1.System Hardening: It’s a process of reducing the attacking surface in the system thereby making it more robust and secure.

**Types of System Hardening:**

**1. Server Hardening:**

1.It focus mainly on protecting the Ports, Data, Permissions and functions of Data servers.

2.Strong Passwords, locking accounts after several times of incorrect login, multi-factor authentication, Disabling ports.

**2.Software Application hardening:**

1.It focuses on the application deployed on the server

2.Antiviruses, Spywares, malware protecting applications, establishing the intrusion detection system.

**3.Operating System hardening:**

1.It focuses on protecting the system own operating system.

2.limiting the access to work with the OS within the personnels and Uninstalling the unwanted drivers.

**4.Database hardening:**

It focuses on 3 things,

1.Data present in the database.

2.Managing the level of access and permission to each user has.

3.Encrypting the data present in the database and removing the unnecessary functions.

Hardening can be achieved implementing the role-based-access policy and restricting admin and user privileges.

**5.Netwok hardening:**

1.It refers to protecting the channels used to communicate btw to ports, by establishing the **intrusion detection** system to detect the potential attacks in the system in advance.

2. Configuring the **firewalls** and **encrypting** the organizational network traffic is also good practice of hardening.

**Standards for System Hardening:**

All the system hardening standards layout the rules on,

1.Patching

2.Updates on the OS

3.Data Encryption

4.Access control

5.System backup

6.Auditing and Monitoring.

**Common Org. that maintains the guidelines for the System Hardening:**

1.National Institute of Standards and Technology (NIST)

2.Computer Information Security (CIS) benchmark

3.Microsoft

**Why Standards are required:**

Standards make sure to identify the attacking surface before released into the market and ensures us that the system cannot exploited easily to get the access.

**How to perform system hardening:**

System hardening can be performed by following the guidelines mentioned by the orgs. like NIST, CIS etc.

**Lynis** is a tool for hardening your system in Linux.

**Approaches to implement system hardening:**

**1.Network Segmentation:**

Dividing the network into smaller segments that can be easily managed and monitored.

**2.Access Control:**

Implementing measures to control who has access to which parts of a system and what actions they can take.

**3.Intrusion prevention:**

Implementing security measures to detect and prevent unauthorised access or activity on a system is known as intrusion prevention.

**4.Encryption:**The process of encrypting data to prevent unauthorized individuals from accessing it.

**Importance of system hardening:**

1.Identifies the system misconfigurations.

2.Removes the unwanted programs.

**Benefits of system hardening:**

1.Secure System

2.Performance Increase

3.Auditing and Compliance streamlines

**Testing the effectiveness of the system hardening mechanism:**

It can be done by audit-based or review-based.

It depends on the type of the application and sensitivity of the data.

**Data Obfuscation:**

Data Obfuscation refers to masking the data to make data and source non-understandable to humans.

This technique is mainly used to protect data.

Testing the effectiveness of Data Obfuscation:

1.Version of Keys should be maintained properly to decode the Obfuscation data.

**Data Obfuscation techniques:**

**1.Masking:** It’s a way of creating different versions of the data, with similar structure, by changing the data, without changing the data types.

**2.Encryption:**  Encryption is very secure that is make the data understandable for the users without decrypting it.

Cryptographic methods are used to encrypting the data.

**3.Tokenization:**

Tokenization is replacing the data with the meaningless values.

Ex: Toke data can be used in production envt. Where third party companies will user the transaction details.

**Malware scanning:**

It’s a security testing technique used to identify the presence of a malware in the **application, computer system** or **network.**

“Eicar” is a tool used to identify the effectiveness of **anti-malware** without developing the real malicious piece of code.

Different approaches to identify the male:

**1.Signature-based detection:**

This method compares the file or software under test with known malware signatures. If a match is found, the file is identified as malicious.

**2.Behaviour-based detection:**

This involves monitoring the behaviour of the file or software while it is running.

**3.Sandboxing:**

A file or software runs in an isolated environment called a sandbox.

**4.Heuristic analysis:** This technique involves analysing the file or software code to identify the suspicious behaviour.

**Intrusion Detection:**

Intrusion detection system analyses the network traffic for malicious activity and send an alert immediately.

Each illegal activity is recorded either SIEM system or notified to an administrator.

**How does it works:**

The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.

If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.

The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

**Classification of Intrusion Detection System:**

**1.Network Intrusion Detection System (NIDS):**

1.It was set up on the planned point of the network and observes the traffic passing through the subnet and compares this with the predefined set of rules and then informs to the administrator if found anything is abnormal.

**2.Host Intrusion Detection System (HIDS):**

1.HIDS runs on the individual host and observes the each incoming and out going

Packets and from each individual devices and inform to Admin, if found anything abnormal.

2.It takes the snapshot of existing system and compares it with the previous system.

3.If any analytical files are edited then the alert will be sent.

4.Mission-critical-system is the example of HIDS, which are not expected to change their layout.

**3.Protocol-based Intrusion detection system (PIDS):**

1.A system or agent resides on the inside the frontend of the server, controlling and interpreting the protocol between the device and server.

2.Securing the webserver by monitoring the https protocols.

**4.Application protocol-based intrusion detection system:**

**5.Hybrid intrusion detection system:**

1. Prelude is an example of HIDS.

**Benefits of Intrusion Detection System:**

1.Detects malicious activity.

2.Improves network performance

3.Compilance requirements

4.Provides Insights.

**Detection Methods of IDS System:**

**1.Signature-based method:**

**2.Analomy-based method:**

**Authentication and Authorization:**

Authentication is process of identifying the user.

Authorization is process of identifying whether the user has the necessary permissions to access the resource.

Authentication works on ID token.

Authorization works on Access token.

**Authentication techniques:**

1.Password-based authentication system.

2. Password-less authentication system.

3.Two-factor/multi-factor authentication

4.Single-sign-on

5.Socical Authentication.

**Authorization techniques:**

1.Role-based access token.

2.JSON web token (JWT) authentication.

3.SAML authorization

4.OAuth 2.0 authorization.

**How Vulnerabilities arise in Authentication:**

1. Weak Authentication system that is not able to sustain brute-force attack.
2. **Broken Authentication**: Occurs due to Logic Flaws and Poor coding.

**Impact of Vulnerabilities in Authentication:**

1.Loss of sensitive data, based on the compromised account.

**Vulnerabilities in Authentication mechanism:**

1.Vulnerability in Password-based authentication system.

2.Vulnerability in multi-factor-authentication.

3.Vulnerability in other authentication mechanism.

**Encryption:**

Encryption is process of encoding the data (plain text) into cypher text, using cryptographic algorithm and secrets.

Only the authorised person can access the data using the decryption mechanism.

**Symmetric Encryption:**

This method uses a same key for both cipher and decipher the information.

Symmetric encryption algorithms include AES-128, AES-192, and AES-256.

symmetric encryption is the preferred method for transmitting data in bulk.

**Asymmetric Encryption: (**Public Key Encryption**)**

This method uses a different key but related keys to encrypt and decrypt the data.

**Data Encryption standards:**

Similar to the symmetric encryption, but uses AES algorithm, which is more secure.

**Triple Data Encryption standards (3DES):**

As the single AES algorithm is become a weaker to brute force attacks, Triple DES runs the AES 3 times to with 3 different keys.

**End to End Encryption (E2EE):**

It ensures only the two users communicating with one another are able to read the message.

It most **secure** way to communicate privately and securely on the online, even the intermediatory such as service provider are also not able decrypt the message.