CYBERSECURITY

*This note may contain some extra content relevant to Cybersecurity. follow the syllabus properly

UNIT 1

Hacking Vocabulary

- **Hack value** – Perceived value or worth of a target as seen by the attacker.
- **Vulnerability** – A system flaw, weakness on the system (on design, implementation etc).
- **Threat** – Exploits a vulnerability.
- **Exploit** – Exploits are a way of gaining access to a system through a security flaw and taking advantage of the flaw for their benefit.
- **Payload** – Component of an attack; is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** – Attack that occurs before a vendor knows or is able to patch a flaw.
- **Daisy Chaining / Pivotting** – It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.
- **Doxxing** – Publishing PII about an individual usually with a malicious intent.
- **Malware** – Think of it as digital germs that can make your computer sick.
- **Virus** – It is a type of malware that spreads from computer to computer, like a coldor infection.
- **Phishing** – This is the process where someone tries to trick you into giving awayyour personal information, like your password.
- **Hacking** – This is when someone tries to break into your computer or phone withoutpermission.
- **Firewall** – Like a guard at a door, it stops unwanted visitors from entering yourdigital world.
- **Encryption** – It's like putting a secret code on your information so only you canread it.
- **Antivirus** – This is like medicine for your computer, helping to fight off digital germs.

- **Identity theft** – When someone steals your personal information and pretends tobe you, it is known as Identity theft.
- **Data breach** – When someone gets access to your private information without youknowing, it is called Data breach.
- **Spam** – Annoying emails that you didn't ask for, which appear continuously in yourfeed, are called Spam.
- **Botnet** – A group of computers controlled by a bad person to do harmful things isknown as a Botnet.
- **Ransomware** – This is like digital kidnapping for your computer, holding it hostageuntil you pay money.
- **VPN** – This is a secret way to hide your online activity and keep your informationsafe.
- **Two-factor authentication** – This enables an extra layer of protection that asks formore than just a password.
- **Access control** – It is the decision of who can see or use something in your control.
- **Authentication** – It is a way of proving who you are in case of a verificationrequirement.

Types of Cyber Security

The various categories of cyber security are explained as follows –

Network Security

This area focuses on the deployment of both hardware and software solutions to protect acomputer network from unauthorized access. Such measures are important fororganizations to defend their assets against potential threats.

Application Security

This area includes the protection of software applications and devices from various threats.Regular updates to applications are important to ensure their defence against frequentattacks.

Information Security

This involves creation of strong and secure data storage protocols to ensure the security ofinformation, both while stored and during transmission.

Identity Security

This area includes the processes that determine the access levels granted to individualswithin an organization.

Mobile Security

This focuses on the protection of data stored on mobile devices, including smartphones,laptops, tablets, and similar gadgets, from a range of malicious threats.

Cloud Security

This domain is dedicated to safeguarding information stored within digital or cloudinfrastructures, utilizing various cloud service providers such as AWS, Azure, and Google.

Role of Cybersecurity in Business

Cybersecurity is integral to all businesses and organizations, whether it's a small startup or a large multinational corporation. It plays a crucial role in the financial operations of any business. The following points briefly discuss the role of cybersecurity in business:

1. **Secure Transactions**
   Cyberattacks can steal money directly or indirectly, damaging the reputation of an organization, which can lead to loss of customers and revenue.
2. **Customer Trust**
   If someone steals your customers' information, it erodes trust, resulting in financial troubles for your business.
3. **Safety of Ideas**
   Business ideas, plans, and sensitive information are critical assets. Cybersecurity ensures they remain confidential and protected from external threats.

4. **Avoiding Downtime**
   Cyberattacks can disrupt business operations, leading to loss of time and money. Effective cybersecurity measures help maintain smooth operations.
5. **Legal Requirements**
   Many laws and regulations require protective measures for customer data. Cybersecurity helps businesses comply with these legal obligations.

Basics of Cyber Technology

The rise of cyber technology and the invention of the Internet are significant milestones in the modern era of technology. With these advancements, there has also been an increase in cybercrimes and attacks. Before delving deeper into these subjects, it is essential to understand the foundational concepts that form the basis of Cyber Technology. These include topics such as networking, the OSI Model, the Internet, networking protocols, and other related concepts.

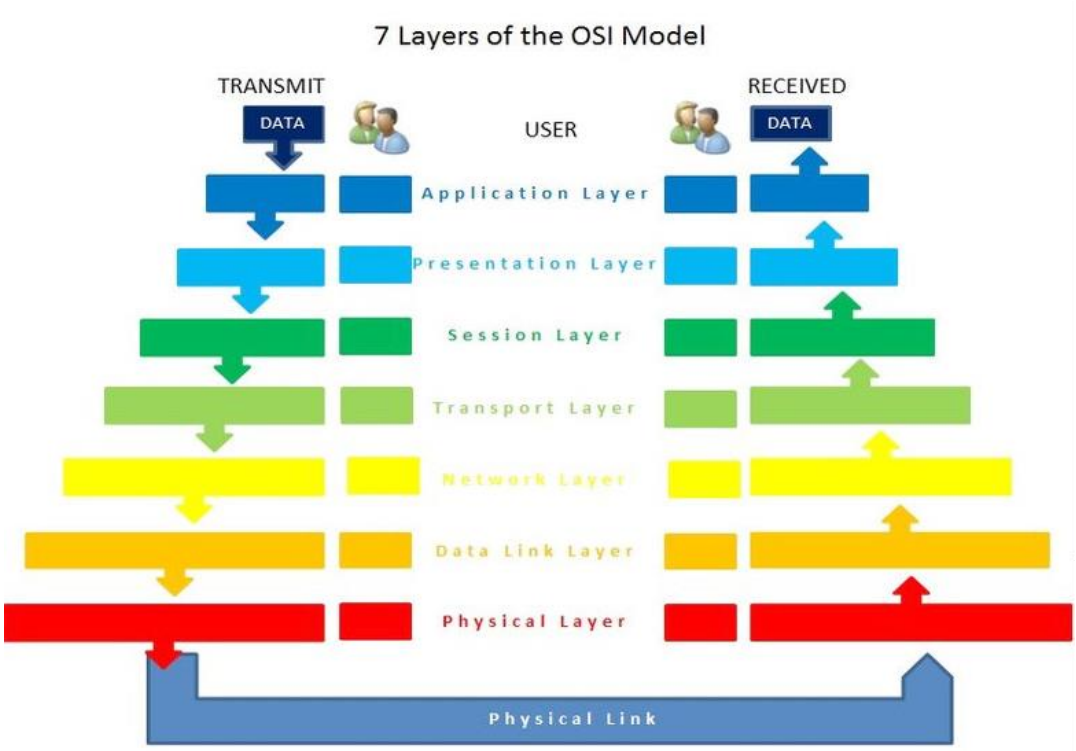
The OSI Model in Networks

Think of the Internet as a massive building, and the OSI model is like the blueprint of this building, divided into seven layers, each responsible for specific tasks. Let's explore these layers from the bottom up:

1. **Physical Layer**
2. **Data Link Layer**
3. **Network Layer**
4. **Transport Layer**
5. **Session Layer**
6. **Presentation Layer**

7. Application Layer

Each layer depends on the one below it, working together to create a smooth and efficient network.



Internet and the World Wide Web

Imagine the Internet as a global nervous system connecting billions of devices. It is a vast network of networks, enabling communication between devices ranging from smartphones to complex machinery. This network relies on sophisticated protocols to route information efficiently. While you can perform activities like sending emails, transferring files, or playing online games without the World Wide Web, the Internet is the fundamental platform that makes these possible.

Built on top of the Internet, the World Wide Web is the user-friendly interface we interact with daily. Think of it as a digital library with interconnected pages linked by hyperlinks. This interconnectivity, often referred to as the "web," allows you to seamlessly navigate from one piece of

information to another. Essentially, the web is a way to access and share information over the Internet.

Internet Protocols: TCP and UDP

TCP/IP functions like a postal service for the Internet, governing how data is transmitted between devices. At the transport level, there are two primary methods for sending data:

1. **TCP (Transmission Control Protocol): The Reliable Service**
   TCP is akin to certified mail, ensuring that your data arrives safely and in the correct order.
2. **UDP (User Datagram Protocol): The Quick Service**
   UDP is like sending a postcard—it's fast but less reliable. It doesn't guarantee that your data will arrive or that it will arrive in the correct order.

Encryption

Encryption is the process of securing data so that only authorised parties can access it. Different encryption techniques include:

1. **Hash Functions**
   Hash functions are like creating a unique fingerprint for your data. Even a small change in the data results in a completely different fingerprint. They are used to verify if a file has been altered and are also employed to store passwords securely.
2. **Digital Signatures**
   Digital signatures are like electronic seals on data, verifying that a message genuinely came from a trusted source and hasn't been altered during transmission. It is similar to signing a physical document.
3. **Symmetric Encryption**
   Symmetric encryption is like using a single key to lock and unlock a

box. You share the same key with whoever needs to access the information.

4. **Asymmetric Encryption**
   Asymmetric encryption involves two keys: a public key to encrypt the data and a private key to decrypt it. The public key can be shared widely, while only you hold the private key.
5. **Hybrid Encryption**
   Hybrid encryption combines both methods. It uses a fast, symmetric key to encrypt the data but employs asymmetric encryption to securely share that symmetric key.

Cybersecurity Aims and Goals

Cybersecurity focuses on the protection and safeguarding of networks, along with the associated data and information. It has evolved from traditional physical security measures to advanced software solutions like antivirus and anti-phishing platforms. In this chapter, we will delve into the main objectives and principles of cybersecurity, providing specific examples to illustrate them. Let's start with the aims and objectives of cybersecurity.

Aims and Objectives of Cybersecurity

Cybersecurity was developed to curb the increasing instances of cybercrimes and online harassment. Some of the main objectives and aims delivered through cybersecurity practices include:

1. **Data Protection**
   Cybersecurity ensures the protection of sensitive data, preventing it from being stolen, altered, or accessed illegally.
2. **Functioning of Systems**
   It enables computers and networks to run smoothly without interruptions, maintaining overall system performance and stability.

3. **Identity Verification**
   Cybersecurity helps in verifying that users and devices are who they claim to be, ensuring authenticity.
4. **Access Control**
   The concept of cybersecurity ensures that only authorised individuals have access to the information they need for their tasks, maintaining strict access controls.
5. **Event Monitoring**
   It facilitates the tracking and recording of all activities on computers and networks, which helps in identifying problems or tracing any malicious activity.
6. **Risk Management**
   Cybersecurity assists in identifying potential risks, assessing their likelihood, and developing strategies to mitigate them as quickly as possible.
7. **Compliance with Rules and Regulations**
   Cybersecurity practices require adherence to laws and industry standards to protect data and ensure compliance.
8. **Disaster Recovery**
   Cybersecurity principles help in creating recovery plans to address issues arising from cyberattacks or natural disasters, ensuring business continuity.
9. **Awareness Generation**
   Guidelines and best practices help employees understand how to safeguard themselves and the organisation against cyber threats.
10. **Quick Response**
    Cybersecurity principles help in devising rapid response strategies to effectively handle cyberattacks and resolve issues promptly.

11. **Maintaining Organisational Reputation**
    By reducing or preventing cyberattacks, cybersecurity measures help maintain the trust of customers and partners, thereby protecting the reputation of the organisation.

Cyber Attacks

Cyber attacks refer to malicious attempts to damage, disrupt, or gain unauthorized access to computer systems, networks, or devices. These attacks can cause financial loss, data breaches, and damage to an organization's reputation. Understanding the types, methods, and prevention strategies of cyber attacks is essential for maintaining a secure digital environment.

Types of Cyber Attacks

1. **Malware Attacks**
   Malware, or malicious software, is designed to infiltrate, damage, or disable computers and networks. Common types of malware include viruses, worms, Trojans, ransomware, and spyware. These programs can steal data, disrupt operations, or even take control of systems.
2. **Phishing Attacks**
   Phishing involves tricking users into revealing sensitive information, such as passwords or credit card details, by pretending to be a trustworthy entity. Phishing attacks are usually carried out through emails, messages, or fake websites that look legitimate.
3. **Denial-of-Service (DoS) Attacks**
   A DoS attack aims to overwhelm a server, network, or website with excessive traffic, causing it to crash or become unavailable. When multiple systems are used to carry out this attack, it is called a Distributed Denial-of-Service (DDoS) attack.
4. **Man-in-the-Middle (MitM) Attacks**
   In a MitM attack, the attacker intercepts communication between two parties, eavesdropping on the exchange or altering the

information being transmitted. This can happen on unsecured Wi-Fi networks or during online transactions.

5. **SQL Injection Attacks**
   SQL injection is a technique where attackers insert malicious code into a database query via a web application's input field. This allows them to gain unauthorized access to the database, steal information, or manipulate data.
6. **Ransomware Attacks**
   Ransomware is a type of malware that encrypts the victim's data, rendering it inaccessible until a ransom is paid. It can severely disrupt business operations, and even after the ransom is paid, there is no guarantee that the data will be restored.
7. **Zero-Day Exploits**
   A zero-day attack occurs when cybercriminals exploit a software vulnerability that is unknown to the vendor. Since the vendor is unaware of the flaw, no patch exists, making it a significant security risk until the vulnerability is addressed.
8. **Brute Force Attacks**
   Brute force attacks involve using automated tools to guess passwords by trying numerous combinations until the correct one is found. These attacks target weak or easily guessable passwords.

Common Methods Used in Cyber Attacks

1. **Social Engineering**
   Attackers manipulate individuals into revealing confidential information by exploiting their trust or fear. Social engineering techniques include phishing, pretexting, baiting, and tailgating.
2. **Exploiting Software Vulnerabilities**
   Attackers often target unpatched or outdated software that has

known vulnerabilities. They use these weaknesses to gain unauthorized access or cause damage.

3. **Malicious Links and Attachments**
   Cybercriminals may use emails, messages, or websites to share links or attachments containing malware. Clicking on these links or opening attachments can lead to system compromise.

Impact of Cyber Attacks

1. **Data Breaches**
   Cyber attacks can lead to data breaches, exposing sensitive information such as personal details, financial data, or intellectual property. This can cause significant financial loss and legal consequences.
2. **Financial Loss**
   Businesses may face direct financial loss from theft or extortion, along with indirect costs like recovery expenses, legal fees, and loss of customer trust.
3. **Reputation Damage**
   Companies suffering from cyber attacks may lose customers' trust, which can affect their reputation and market position.
4. **Operational Disruption**
   Attacks like DDoS or ransomware can disrupt business operations, leading to downtime and loss of productivity.

Preventive Measures Against Cyber Attacks

1. **Regular Software Updates**
   Keeping software, operating systems, and applications up to date ensures that known vulnerabilities are patched, reducing the risk of attacks.

2. **Strong Password Policies**
   Enforcing strong, unique passwords and enabling multi-factor authentication (MFA) helps in protecting accounts from unauthorized access.
3. **Data Encryption**
   Encrypting sensitive data ensures that even if it is intercepted, it cannot be easily read or misused.
4. **Network Security**
   Implementing firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) can help in monitoring and protecting networks from unauthorized access.
5. **Regular Backups**
   Regularly backing up data ensures that, in case of an attack, you can restore your systems without paying a ransom or losing essential information.
6. **User Education and Awareness**
   Educating employees about cybersecurity risks, phishing, and safe online practices can significantly reduce the likelihood of successful cyber attacks.

Vulnerability Assessment and Its Features

A vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities within a system. It involves scanning networks, software, and systems to find security weaknesses. Features include:

1. **Identification of Potential Vulnerabilities**
2. **Prioritization Based on Severity**
3. **Reporting and Recommendations for Fixes**

Concept and Types of Scanning Methodology

Scanning involves exploring a network to detect devices, open ports, and vulnerabilities. Common types include:

1. **Network Scanning**
   Identifying active devices and their IP addresses within a network.
2. **Port Scanning**
   Checking which ports are open and what services are running on them.
3. **Vulnerability Scanning**
   Automated tools to identify known vulnerabilities in systems and software.

Penetration Tests

Penetration testing, or "pen testing," involves simulating a cyber attack to find security weaknesses before actual attackers can exploit them. Penetration tests may include:

1. **External Testing**
   Testing the security of external systems like websites, servers, and firewalls.
2. **Internal Testing**
   Assessing security from within the network to see how much damage an internal attacker could cause.
3. **Blind Testing**
   The tester has limited information, simulating a real-world attack scenario.
4. **Double-Blind Testing**
   Neither the tester nor the organization's IT team is aware of when the attack will take place, testing both security and response protocols.

Network Security Threats and Countermeasures

1. **Common Network Security Threats**
    - **Malware**: Viruses, worms, Trojans that disrupt network systems.
      Countermeasure: Use anti-malware software and regular system updates.
    - **Phishing**: Trick users into revealing sensitive information.
      Countermeasure: Educate users on recognizing phishing attempts and use email filters.
    - **DDoS (Distributed Denial of Service)**: Overloading network resources to cause downtime.
      Countermeasure: Implement DDoS protection services and traffic monitoring.
    - **Man-in-the-Middle (MitM) Attacks**: Intercepting communication between two parties.
      Countermeasure: Use encryption (SSL/TLS) and VPNs to secure data transfer.
    - **SQL Injection**: Exploiting vulnerabilities in web applications to access databases.
      Countermeasure: Input validation and secure coding practices.

Network Security Devices

1. **Firewalls**: Control incoming and outgoing network traffic based on predetermined security rules.
2. **Intrusion Detection Systems (IDS)**: Monitor network traffic for suspicious activity.
3. **Intrusion Prevention Systems (IPS)**: Actively block detected threats.

4. **Virtual Private Networks (VPNs)**: Secure connections between devices over the internet.
5. **Proxy Servers**: Intermediate servers that filter requests and hide user IP addresses.

Types of Network Securities

1. **Physical Security**: Protects the physical components of the network (servers, cables).
2. **Technical Security**: Safeguards data on the network with encryption, firewalls, and anti-malware tools.
3. **Administrative Security**: Policies and procedures to control access to the network.

Network Access Control (NAC)

1. **Definition**: Mechanism to enforce security policies by managing which devices can connect to the network.
2. **Types of NAC**:
    - **Pre-admission NAC**: Validates devices before granting access.
    - **Post-admission NAC**: Continuously monitors devices while they are connected.

Characteristics of Network Access Control

- **Authentication**: Verifies the identity of devices and users.
- **Authorization**: Determines what resources users can access.
- **Accountability**: Tracks user activity and network access.

Application Security

1. **Definition**: Measures taken to secure applications from external and internal threats.
2. **Application Security Tools**:
    - **Static Application Security Testing (SAST)**: Scans source code for vulnerabilities.
    - **Dynamic Application Security Testing (DAST)**: Analyzes applications during runtime.
    - **Web Application Firewalls (WAFs)**: Protect web applications from attacks like SQL injection and XSS.

Firewalls and Its Types

1. **Packet-Filtering Firewalls**: Inspect packets and allow or block them based on rules.
2. **Stateful Inspection Firewalls**: Track active connections and make decisions based on the state.
3. **Proxy Firewalls**: Act as intermediaries between users and servers.
4. **Next-Generation Firewalls (NGFWs)**: Combine traditional firewall features with advanced security.

Virtual Private Network (VPN)

1. **Definition**: Creates a secure and encrypted connection over a less secure network.
2. **Benefits**: Protects data privacy, hides IP address, and allows secure remote access.

Tunneling Protocol and Types

- **PPTP (Point-to-Point Tunneling Protocol)**: Simple, but less secure.

- **L2TP (Layer 2 Tunneling Protocol)**: More secure, often paired with IPsec.
- **OpenVPN**: Highly secure and widely used.

IDS vs. IPS

1. **Intrusion Detection System (IDS)**: Detects and alerts on suspicious activities.
2. **Intrusion Prevention System (IPS)**: Detects, alerts, and actively blocks suspicious activities.
3. **Types of IDS/IPS**:
    - **Network-Based IDS/IPS (NIDS/NIPS)**: Monitors the entire network.
    - **Host-Based IDS/IPS (HIDS/HIPS)**: Monitors specific devices or hosts.

Introduction to Web Application Vulnerabilities

1. **Common Web Vulnerabilities**:
    - **Cross-Site Scripting (XSS)**
    - **SQL Injection**
    - **Cross-Site Request Forgery (CSRF)**
    - **Insecure Direct Object References (IDOR)**

Basic Practices of Web Application Security

1. **Use Strong Authentication**
2. **Regularly Update and Patch Systems**
3. **Implement HTTPS**

4. Input Validation to Prevent SQL Injection

Common Cyberattacks on Web Applications

- Cross-Site Scripting (XSS)
- SQL Injection
- DDoS Attacks
- Session Hijacking

Mobile Application Vulnerabilities

1. Insecure Data Storage
2. Weak Server-Side Controls
3. Unsecure Communication

Mobile Security Threats

- Malware
- Phishing
- Unauthorized Access

Mobile Application Security

- Use Encryption
- Implement Secure Authentication
- Regular Security Updates

Fundamentals of Mobile Device Management (MDM)

1. Definition: MDM involves managing, monitoring, and securing mobile devices in an organization.
2. Key Features:
    - Remote Wipe: Erase data if the device is lost.

- **Device Encryption**: Secure data storage.
- **App Management**: Control what applications can be installed.

Overview of Mobile Device Management

- **Centralized Management**
- **Data Security**
- **Compliance Enforcement**

Cloud Computing Threats and Solutions

1. **Threats**:
   - **Data Breaches**
   - **Account Hijacking**
   - **Denial of Service (DoS)**
2. **Solutions**:
   - **Data Encryption**
   - **Access Controls**
   - **Regular Security Audits**

1) What is Cyber Security, and why is it important in today's digital age?

Definition: Cyber security refers to the practices and technologies designed to protect computers, networks, and data from unauthorized access, attacks, or damage.

Importance:

- Data Protection: It safeguards sensitive information like financial details, personal data, and intellectual property.

- Prevention of Cyber Attacks: Helps prevent attacks like malware, phishing, and ransomware.
- Ensures Business Continuity: Protects businesses from disruptions caused by cyber threats, maintaining operational efficiency.
- Legal Compliance: Many organizations are required by law to implement robust security measures to protect customer data.

Reference:
https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html

2) What are the key principles of information security?

- Confidentiality: Ensures that information is only accessible to those who are authorized to see it.
- Integrity: Maintains the accuracy and completeness of data throughout its lifecycle.
- Availability: Ensures that authorized users have timely and reliable access to information when needed.

Reference Link: https://www.iso.org/standard/54534.html

3) CIA Triad – The Three Pillars of Information Security Architecture ?

Confidentiality:

- Protects data from unauthorized access and ensures privacy.
- Implemented using encryption, access controls, and authentication mechanisms.

Integrity:

- Ensures that data is accurate and has not been tampered with or altered by unauthorized users.
- Maintained through checksums, hashing algorithms, and digital signatures.

Availability:

- Ensures that data and systems are accessible to authorized users whenever needed.
- Achieved using redundancy, regular maintenance, and robust backup solutions.

Reference Link: https://www.nist.gov/cyberframework/online-learning/five-functions/cybersecurity-framework

4) What are some common cyber security threats, and how can they be mitigated ?

Phishing:

- Threat: A technique where attackers trick users into providing sensitive information by pretending to be a legitimate entity.
- Mitigation: Educate users, implement anti-phishing tools, and verify the authenticity of emails.

Malware:

- Threat: Malicious software that can disrupt, damage, or gain unauthorized access to systems.
- Mitigation: Use updated antivirus software, avoid downloading from untrusted sources.

Ransomware:

- Threat: Malware that encrypts data and demands ransom for decryption.

- Mitigation: Regular data backups, awareness training, and endpoint protection.

Reference Link: https://us-cert.cisa.gov/ncas/tips/ST04-014

5) What are access controls, and what are their various types?

Access Controls:

- Mechanisms to ensure that only authorized individuals can access specific resources.
- Help protect data confidentiality and integrity.

Types:

- Discretionary Access Control (DAC): The owner decides who can access the data.
- Mandatory Access Control (MAC): Access is granted based on security clearances; enforced by administrators.
- Role-Based Access Control (RBAC): Permissions are granted based on user roles within the organization.
- Attribute-Based Access Control (ABAC): Access is determined by user attributes (e.g., department, role, time of access).

6) Differentiate between active reconnaissance and passive reconnaissance in cybersecurity?

Active Reconnaissance:

- Involves directly interacting with the target system to gather information.
- Examples: Port scanning, network mapping.

- Risk: May trigger alarms or alerts, as the activity is detectable.

Passive Reconnaissance:

- Involves gathering information without directly interacting with the target.
- Examples: Searching for information on websites, social media, and public databases.
- Risk: Less likely to be detected by security systems.

7) What are the different types of cyber attacks?

Denial of Service (DoS) and Distributed Denial of Service (DDoS):

- Attack: Overloads a system, making it unavailable.
- Example: DDoS attack on a website using botnets.

SQL Injection:

- Attack: Injects malicious SQL code into a query to manipulate a database.
- Example: Retrieving unauthorized user data from a website.

Man-in-the-Middle (MitM):

- Attack: Intercepts communication between two parties to steal or manipulate data.
- Example: Eavesdropping on login credentials over unsecured Wi-Fi.

8) What is vulnerability assessment, and why is it crucial for organizations?

Definition: The process of identifying, quantifying, and prioritizing vulnerabilities in a system.

Features:

- Comprehensive Scanning: Regularly scans systems to detect potential vulnerabilities.

- Risk Prioritization: Identifies critical vulnerabilities that need immediate attention.
- Report Generation: Provides detailed reports with recommendations for remediation.

Reference Link: https://www.kaspersky.com/resource-center/definitions/vulnerability-assessment

Discretionary Access Control (DAC)

Definition:

Discretionary Access Control (DAC) is a type of security model that allows the owner of the resource (file, system, data) to determine who can access it. The owner has complete control over the permissions, and can decide to grant or revoke access to any user.

How It Works:

- Users are given access based on the discretion of the owner.
- Access rights can be assigned to individuals or groups, and permissions may include reading, writing, or executing the resource.

Examples:

- File-sharing systems, where a user can decide which colleagues can read or edit a document.
- Social media platforms, where users can choose who can view or comment on their posts.

Advantages:

- Flexibility: The owner has full control over permissions, making it easy to manage access for different users.
- Ease of Use: Straightforward to implement in systems where owners need to share or restrict access.

Disadvantages:

- Security Risks: Since control lies with individual users, a lack of careful management can lead to accidental data exposure.
- Scalability Issues: Managing permissions can become complex if there are many resources and users.

Reference Link: https://www.sciencedirect.com/topics/computer-science/discretionary-access-control

Mandatory Access Control (MAC)

Definition:

Mandatory Access Control (MAC) is a strict security model where access permissions are determined by a central authority, not by the owner of the data. Permissions are assigned based on policies and user clearance levels.

How It Works:

- Users are assigned security clearances, while data objects are tagged with classifications (e.g., confidential, top secret).
- Access is granted based on matching the user's clearance with the classification of the data.

Examples:

- Government and military systems, where only personnel with specific security clearances can access classified information.
- Corporate environments that handle sensitive data, such as financial records or trade secrets.

Advantages:

- High Security: Centralized control minimizes the risk of unauthorized access, making it ideal for handling sensitive information.
- Policy-Driven: Ensures consistency in access control across the organization.

Disadvantages:

- Limited Flexibility: Users cannot modify permissions on their own; all changes must go through administrators.
- Complex Management: Implementing MAC can be complex, especially in environments with diverse user roles and data classifications.

Role-Based Access Control (RBAC)

Definition:

Role-Based Access Control (RBAC) is a widely-used model where access permissions are assigned based on the roles of users within an organization. Roles are defined according to job functions, and permissions are granted to roles rather than individual users.

How It Works:

- Users are assigned one or more roles, and each role has specific permissions (e.g., read, write, edit).
- If a user's role changes, updating their permissions is straightforward by reassigning their role.

Examples:

- Corporate Settings: In an office, employees might be assigned roles such as "Admin," "Manager," or "Employee," with each role having specific access rights.
- Software Applications: Administrators can control who has access to certain features or data by assigning roles.

Advantages:

- Simplifies Management: Easy to manage access rights, especially when there are many users and systems.
- Scalable: Roles can be created or modified without changing the individual permissions for every user.

Disadvantages:

- Rigid Structure: If roles are not defined properly, it may lead to unnecessary access or restrictions.
- Initial Setup: Requires careful planning during the initial setup to ensure that roles accurately reflect job functions.

Reference Link: https://csrc.nist.gov/publications/detail/sp/800-162/final

Attribute-Based Access Control (ABAC)

Definition:

Attribute-Based Access Control (ABAC) is an advanced model where access rights are granted based on user attributes (such as department, job title, location) and the attributes of the resource being accessed.

How It Works:

- Rules are created that specify which attributes must match for access to be granted.
- Access control policies consider multiple attributes to make dynamic access decisions.

Examples:

- Cloud Services: Access can be determined by attributes like time of day, location, and the type of device used.
- Corporate Networks: Policies might allow access to sensitive data only if the user is connected to a secure network.

Advantages:

- Granular Control: Provides a high level of detail in access control, enabling more precise security measures.
- Dynamic Access: Policies can adapt to changing situations, providing flexibility without compromising security.

Disadvantages:

- Complexity: Designing and implementing ABAC policies can be complex.

- Performance: Evaluating multiple attributes may lead to performance issues if not optimized properly.

Active Reconnaissance

Definition:

Active reconnaissance involves interacting directly with the target system to gather information. This is typically done using tools that send out probes to discover vulnerabilities or open ports.

Examples:

- Port Scanning: Scanning a server to check which ports are open and what services are running on them.
- Network Mapping: Using tools like Nmap to discover hosts on a network and their operating systems.

Advantages:

- Detailed Information: Provides in-depth information about the target system, helping in the identification of specific vulnerabilities.
- Effective for Penetration Testing: Useful for ethical hackers to simulate real-world attacks and improve security.

Disadvantages:

- Risk of Detection: Since it involves direct interaction, there is a high chance that security systems will detect and block the activities.

Reference Link: https://www.techopedia.com/definition/27703/active-reconnaissance

Passive Reconnaissance

Definition:

Passive reconnaissance involves gathering information without directly interacting with the target system. It relies on publicly available data and does not alert the target of the probing activity.

Examples:

- WHOIS Lookup: Checking domain registration details.
- Social Media Analysis: Extracting information about an organization or individual from social networks.

Advantages:

- Undetectable: Since there is no direct interaction, passive reconnaissance remains undetected by the target.
- Safe: Can gather a lot of useful information without risk.

Disadvantages:

- Limited Information: May not provide as much detail as active reconnaissance techniques.

Vulnerability Assessment and Its Features

Definition:

A vulnerability assessment is a systematic approach to identifying, analyzing, and evaluating vulnerabilities in a system, network, or application.

Key Features:

- Automated Scanning: Utilizes tools to scan systems for known vulnerabilities, such as outdated software, unpatched applications, and weak passwords.
- Risk Evaluation: Helps prioritize vulnerabilities based on the risk they pose, allowing organizations to address the most critical issues first.
- Detailed Reporting: Generates comprehensive reports that include identified vulnerabilities, their potential impacts, and recommendations for mitigation.
- Continuous Monitoring: Some tools offer ongoing monitoring to detect new vulnerabilities as they emerge.

Benefits:

- Proactive Security: Identifying vulnerabilities before they are exploited helps organizations strengthen their security posture.
- Compliance: Assists in meeting regulatory requirements that mandate regular security assessments.

Reference Link: https://www.kaspersky.com/resource-center/definitions/vulnerability-assessment

Concept and Types of Scanning Methodology

Definition:

Scanning methodologies are techniques used to discover systems, services, and vulnerabilities on a network. They are often a part of the reconnaissance phase in penetration testing.

Types of Scanning:

- Port Scanning: Identifies open ports on a network and the services running on them. Tools like Nmap are commonly used for this purpose.
- Network Scanning: Discovers devices connected to a network and maps the network topology.
- Vulnerability Scanning: Checks systems for known vulnerabilities that could be exploited. Tools like Nessus and OpenVAS are widely used.
- Web Application Scanning: Specifically looks for vulnerabilities in web applications, such as SQL injection and Cross-Site Scripting (XSS).

Benefits:

- Enhanced Security: Helps in identifying weaknesses that could be exploited by attackers.
- Improved Network Management: Assists administrators in maintaining an inventory of devices and services running on their networks.

Penetration Tests

Definition:

Penetration testing, also known as a pen test, is a simulated cyber attack against a computer system, network, or web application to identify security vulnerabilities that could be exploited by real attackers.

Purpose:

- To assess the effectiveness of security measures.
- To identify weak points in the system before attackers can exploit them.
- To provide a detailed report of vulnerabilities and recommend corrective measures.

Types of Penetration Testing:

- Black Box Testing: The tester has no prior knowledge of the system. This mimics the approach of an external attacker.
- White Box Testing: The tester has full knowledge of the system, including architecture, source code, and internal structures.
- Gray Box Testing: The tester has partial knowledge of the system, representing an internal threat scenario.

Benefits:

- Realistic Assessment: Simulates real-world attack scenarios to provide a more accurate assessment of security.
- Regulatory Compliance: Helps businesses meet compliance requirements by regularly testing their security measures.

Tools: Some commonly used penetration testing tools include Metasploit, Burp Suite, and Wireshark.

Unit -2

Network Security Threats and Countermeasures

Definition:

Network security threats are risks that can compromise the integrity, confidentiality, or availability of data on a network.

Common Threats:

- Malware: Viruses, worms, and ransomware that can corrupt files or lock systems.
- Phishing: Attempts to steal sensitive information through deceptive emails or websites.
- Man-in-the-Middle (MitM) Attacks: Intercepting communications between two parties to steal or alter data.
- DDoS (Distributed Denial of Service): Overloading a network or service to make it unavailable.

Countermeasures:

- Firewalls: Block unauthorized access.
- Intrusion Detection and Prevention Systems (IDS/IPS): Monitor network traffic to detect and prevent suspicious activity.
- Encryption: Secures data in transit and at rest.
- Regular Updates and Patching: Fix known vulnerabilities.

Reference Link: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Network Security Devices

Types of Devices:

- Firewalls: Act as a barrier between trusted and untrusted networks.

- Routers: Direct data traffic and can implement basic security measures.
- Switches: Control data flow and isolate network segments to prevent unauthorized access.
- IDS/IPS: Detect and prevent unauthorized or malicious activities.
- VPN Gateways: Securely connect remote users to a corporate network.

Importance:

- Network Integrity: Protects against external threats and ensures reliable data flow.
- Data Confidentiality: Prevents data breaches and information leaks.

Reference Link: https://www.fortinet.com/resources/cyberglossary/network-security

Types of Network Securities

1) Physical Security: Protects network devices from physical tampering or damage.
2) Technical Security: Utilizes software and hardware solutions like firewalls, encryption, and anti-virus systems.
3) Administrative Security: Policies and procedures that dictate who can access the network and under what conditions.

Network Access Control (NAC)

Definition:

A security solution that manages and enforces access to network resources based on user, device, and location.

Characteristics:

- Authentication: Verifies user credentials.
- Authorization: Determines access levels based on user role.
- Endpoint Security: Ensures devices meet security policies before they are granted network access.

Application Security

Definition:

Measures taken to secure applications during their development, deployment, and usage.

Tools:

- Web Application Firewalls (WAF): Protects against common web attacks like SQL injection and XSS.
- Static Application Security Testing (SAST): Analyzes source code for vulnerabilities.
- Dynamic Application Security Testing (DAST): Tests running applications for security flaws.

Reference Link: https://owasp.org/www-project-top-ten/

Firewalls and Its Types

Definition:

A network security device that monitors and controls incoming and outgoing traffic based on security rules.

Types:

- Packet-Filtering Firewall: Examines packets and blocks those that do not meet predefined rules.
- Stateful Inspection Firewall: Tracks active connections and decides whether packets are part of a legitimate session.

- Proxy Firewall: Intercepts all messages entering or leaving the network and hides the true network addresses.

Virtual Private Network (VPN)

Definition:

A VPN creates a secure, encrypted connection over a less secure network (e.g., the Internet).

Benefits:

- Privacy: Masks IP address and encrypts data.
- Remote Access: Securely connects remote users to the corporate network.

Tunneling Protocol and Types

Definition:

Tunneling protocols encapsulate data packets for transmission over a network.

Types:

- PPTP (Point-to-Point Tunneling Protocol): Provides a secure, encrypted connection.
- L2TP (Layer 2 Tunneling Protocol): Often combined with IPsec for enhanced security.
- SSL/TLS: Provides encryption for web-based traffic.

Reference Link: https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/

IDS vs. IPS

Definition:

IDS (Intrusion Detection System) monitors network traffic and alerts if suspicious activity is detected. IPS (Intrusion Prevention System) actively prevents the activity from occurring.

Key Difference:

- IDS: Passive, alerts admins of threats.
- IPS: Active, blocks threats in real-time.

Web Application Vulnerabilities

Common Issues:

- SQL Injection: Inserting malicious SQL queries to manipulate databases.
- Cross-Site Scripting (XSS): Injecting scripts into web pages viewed by other users.
- CSRF (Cross-Site Request Forgery): Trick users into performing actions without their knowledge.

Reference Link: https://owasp.org/www-project-top-ten/

Mobile Application Security

Threats:

- Malware: Infects mobile devices through malicious apps.
- Phishing: Fake apps or links that steal personal information.
- Security Practices:
- App Sandboxing: Isolates apps to prevent interaction with other apps.
- Data Encryption: Protects sensitive information on mobile devices.

Reference Link: https://developer.android.com/topic/security/best-practices

Cloud Computing Threats and Solutions

Threats:

- Data Breaches: Unauthorized access to sensitive data stored in the cloud.
- Account Hijacking: Attackers gaining access to cloud accounts.

Solutions:

- Encryption: Ensures data privacy in transit and at rest.
- Multi-Factor Authentication (MFA): Adds an extra layer of security.

Reference Link: https://www.ibm.com/in-en/cloud/learn/cloud-security