaining this balance:-

1. Controlling speed by selecting the space to be allocated for the hash table
2. Controlling space by choosing a speed of recovery

Hashed passwords cannot be modified, stolen, or jeopardized. No well-recognized and efficient key or encryption scheme exists that can be misused. Also, there is no need to worry if a hash code is stolen since it cannot be applied anywhere else.

Two files can be compared for equality easily through hashing. There is no need to open the two documents individually. Hashing compares them word-by-word and the computed hash value instantly tells if they are distinct. This advantage can be used for the verification of a file after it has been shifted to a new place. It is an example of Sync Back which is a file backup program.

In DBMS, hashing is used to search the location of the data without using index structure. This method is faster to search using the short hashed key instead of the original value.

**Application of Hashing**:

* Password Verification
* Compiler Operation
* Rabin-Karp Algorithm
* Data Structures

Digital signature :-

The digital signature **confirms the integrity of the message**. This signature ensures that the information originated from the signer and was not altered, which proves the identity of the organization that created the digital signature. Any change made to the signed data invalidates the whole signature

**digital signature** is precisely an electronic form of signature used to authenticate any digital document and identity of the signer. It is important and in vogue because it is safer and secure than traditional pen-paper signatures. The electronic signature is complicated to falsify because it operates through mathematical algorithms. Due to its easy nature, encryption capabilities it can be adapted by different businesses. In the 21st century, there are several digital signature uses, important for restructuring and revamping any business model.

Digital signatures are available for a long time but the passing of The Electronic Signatures in Global and National Commerce Act.

The impact of digital signature is becoming clearer every day. Numerous organizations have started using it to smoothen the workflow while at the same time protecting the integrity of the important documents

**5.List and Explain different types of Malwares?**

Malware can be classified into 9 types they are:-

* 1. Spyware
  2. Backdoor
  3. Ransomware
  4. Scareware
  5. Rootkit
  6. Trojan horse
  7. Virus
  8. Adware
  9. Worms

1.Spyware:-

Spyware is **any software that installs itself on your computer and starts covertly monitoring your online behaviour without your knowledge or permission**. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties

2.Backdoor:-

A backdoor is **a malware type that negates normal authentication procedures to access a system**. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

3.Ransomware:-

Ransomware is **a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files**. A criminal group will then demand a ransom in exchange for decryption

4.Scareware:-

Scareware is **a type of malware attack that claims to have detected a virus or other issue on a device and directs the user to download or buy malicious software to resolve the problem**. Generally speaking, scareware is the gateway to a more intricate cyberattack and not an attack in and of itself.

5.Rootkit:-

 Rootkit malware is **a collection of software designed to give malicious actors control of a computer network or application**. Once activated, the malicious program sets up a backdoor exploit and may deliver additional malware, such as ransomware, bots, key loggers

6.Trojan horse:-

A Trojan Horse (Trojan) is **a type of malware that disguises itself as legitimate code or software**. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device

7.Virus:-

Malware is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed. **A virus is a specific type of malware that self-replicates by inserting its code into other programs**

8.Adware:-

Adware is **unwanted software designed to throw advertisements up on your screen, most often within a web browser**. Some security professionals view it as the forerunner of the modern-day PUP (potentially unwanted program).

9.Worms:-

**A computer worm is a subset of the Trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system**. Typically, a worm spreads across a network through your Internet or LAN (Local Area Network) connection.

**6.Illustrate the vulnerability in different layer in OSI model?**

OSI layer vulnerabilities:

**Physical destruction, obstruction, manipulation or malfunction of physical assets including loss of power, loss of environmental control, thef of data and hardware**. Physical damage or destruction of data and hardware

1.Physical destruction Vulnerability:-

Physical vulnerability describes **the ability of the built environment, including homes, roads, bridges, hospitals, schools, and government buildings, to withstand impacts**. Generally, physical vulnerability is represented as the monetary value of physical assets in the hazardous zone.

2.Obstraction vulnerability:-

The obstruction can be complete or partial. There are many causes. The most common are adhesions, hernias, cancers, and certain medicines

3. Assets vulnerability:-

A vulnerability is **an organisational flaw that can be exploited by a threat to destroy, damage or compromise an asset**. You are most likely to encounter a vulnerability in your software, due to their complexity and the frequency with which they are updated.

4. Physical vulnerability:-

Physical vulnerability describes **the ability of the built environment, including homes, roads, bridges, hospitals, schools, and government buildings, to withstand impacts**. Generally, physical vulnerability is represented as the monetary value of physical assets in the hazardous zone.

5.Environment vulnerability:-

It refers to both, the susceptibility to the negative socioeconomic impacts of environmental variability and the degree to which a community is capable of coping with, resisting, and recovering from the impacts of specific environmental events.

6. Data vulnerability:-

A vulnerability is a weakness or error in a system or device's code that, when exploited, can compromise the confidentiality, availability, and integrity of data stored in them through unauthorized access, elevation of privileges, or denial of service

**7.Explain Security Principles-CIA and AAA?**

CIA:-

A Simple but Widely Applicable security model is the CIA triad ; standing for Confidentiality, integrity and Availability ;three key principles which should guaranteed in any kind of secure system.

Confidentiality:-

Confidentiality is the Ability to hide information from those people unauthorised to view it .it is perhaps the most obvious aspect of the CIA triad when it comes to Security ; but corresponding ,it is also the one which is attacked most often cryptography and Encryption Methods Are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

Integrity:-

The ability to ensure that data is an accurate and unchanged representation of the original secure information one type of security attack is to intercept some important data and make changes it before sending it on to the intended receiver

Availability:-

It is important to ensure that the information concerned is readily accessible to the authorised viewer at all times .some type of security attack attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. for example by breaking the web site for a particular search engine a rival may become more popular.

2.AAA:-

AAA stands for authentication, authorization, and accounting. AAA is **a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for service. And it is an one of the principle**

### **Authentication:-**

Authentication involves a user providing information about who they are. Users present login credentials that affirm they are who they claim. As an identity and access management (IAM) tool, a AAA server compares a user’s credentials with its database of stored credentials by checking if the username, password, and other authentication tools align with that specific user.

The three types of authentication include something you know, like a password, something you have, like a Universal Serial Bus (USB) key; and something you are, such as your fingerprint or other biometrics.

### **Authorization:-**

Authorization follows authentication. During authorization, a user can be granted privileges to access certain areas of a network or system. The areas and sets of permissions granted a user are stored in a database along with the user’s identity. The user’s privileges can be changed by an administrator. Authorization is different from authentication in that authentication only checks a user’s identity, whereas authorization dictates what the user is allowed to do.

For example, a member of the IT team may not have the privileges necessary to change the access passwords for a company-wide virtual private network (VPN). However, the network administrator may choose to give the member access privileges, enabling them to alter the VPN passwords of individual users. In this manner, the team member will be authorized to access an area they were previously barred from.

### **Accounting:-**

Accounting keeps track of user activity while users are logged in to a network by tracking information such as how long they were logged in, the data they sent or received, their Internet Protocol (IP) address, the Uniform Resource Identifier (URI) they used, and the different services they accessed

Accounting may be used to analyse user trends, audit user activity, and provide more accurate billing. This can be done by leveraging the data collected during the user’s access. For example, if the system charges users by the hour, the time logs generated by the accounting system can report how long the user was logged in to the router and inside the system, and then charge them accordingly.

**8.What are the challenges in cyber security?**

**Top 5 cybersecurity challenges :-**

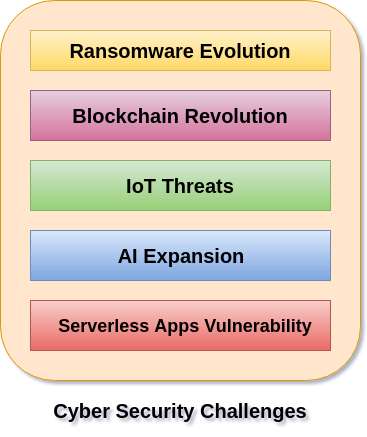
* Ransomware Evolution
* Block chain Revolution
* IOT Threats
* AI Expansion
* Server less App vulnerability

1.Ransomware Evolution:-

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cybersecurity, data professionals, IT, and executives.

Ransomware attacks are growing day by day in the areas of cybercrime. IT professionals and business leaders need to have a powerful recovery strategy against the malware attacks to protect their organization.

It involves proper planning to recover corporate and customers' data and application as well as reporting any breaches against the Notifiable Data Breaches scheme



## 2.Block chain Revolution:-

## Block chain technology is the most important invention in computing era. It is the first time in human history that we have a genuinely native digital medium for peer-to-peer value exchange.

## The block chain is a technology that enables cryptocurrencies like Bitcoin. The block chain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust.

## It is difficult to predict what block chain systems will offer in regards to cybersecurity. The professionals in cybersecurity can make some educated guesses regarding block chain.

## As the application and utility of block chain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches.

## 3.IoT Threats:-

## IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction

## The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks.

## When IoT things were designed, it is not considered in mind about the used in cybersecurity and for commercial purposes.

## So every organization needs to work with cybersecurity professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the risk.

## 4.AI Expansion:-

## AI short form is Artificial intelligence. According to John McCarthy, father of Artificial Intelligence defined AI: "The science and engineering of making intelligent machines, especially intelligent computer programs."

## It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include speech recognition, Learning, Planning, Problem-solving, etc.

## The key benefits with AI into our cybersecurity strategy has the ability to protect and defend an environment when the malicious attack begins, thus mitigating the impact.

## AI take immediate action against the malicious attacks at a moment when a threats impact a business.

## IT business leaders and cybersecurity strategy teams consider AI as a future protective control that will allow our business to stay ahead of the cybersecurity technology curve.

## 5.Server less Apps Vulnerability:-

## Server less architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc

## The server less apps invite the cyber attackers to spread threats on their system easily because the users access the application locally or off-server on their device.

## Therefore it is the user responsibility for the security precautions while using server less application.

## The server less apps do nothing to keep the attackers away from our data. The server less application doesn't help if an attacker gains access to our data through a vulnerability such as leaked credentials, a compromised insider or by any other means then server less.

## 9.write about different methods of infiltration?

## Point infiltration measurements are normally made by applying water at a specific site to a finite area and measuring the intake of the soil.

## There are four types of infiltration: -

## The ponded-water ring or cylinder type,

## The sprinkler type,

## The tension type,

## The furrow type.

## 10.Explain RSA algorithm .using RSA solve p=5, q=11, key=27, d=?

## Let we take massage = 3

## Let n=p\*q=55

## Let (n)=(p-1)(q-1)=(5-1)(11-1)

## =4\*10

## =40

## d=e-1 mod (n)

## d\*e= 1 mod 40

## 3\*27=1 mod 40

## 81 mod 40 = 1

## d=3

## ciper text

## c=me mod n

## =327 mod 55

## = 42

## Plain text

## P=cd mod n

## =423 mod 55

## =3

## 11.Elobarate Diffie –Hellman algorithm

## The Diffie–Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.

## UseofDiffieHellmanxAlgorithm:- Encryption: The Diffie Hellman key exchange algorithm can be used to encrypt; one of the first schemes to do is ElGamal encryption. One modern example of it is called Integrated Encryption Scheme, which provides security against chosen plain text and chosen clipboard attacks.

## 

## 12.Euler totient Function (256,100,165,16,72)

Φ (256)

Φ (n) = pn  - pn-1

=28  - 28-1

=256 -128

=128

Φ(n) 256(1-1/2)

=256\*1/2

=128

## 13.GCD of two numbers (256,145,160,70,5,11)

## 

## Gcd (70,160)=gcd (160,70)

## Gcd (160,70)=gcd (70,160 mod 70)

## =gcd(70,20)

## Gcd (70,20) =gcd (20,70 mod 20)

## =gcd(20,10)

## Gcd (10,10)=gcd (10,20 mod 10)

## =gcd(10,0)

## Gcd=10

## 14.Explain Wireless security issue in cellular network, wifi, LAN system RFID system?

Wireless security issues can affect different types of wireless systems such as cellular networks, Wi-Fi networks, LAN systems, and RFID systems. Here's a brief explanation of some of the security issues in each of these systems:

* Cellular networks: Cellular networks are susceptible to various security threats, including eavesdropping, man-in-the-middle attacks, unauthorized access, and denial-of-service (DoS) attacks. Mobile devices can also be compromised, leading to the theft of sensitive information.
* Wi-Fi networks: Wi-Fi networks are vulnerable to various security threats, including unauthorized access, man-in-the-middle attacks, and DoS attacks. Unsecured Wi-Fi networks can also be used to spread malware and launch attacks on other devices connected to the network.
* LAN systems: LAN systems are vulnerable to various security threats, including unauthorized access, man-in-the-middle attacks, and DoS attacks. Unsecured LAN systems can also be used to spread malware and launch attacks on other devices connected to the network.
* RFID systems: RFID systems are vulnerable to various security threats, including eavesdropping, unauthorized access, and cloning. Unsecured RFID systems can also be used to steal sensitive information, such as credit card numbers, personal identification numbers (PINs), and other sensitive information.

## 15.Explain the following Windows :a)Third Patch management b)Windows autopilot?

## Third patch management:-

## Third-party patching (patch management) is the process of installing patches to third-party applications, that are installed on your company's endpoints, to address bugs or vulnerabilities in the software. Third-party patching is critical for the security of your organization that prevents data breaches.

* Third-party patch management: Third-party patch management refers to the process of managing and updating software applications from non-Microsoft sources. This includes updating software applications such as web browsers, media players, and productivity tools. Third-party patch management is important for keeping systems secure and up-to-date, as many security vulnerabilities are often found in third-party software.

Windows autopilot:-

* Windows Autopilot is **a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use**. Windows Autopilot can be used to deploy Windows PCs or HoloLens 2 devices. For more information about deploying HoloLens 2 with Autopilot, see Windows Autopilot for HoloLens 2
* Windows Autopilot: Windows Autopilot is a service provided by Microsoft that allows for the deployment, reset, and repurposing of Windows 10 devices. Autopilot simplifies the device provisioning process, enabling IT administrators to quickly and easily set up new devices for use by their organizations. This includes personalizing the device, installing apps, and applying policies and settings. With Autopilot, IT administrators can also manage the device's life cycle, from initial deployment to end of life, ensuring that devices are always secure, up-to-date, and fully functional.

**16. Explain Linux Hardening.**

Linux hardening refers to the process of securing a Linux operating system and reducing its potential attack surface. This is achieved by implementing various security measures, such as updating and patching the system, configuring secure permissions and users, disabling unnecessary services, using firewalls and intrusion detection systems, and more. The goal of Linux hardening is to minimize the risk of unauthorized access, theft of data, or other security incidents by making the system less vulnerable to attacks.

**17.Explain SSH Hardening in linux?**

SSH (Secure Shell) hardening refers to the process of improving the security of an SSH server in aLinux system. This involves implementing various measures to reduce the risk of unauthorized access, theft of data, or other security incidents. Some common SSH hardening practices include:

* Updating and patching the SSH server software to the latest version
* Disabling root login through SSH
* Using strong authentication methods, such as key-based authentication instead of password authentication
* Configuring SSH to listen on a non-standard port, to reduce the risk of automated attacks
* Limiting the number of login attempts to prevent brute force attacks
* Disabling legacy protocols, such as Telnet, and using only secure protocols, such as SSH
* Using public key infrastructure (PKI) to secure SSH communications
* Enabling logging and auditing to monitor and track SSH activity.

By implementing these and other SSH hardening measures, organizations can significantly improve the security of their Linux systems and reduce the risk of attacks.

**18.Explain Linux enhancements and infrastructure**

Linux is an open-source operating system that has evolved over the years with many enhancements and improvements. Some of the notable enhancements in recent times include:

* Kernel updates: Regular updates to the Linux kernel provide new features, improved performance, and security fixes.
* User-space improvements: A variety of user-space tools and utilities have been developed and improved, such as package managers, text editors, and shells, providing a more user-friendly experience.
* Virtualization and containerization: Linux has seen widespread adoption as a host for virtual machines and containers, such as Docker and Kubernetes, making it easier to run multiple isolated applications on a single host.
* Cloud computing: Linux has become a popular choice for cloud computing infrastructure, due to its scalability, stability, and security.
* Internet of Things (IoT): Linux is also increasingly being used in IoT devices, providing a stable and secure platform for connecting devices to the internet.

In addition to these enhancements, Linux has a large and thriving infrastructure that includes a massive repository of software packages, a vibrant community of developers and users, and extensive documentation and support resources.

**OR**

**Explain SE Linux & App Armor**

SELinux (Security-Enhanced Linux) and AppArmor are two Linux security frameworks that provide additional security to the operating system by enforcing access controls and restrictions on applications and processes.

* SELinux: SELinux is a mandatory access control system that provides fine-grained control over the actions of processes and applications on the system. It operates by assigning a security context to each process, file, and network object, and using rules to define the actions that each process is allowed to perform. SELinux provides a higher level of security compared to traditional Linux discretionary access controls, as it enforces security policies even if an application or process is compromised.
* AppArmor: AppArmor is a Mandatory Access Control (MAC) system that provides a way to specify security policies for individual applications and processes. Like SELinux, AppArmor enforces these policies, even if an application is compromised, to prevent unauthorized access to system resources and data. Unlike SELinux, AppArmor policies are defined in a user-friendly profile format, making it easier for system administrators to implement and maintain security policies for individual applications.

**19.Explain Repositories in Linux**

A repository in Linux is a collection of software packages, metadata, and configuration files that are stored and organized in a central location. Repositories provide a convenient and organized way to distribute, install, and manage software packages in Linux.

The most common types of repositories in Linux are:

* Official Repositories: These are repositories that are provided and maintained by the Linux distribution. They contain packages that are officially supported by the distribution and are guaranteed to be stable and secure.
* Third-Party Repositories: These are repositories that are created and maintained by individuals or organizations that are not affiliated with the Linux distribution. They may contain packages that are not available in the official repositories, but there is a risk of instability or security issues with packages from these repositories.
* Personal Repositories: These are repositories that are created and maintained by individual users for their personal use. They may contain custom packages or local copies of packages from other repositories.

Repositories are usually managed using a package manager, such as APT (Advanced Package Tool) in Debian-based distributions, or YUM (Yellowdog Updater, Modified) in Red Hat-based distributions. These package managers use the repository metadata to determine the available packages, their dependencies, and the latest versions.

Using repositories, Linux administrators can easily install, update, and manage packages on their systems, making it easier to keep their systems up-to-date and secure.

**OR**

**Explain Package Management in linux**

Package management in Linux is the process of installing, updating, and removing software packages in a Linux system. It is an important aspect of Linux system administration that helps to ensure that systems are kept up-to-date and secure

There are several package management systems available in Linux, including:

* APT (Advanced Package Tool): A package manager used in Debian-based distributions, such as Ubuntu, Debian, and Mint. It uses a database of packages and metadata to resolve dependencies and perform installations, upgrades, and removals.
* YUM (Yellowdog Updater, Modified): A package manager used in Red Hat-based distributions, such as Fedora and CentOS. It uses a repository-based system to resolve dependencies and perform installations, upgrades, and removals.
* RPM (Red Hat Package Manager): A package manager used in Red Hat-based distributions, similar to YUM. It uses packages in the RPM format, and provides a low-level package management system for Red Hat-based distributions.
* DNF (Dandified YUM): A package manager used in Fedora, and a replacement for YUM. It is designed to be faster and more efficient, and includes features such as better dependency resolution and package management.
* Pacman: A package manager used in Arch Linux. It uses a simple, concise syntax to perform installations, upgrades, and removals, and includes features such as automatic dependency resolution.

In general, package management in Linux helps to ensure that systems are kept up-to-date with the latest software packages and security updates, and makes it easier to manage software installations, upgrades, and removals. Package management systems also provide a way to resolve dependencies between packages, ensuring that all required packages are installed and up-to-date.

**20.Illustrate linux operating system Vulnerability**

Like any other operating system, Linux is also vulnerable to security threats and vulnerabilities. Here are some common vulnerabilities in the Linux operating system:

* Unpatched software: Just like any other operating system, the Linux operating system relies on software to function, and it is vulnerable to exploits that target known vulnerabilities in the software. This can be mitigated by keeping all software up-to-date and patched, using a package manager to automate updates, and using security-focused Linux distributions that prioritize security updates.
* Malicious software: Linux is vulnerable to malware, just like any other operating system. This can be mitigated by using anti-virus software, avoiding downloading and installing software from untrusted sources, and being vigilant about security updates.
* Configuration errors: Incorrectly configured systems can be vulnerable to security threats. This can include issues like weak passwords, open network services, and misconfigured firewall rules. Regular system hardening and secure configuration practices can help to mitigate these risks.
* Network attacks: Linux systems that are connected to the internet are vulnerable to network-based attacks, such as denial-of-service (DoS) attacks, Man-in-the-Middle (MitM) attacks, and phishing scams. To mitigate these risks, it is important to use a firewall to restrict incoming and outgoing network traffic, keep all software up-to-date, and educate users about safe online practices.
* Privilege escalation: Linux systems can be vulnerable to privilege escalation attacks, where an attacker takes advantage of a vulnerability in the operating system or software to gain elevated privileges on the system. This can be mitigated by using secure configurations, applying security updates in a timely manner, and using mandatory access controls such as SELinux or AppArmor to restrict the actions of applications and processes.

In conclusion, Linux is a robust and secure operating system, but it is not immune to security threats and vulnerabilities. To minimize the risk of security incidents, it is important to keep all software up-to-date, use secure configurations, and practice safe online habits.

**21.Explain Network Security Concepts a). Firewall b). IDS c). IPS.**

• Firewall. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external network, such as the Internet.

The firewall checks each incoming and outgoing network packet and compares it against its set of security rules to determine whether to block or allow the packet to pass through to its intended destination. The main purpose of a firewall is to prevent unauthorized access to or from a private network while allowing authorized communications to pass through.

• IDS Intrusion Detection System (IDS) is a type of security software designed to automatically detect and alert administrators of unauthorized access, misuse, or malicious activities on a computer system or network. IDS operates by analyzing network traffic and comparing it against a set of predefined security rules or signatures. If the system detects a match between the incoming traffic and a known malicious pattern, it will generate an alert, allowing the administrator to take appropriate action to prevent further damage or compromise. There are two main types of IDS: network-based and host-based. Network-based IDS operates by monitoring network traffic and analyzing it for signs of intrusion, while host-based IDS operates by monitoring individual host systems for signs of intrusion.

• IPS An Intrusion Prevention System (IPS) is a type of network security system that monitors network traffic and actively blocks or stops malicious activity. Unlike an Intrusion Detection System (IDS), which simply alerts administrators of a security breach, an IPS takes proactive measures to prevent intrusions from occurring in the first place.

An IPS typically operates by analyzing network traffic in real-time and comparing it against a set of predefined security rules or signatures. If the system detects a potential threat, it will take immediate action to prevent it from causing harm to the network or its systems. This can involve blocking the offending traffic, resetting the connection, or even isolating the affected system from the network.

In computer science, IPS is considered a crucial component of an overall security strategy, as it provides an additional layer of protection against threats that traditional firewalls may not detect or be able to prevent.

**22. What is IAST? Explain its advantages over SAST and DAST**

IAST stands for International Alphabet of Sanskrit Transliteration, a standard transliteration system for writing Sanskrit words in the Latin alphabet

|  |  |
| --- | --- |
| **SAST** | **DAST** |
| **White box security testing**  The tester has access to the underlying framework, design, and implementation. The application is tested from the inside out. This type of testing represents the developer approach. | **Black box security testing**  The tester has no knowledge of the technologies or frameworks that the application is built on. The application is tested from the outside in. This type of testing represents the hacker approach. |
| **Requires source code**  SAST doesn’t require a deployed application. It analyzes the sources code or binary without executing the application. | **Requires a running application**  DAST doesn’t require source code or binaries. It analyzes by executing the application. |
| **Finds vulnerabilities earlier in the SDLC**  The scan can be executed as soon as code is deemed feature-complete. | **Finds vulnerabilities toward the end of the SDLC** Vulnerabilities can be discovered after the development cycle is complete. |
| **Less expensive to fix vulnerabilities**  Since vulnerabilities are found earlier in the SDLC, it’s easier and faster to remediate them. Findings can often be fixed before the code enters the QA cycle. | **More expensive to fix vulnerabilities**  Since vulnerabilities are found toward the end of the SDLC, remediation often gets pushed into the next cycle. Critical vulnerabilities may be fixed as an emergency release. |
| **Can’t discover run-time and environment-related issues**  Since the tool scans static code, it can’t discover run- time vulnerabilities. | **Can discover run-time and environment-related issues**  Since the tool uses dynamic analysis on an application, it is able to find run-time vulnerabilities. |
| **Typically supports all kinds of software** Examples include web applications, web services, and thick clients. | **Typically scans only apps like web applications and web services**  DAST is not useful for other types of software. |

# **23.Explain the Software Development Life Cycle.**

The Software Development Life Cycle (SDLC) is a systematic approach to software development that provides a framework for developing and maintaining software. It involves several stages, including:

* + Requirements gathering and analysis: This stage involves gathering and analyzing the requirements of the software, defining the scope of the project, and determining the feasibility of the project.
  + Design: This stage involves creating a detailed design of the software, including the architecture, user interface, and data structures.
  + Implementation or coding: This stage involves writing the code for the software, testing it, and fixing any bugs.
  + Testing: This stage involves verifying that the software meets the requirements and identifying any problems. This stage includes unit testing, integration testing, and system

testing.

* + Deployment: This stage involves installing the software in the production environment, making it available to the users.
  + Maintenance: This stage involves fixing any problems that arise after the software is deployed, making modifications to the software, and ensuring that it continues to meet the needs of the users.

# **24.Illustrate static code analysis vs dynamci code analysis.**

Static code analysis and dynamic code analysis are two methods used for evaluating the quality and security of software code.

Static code analysis involves analyzing the source code of a software application without executing it. It is performed by automated tools that analyze the code for potential security vulnerabilities, coding standards, and other software quality issues. The goal of static code analysis is to identify problems early in the development process, when they are easier and less expensive to fix.

Dynamic code analysis, on the other hand, involves executing the code and observing its behavior as it runs. This type of analysis is performed by tools that can monitor the code during runtime, identifying potential security vulnerabilities and other problems as they occur. The goal of dynamic code analysis is to identify problems that may not be detected by static code analysis, such as memory leaks and performance issues.

**25.Explain RASP and Web application firewall(WAP).**

RASP (**Runtime Application Self-Protection**) and WAF (**Web Application Firewall**) are two technologies used to protect web applications from cyber threats.

**RASP** is a security technology that integrates directly into an application's runtime environment, providing real-time protection against threats. RASP uses information from the runtime environment, such as data inputs and system interactions, to monitor and detect security threats. It can block malicious requests before they reach the application, reducing the risk of attack.

**WAF**, on the other hand, is a security technology that operates at the network layer, analyzing incoming and outgoing traffic to detect and block malicious traffic. WAFs use a set of rules to identify and block traffic that is potentially harmful, including attacks such as SQL injection and cross-site scripting (XSS).

**26.What is threat modeling? Explain different threat modeling methodologies.**

Threat modeling is the process of identifying, analyzing and prioritizing potential threats and vulnerabilities in a system, application, or organization, in order to improve its security.

There are several methodologies for threat modeling, including:

* STRIDE: This methodology categorizes threats into six categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of privilege.
* PASTA: This methodology stands for Process for Attack Simulation and Threat Analysis. It involves several phases including threat identification, risk assessment, and mitigation strategies.
* Trike: This methodology focuses on identifying attack scenarios and then creating defense strategies. It involves three main steps: Threat identification, Risk analysis, and Mitigation strategy.
* Trivial File Transfer Protocol (TFTP) Modeling: This methodology focuses on identifying threats in a network-based system, particularly in the areas of authentication and data transfer.
* VAST: This methodology stands for Visual, Agile, and Simple Threat modeling. It involves creating a visual representation of the system being analyzed, and then using agile techniques to identify potential threats.

**27.Explain different types of Cloud Models. Illustrate IaaS, SaaS and PaaS.**

There are three main types of cloud models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

**Infrastructure as a Service (IaaS):** IaaS provides access to a virtualized computing infrastructure, including servers, storage, and network resources. Customers can rent these resources on-demand, and can configure and manage their own virtual machines and operating systems. Examples of IaaS providers are Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

**Platform as a Service (PaaS):** PaaS provides a platform for customers to develop, run, and manage applications and services, without having to worry about the underlying infrastructure. PaaS includes everything that IaaS provides, plus a development environment, middleware, and application services. Examples of PaaS providers are Heroku, Google App Engine, and Microsoft Azure App Service.

**Software as a Service (SaaS):** SaaS provides access to applications over the internet, without the need for customers to install and run the applications on their own computers. SaaS applications are typically subscription-based and can be used from any device with an internet connection. Examples of SaaS providers are Salesforce, Microsoft Office 365, and Google G Suite.

**28. How Shared Responsibility Model is useful in Cloud Service. Explain**

The Shared Responsibility Model is a key concept in cloud computing that defines the roles and responsibilities of both the cloud service provider (CSP) and the customer when it comes to securing the data and infrastructure in the cloud.

Under this model, the CSP is responsible for providing a secure and scalable infrastructure, while the customer is responsible for securing their data and applications that run on that infrastructure. The benefit of this mo How Shared Responsibility Model is useful in Cloud Service. Explain

The Shared Responsibility Model is a key concept in cloud computing that defines the roles and responsibilities of both the cloud service provider (CSP) and the customer when it comes to securing the data and infrastructure in the cloud.

Under this model, the CSP is responsible for providing a secure and scalable infrastructure, while the customer is responsible for securing their data and applications that run on that infrastructure. The benefit of this model is that it allows organizations to take advantage of the benefits of cloud computing while ensuring that their data and systems are secure. This can include cost savings, increased agility, and the ability to quickly scale resources as needed.

By clearly defining the responsibilities of each party, the Shared Responsibility Model helps organizations better understand what they need to do to secure their cloud environment and makes it easier for them to work with their CSP to achieve their security goals.del is that it allows organizations to take advantage of the benefits of cloud computing while ensuring that their data and systems are secure. This can include cost savings, increased agility, and the ability to quickly scale resources as needed.

By clearly defining the responsibilities of each party, the Shared Responsibility Model helps organizations better understand what they need to do to secure their cloud environment and makes it easier for them to work with their CSP to achieve their security goals.

**29.Explain Identity Access management(IAM) benefits.**

Identity and Access Management (IAM) is a critical security control for organizations that use cloud services. The main benefits of IAM are:

* Centralized management: IAM provides a single, centralized platform for managing user identities and access to resources. This makes it easier for organizations to manage access to their cloud infrastructure, applications, and data.
* Fine-grained control: IAM enables organizations to set granular access policies that determine who can access what resources, and what actions they can perform. This allows organizations to strike a balance between providing users with the access they need to do their jobs, and protecting sensitive data and systems.
* Compliance: IAM can help organizations meet regulatory and compliance requirements by providing a comprehensive audit trail of who has accessed what resources and when.
* Scalability: IAM can be easily scaled to accommodate the growth of an organization, making it an ideal solution for organizations that are rapidly expanding.
* Reduced risk: By providing a centralized and automated approach to identity and access management, IAM helps organizations reduce the risk of unauthorized access to sensitive data and systems, which can lead to data breaches and other security incidents

**30.Explain IAM best practices in cloud**

Here are some best practices for using Identity and Access Management (IAM) in cloud computing:

* Least privilege: Grant the minimum necessary permissions to users, groups, and resources.
* Multi-factor authentication (MFA): Use MFA for privileged users to add an extra layer of security.
* Use roles instead of shared credentials: Assign roles to users, applications, or services instead of sharing credentials.
* Regular review of permissions: Regularly review and remove unused or excessive permissions.
* Use groups: Organize users into groups and assign permissions to groups instead of individual users.
* Enable logging: Enable logging to track and audit IAM activities.
* Implement a password policy: Establish a strong password policy and enforce it for all users.
* Secure access keys: Secure access keys used by applications and services, and rotate them regularly.
* Use AWS Organizations: Use AWS Organizations to manage multiple AWS accounts and enforce resource-level permissions.
* Encrypt sensitive data: Encrypt sensitive data at rest and in transit to protect it from unauthorized access.

**31. Explain Security principles in cloud ?**

* Data in transit protection
* Asset protection and resilience
* Separation between customers
* Governance framework
* operational security
* personnel security
* Secure development
* Supply chain security
* Secure user management
* Identity and Authentication
* External interface protection
* Secure service administration
* Audit information and alerting for customers
* Secure use of the service

**32. Explain top 10 OWASP issues in web application? Or Explain issues in web vulnerability?**

* SQL injection
* Cross site Scripting
* Broken Authentication and Session management
* Insecure Direct object Reference
* Cross site request forgery
* Security Misconfiguration
* Insecure Cryptographic storage
* Failure to restrict URL Access

**33. Explain top 10 OWASP issues in Mobile Application? Or Explain top 10 OWASP in mobile vulnerability?**

* Weak server side controls
* Insecure Data storage
* Insufficient Transport layer protection
* Unintended Data Leakage
* Poor Authorization and Authentication
* Broken cryptography
* Client side injection
* Security Decisions Via untrusted inputs
* Improper session handling
* Lack of binary protections

**34.Explain issues in cloud services? Or Explain cloud vulnerabilities? Or Explain cloud misconfiguration?**

* Privacy
* Compliance
* Security
* Sustainability
* Abuse
* Higher cost
* Recovery of lost data in contingency
* Unkeeping (management) of cloud
* Lack of resources/ Skilled expertise
* Pay-per-use Service charges

**35**. **Define Incident management. Explain the procedure followed during incident management and different states briefly.**

Incident management is a series of steps taken to identify, analyze, and resolve critical incidents which could lead to issues in an organization if not restored.

Incident management restores normal service operation while minimizing impact to business operations and maintaining quality.

**Procedure followed during incident management are:**

* Incident identification
* Incident categorization
* Incident prioritization
* Incident closure
* Incident response

**36. Explain Patch management that takes place during the software fixes.**

* Patch management is a process of identifying, testing, and installing software updates and patches to resolve vulnerabilities, bugs, and other issues in a computer system. It is an important aspect of software maintenance that helps keep the system secure, stable, and functioning optimally.
* During patch management, the following steps take place:
* **Identification:** System administrators identify the need for patches by monitoring software updates from vendors, security alerts, and other sources.
* **Testing:** Patches are tested in a controlled environment to ensure that they will not cause any harm to the system or its components.
* **Deployment**: Once the patches have been tested and deemed safe, they are deployed to the production systems, either automatically or manually.
* **Monitoring**: System administrators monitor the performance of the systems after the patches have been applied to ensure that they have resolved the issues they were intended to fix.

**37. Explain Vulnerability life cycle. Elaborate the types of vulnerabilities.**

* The vulnerability life cycle refers to the process of identifying, evaluating, and mitigating security vulnerabilities in a system. It usually involves the following stages:
* Discovery: A vulnerability is discovered either by security researchers, security teams, or through automated scanning tools.
* Assessment: The discovered vulnerability is evaluated to determine its severity, impact, and potential for exploitation.
* Notification: The vendor or responsible party is notified of the vulnerability so that they can take appropriate action to address it.
* Mitigation: The vendor releases a patch or update to fix the vulnerability, or the responsible party implements workarounds or other measures to reduce the risk of exploitation.
* Deployment: The patch or update is deployed to the affected systems, or the workarounds or other mitigation measures are implemented.
* Verification: The effectiveness of the patch or update is verified, and the risk of exploitation is assessed.

**Types of Vulnerabilities:**

* **Software vulnerabilities:** These are weaknesses in the code of software applications that can be exploited by attackers to compromise the security of a system.
* **Configuration vulnerabilities:** These are vulnerabilities that arise from incorrect or insecure configuration of systems and applications.
* **Design vulnerabilities**: These are vulnerabilities that are inherent in the design of a system or application and cannot be easily fixed through patches or updates.
* **Physical vulnerabilities:** These are vulnerabilities that arise from physical security issues, such as the theft of hardware or unauthorized access to data centers.
* **Social engineering vulnerabilities:** These are vulnerabilities that arise from the manipulation of users into disclosing sensitive information or performing actions that compromise the security of a system.

**38. Explain GRC in an company and its benefits**

* GRC stands for Governance, Risk Management, and Compliance. It refers to a set of processes and technologies used by organizations to manage and monitor compliance with legal and regulatory requirements, manage risks and ensure that the company is operating in an ethical and transparent manner.

**The benefits of a strong GRC program in a company include:**

* **Improved Risk Management:** By having a clear understanding of the risks facing the company and implementing strategies to manage those risks, companies can minimize potential harm and maximize opportunities.
* **Increased Compliance**: GRC helps ensure that the company is following all relevant laws, regulations, and ethical standards, reducing the risk of fines, legal action and reputational damage.
* **Enhanced Transparency**: A strong GRC program promotes transparency in the company's operations and decision-making processes, which can increase trust among stakeholders and enhance the company's reputation.
* **Efficient Use of Resources**: By streamlining processes and utilizing technology to automate GRC activities, companies can reduce the time and cost associated with managing risks and ensuring compliance.
* **Improved Decision Making**: By having a comprehensive understanding of the company's risks and compliance obligations, companies can make better-informed decisions that promote long-term success.

**39. Explain ERM and types of risk faced by enterprise?**

ERM stands for Enterprise Risk Management. It is a systematic and comprehensive approach to managing an organization's risks and uncertainties, which are inherent in achieving its objectives. It involves identifying, assessing, and prioritizing potential risks, and implementing processes and controls to manage them. The objective of ERM is to balance risk and reward, minimize the impact of adverse events, and ensure the continuation of the organization's operations.

**There are several types of risks faced by enterprises:**

* **Financial risks** - risks related to financial losses, such as market risk, credit risk, liquidity risk, and operational risk.
* **Strategic risks -** risks associated with an organization's decisions and actions, such as competition, mergers and acquisitions, and market entry.
* **Compliance risks** - risks related to regulatory and legal non-compliance, such as data protection, anti-corruption, and anti-money laundering regulations.
* **Reputation risks** - risks related to the damage or loss of an organization's reputation and brand, such as negative publicity, cyberattacks, and social media controversies.
* **Operational risks** - risks related to the efficient and effective functioning of an organization's operations, such as supply chain disruptions, technology failures, and natural disasters.
* **Human resources risks** - risks related to the management of an organization's human capital, such as workforce shortages, high employee turnover, and legal disputes.

**40. Explain DevOps and Security Challenges?**

* DevOps is a software development practice that emphasizes collaboration and communication between development and operations teams. The goal of DevOps is to improve the speed and reliability of software delivery, as well as to increase the efficiency and responsiveness of the overall development process.
* **Security challenges in DevOps include:**
* **Configuration management**: ensuring the consistency and security of configurations across multiple environments, from development to production.
* **Continuous Integration and Continuous Deployment (CI/CD):** securing the pipeline and ensuring that only authorized changes are deployed to production.
* **Infrastructure as Code (IaC):** managing the security of infrastructure components defined as code, such as cloud resources or containerized applications.
* **Container security**: securing the lifecycle of containers, from build to deployment and runtime.
* **Secrets management**: securely storing and managing sensitive information, such as passwords and access keys, in the DevOps environment.
* **Compliance:** ensuring that DevOps practices align with regulations and industry standards, such as those related to data privacy and security

**41.Elaborate Core Principles and Patterns of DevOps**

* Create a Collaborative Environment.
* Automate, Automate, Automate
* Monitor the Process Continuously
* Implement End-to-End Responsibility
* Foster Continuous Improvement
* Don’t Be Afraid to Fail. Learn From It
* It’s All About the Customer

**42.Explain CI/CD in DevOps**

**CI : -**

* CI stands forContinuous integration (CI)
* CI allows developers to write, update, or fix a feature, then commit a code to the central code repository reliably, multiple times a day.
* Each update triggers an automated build and testing sequence for a given project, ensuring that code changes that merge into the repository are reliable.

**CD : -**

* CD stands forcontinuous delivery/deployment (CD)
* **CD is the implementation of automating the entire software release process.**
* Once code has passed all of the tests, deployment becomes the last step in the process.
* In a DevOps pipeline, CD often is referred to as continuous delivery but can also mean continuous deployment.

**43.How IT services are managed using ITIL Process. Explain it.**

## 1: Service Strategy

Service strategy is the core stage of the ITIL service lifecycle. Without a solid IT strategy that is aligned with the organization’s business strategies, an IT service is unlikely to succeed.

## 2: Service Design

The Service Design stage in the ITIL Process is the planning and design phase of IT strategies. **Ideas are formed out of inspiration drawn from IT strategies, be it new services or updates on existing services.**

## 3: Service Transition

The Service Transition stage in the ITIL Process is the phase where designed new services or changed services are built, tested, implemented, verified and transferred into operations.

## 4: Service Operation

The Service Operation stage in the ITIL Process is the phase where designed services are put into a live environment and end customers start to use services of the organization. This is the make of break phase where consumers finally interact with the service.

## 5: Continual Service Improvement

The Continual Service Improvement (CSI) stage in the ITIL Process binds all other four service lifecycle stages together and aims to identify and analyze the improvement points in these stages and then implement the improvement plans to mitigate any points of pain in the processes.

**44.Explain how data is protected in cloud using Secrets Management**

* Use multi-factor authentication (MFA) with each account.
* Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
* Set up API and user activity logging with AWS CloudTrail.
* Use AWS encryption solutions, along with all default security controls within AWS services.
* Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
* If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint.

**45.Explain Android Mobile OS architecture vs iOS Mobile OS.**

| **Parameters of Comparison** | **Android** | **iOS** |
| --- | --- | --- |
| Owned by | Google LLC | Apple Inc. |
| Created by | Android Inc. | Apple Inc. |
| Mainly developed by | Google and Open Handset Alliance | Apple |
| Launched on | 23 September 2008 | 29 June 2007 |
| Used in | Mobiles, tablets, gaming consoles, smart TVs, etc. | iPhone, iPad, iPod Touch, iPod Nano, and Apple TV |
| Kernel used | Linux | XNU hybrid |
| Languages used (programming) | C, Java, C++, and others | Swift, Objective-C, C++, and others |
| Type of software | Open Source | Closed Source |
| Virtual assistant | Google Assistant | Siri |
| No. of languages available | 100+ | 40 |
|  |  |  |
|  |  |  |

**46.Explain SIEM?**

* SIEM Stands for security information and event management (SIEM)
* It  is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

At the most basic level, all SIEM solutions perform some level of data aggregation, consolidation and sorting functions in order to identify threats and adhere to data compliance requirements

**Benefits of SIEM**

* **Advanced real-time threat recognition**
* **Regulatory compliance auditing**
* **AI-driven automation**
* **Improved organizational efficiency**
* **Detecting Advanced and Unknown Threats**
* **Conducting Forensic Investigations**
* **Assessing and Reporting on Compliance**
* **Monitoring Users and Applications**

**47.Give two KRI examples each for the following domains:**

**Patch Management**

* Deploying of all security patches for all operating system or IT assets.
* Uploading of OS master or golden image.
* Definition of the priority of vulnerability remediation
* Verification of the success of a deployed patch or remediation solution.
* Definition of SLAs for detecting analyzing & patching.

**Anti-virus management**

* Application patch latency.
* Number of successful & unsuccessful logins
* No of virus blocked
* Number of SPAM emails blocked system usage time of day logins
* No of phishing attempts.

**Change Management**

* **Identify What Will Be Improved**
* **Present a Solid Business Case to Stakeholders**
* **Plan for the Change**
* **Provide Resources and Use Data for Evaluation**
* **Communication**
* **Monitor and Manage Resistance, Dependencies, and Budgeting Risks**
* **Celebrate Success**

**48.Design a sample cyber security dashboard for reporting to top management?**

* **Security Incident :-** This Section display the number of security incident that have occurred over a specific period of time such as the past month the data can be presented in a graph or chat format.
* **Vulnerability:** This section display the number of vulnerability that have been identified & are yet to be patched.
* **Patch management :-** This section display the percentage of system that have been patched with in specific of time.
* **Network traffic:-** This section display the total amount of network traffic including incoming & outgoing traffic over a specific period of time.
* **Security Compliance**:- This section display the percentage of system that are compliant with security policies & regulations.
* **Threat Intelligence**:- This section display the latest known threat intelligence such as new threats & vulnerability as well any relevant mitigation strategies.

**49.Explain docker and docker files.**

**DOCKER**

**Docker** is a set of [platform as a service](https://en.wikipedia.org/wiki/Platform_as_a_service) (PaaS) products that use [OS-level virtualization](https://en.wikipedia.org/wiki/OS-level_virtualization) to deliver software in packages called [*containers*](https://en.wikipedia.org/wiki/Container_(virtualization)).

* The service has both free and premium tiers.
* The software that hosts the containers is called **Docker Engine**.
* **Docker** is a tool that is used to automate the deployment of applications in **lightweight containers** so that applications can work efficiently in different environments.
* **Docker takes away repetitive, mundane configuration tasks and is used throughout the development lifecycle for fast, easy and portable application development – desktop and cloud.**
* **Docker’s comprehensive end to end platform includes UIs, CLIs, APIs and security that are engineered to work together across the entire application delivery lifecycle.**

**DOCKER FILES**

* Docker file is a simple text file that consists of instructions to build Docker images.
* A Docker Image is a read-only file with a bunch of instructions. When these instructions are executed, it creates a Docker container.
* Docker file consists of specific [commands](https://www.simplilearn.com/tutorials/docker-tutorial/docker-commands) that guide you on how to build a specific Docker image.

**50.Define Metrics. Explain type of Metrics. OR Explain Security Metrics from OWASP**

Metrics are measures of quantitative assessment commonly used for assessing, comparing, and tracking performance or production. Generally, a group of metrics will typically be used to build a dashboard that management or analysts review on a regular basis to maintain performance assessments, opinions, and business strategies.

**Types of Metrics**

1.Process Metrics

Process metrics are used to measure the characteristics of the process of software development. The example includes the efficiency of detection of fault etc. The characteristics of the methods, tools, and techniques used for software development can be measured using process metrics.

**2. Product Metrics**

The characteristics of the software product are measured using product metrics. Some of the important characteristics of the software are:

* Software size and complexity
* Software reliability and quality

Computation of these metrics is done for different stages of the software development lifecycle.

**3. Internal Metrics**

The properties which are of great importance to a software developer can be measured using the metrics called internal metrics. An example is a measure of Lines of code (LOC).

**4. External Metrics**

The properties which are of great importance to a user can be measured using the metrics called external metrics. An example is portability, reliability, usability, etc.

**5. Project Metrics**

The progress of the project is checked by the project manager using the metrics called project metrics. Various metrics such as time, cost, etc., are collected by using the data from the projects in the past, and they are used as an estimate for the new software.

**Security Metrics from OWASP**

OWASP Information Security Metrics Bank project aims at helping organizations quickly assess their cybersecurity capabilities with a pre-defined set of metrics developed within a framework that provides clear measurement process, criteria and objectives. This framework is maintained by the open-source community.