Assignment - 2

Q) 1) Name and explain the possible vulnerabilities associated with user applications running in their computing systems when connected to internet.

Ans → i) Unpatched Software → Applications that are not updated regularly may contain known security flaws. Hackers exploit these weakness to gain unauthorised access or control.

ii) Weak authentication and Passwords → Using weak or reused passwords makes it easy for attackers to guess or brute-force login credentials.

iii) Insecure Network Communication → If applications transmit data over unencrypted connections, attackers can intercept or alter the data using Man-in-the-middle attacks.

iv) Phising and Social Engineering → Users may be tricked into downloading malicious files or revealing sensitive information through fake websites or emails.

v) Malware and Ransomware → Applications can be infected with malicious software that damages, steals, or encrypts user data.

vi) Improper Access Controls → If an application doesn't correctly limit user permissions, attackers may gain access to restricted areas or perform unauthorized actions.

2) State, how the SQLI (Structured Query Language Injection) a common possible cyber-attack works to cause harm during web browsing. Also narrate the mitigation process to prevent such type of attack.

Ans → SQL injection is a cyber-attack where an attacker injects malicious SQL statements into a query through user input fields. This occurs when a web application does not properly sanitize or validate user input, allowing the attacker to manipulate the underlying database.

Mitigation techniques → i) Use prepared statements → Safely separates SQL logic from data

ii) Input Validation and Sanitization → Allow only expected input formats.

iii) Use ORM (Object Relational Mapping) Tools → Tools like Django ORM, SQL Alchemy automatically handle SQL queries safely.

iv) Least Priviledge Access → Give the web application limited database permissions. Avoid using admin level database users.

v) Web Application Firewalls (WAF) → WAFs can detect and block known SQLi attack patterns in real time.

3) List and define the flaws in cryptography process which may lead to a possible cryptographic vulnerability.

Ans → i) Weak algorithms → Use of outdated or easily breakable cryptographic algorithms.

ii) Poor key management → Insecure generation, storage, distribution or handling of cryptographic keys.

Name: _____ Regd No: _____

iii) Improper Implementation → Flaws in how cryptographic algorithms are coded or integrated into applications.

iv) Use of hardcoded or predictable keys → Keys that are static, hardcoded or easily guessable.

v) Reuse of Nonces or initialization vectors → Reusing a nonce or IV in algorithm like AES-GCM or CBC mode weakens encryption and can ~~lead~~ lead to data leakage.

vi) Lack of Encryption for sensitive data → Storing ~~data~~ or transmitting sensitive data without encryption.

4) Briefly explain the unwanted files/programs that are downloaded to a user system through internet access which later creates a malware attack.

Ans → i) Trojan Horse → A program that appears to be legitmate (like a game or utility) but secretly contains malicious code.

ii) Worms → Self-replicating programs that ~~user~~ spread across networks without user interaction.

iii) Spyware → Software that secretly monitors user activity, such as keystrokes or browsing behaviour.

iv) Adware → Automatically ~~ads~~ displays or download advertisements, often without user consent.

v) Ransomware → Encrypts user files or locks the system, demanding payment for access.

vi) Rootkits → Tools that hide the presence of malware by modifying system processes or kernel.

5) What is meant by DNS cache poisoning associated with DNS attack? Discuss briefly, how DNS sinkhole can be used to prevent DNS attack?

Ans → DNS cache poisoning is a type of DNS attack where an attacker inserts false DNS records into a resolver's ~~ca~~ cache. This causes the DNS server to return an incorrect IP address, redirecting users to malicious or fake websites without their knowledge.

DNS sinkhole is a defensive mechanism that redirects malicious DNS queries to a controlled and safe IP address, instead of allowing them to reach harmful destinations.

How DNS sinkhole prevents DNS attacks →

i) Detection → The sinkhole monitors DNS traffic and identifies requests to known malicious domains.

ii) Redirection → Instead of resolving the domain to the real (malicious) IP, it resolves to a non-routable or safe IP (like 127.0.0.1)

iii) Protection → Prevents devices from communicating with malware servers, thus blocking command-and-control (C&C) communication or malware downloads.

iv) Logging → Allows administrations to track which devices attempted access, helping with incident response.

Name: _____ Regd No: _____

6) Explain the following processes adopted by adversaries to launch an on-path attack in computer network.

i) Session replay ii) Message replay iii) Credential replay iv) Credential Stuffing

Ans → i) Session replay → Session replay is an attack where the adversary captures and reuses valid session tokens or authentication messages to impersonate a legitimate user. Bypass authentication and impersonate the user.

ii) Message replay → It involves capturing a legitimate message or data packet transmitted over the network and resending it to the recipient to decieve or manipulate the system. Reexecute valid actions for malicious benefit.

iii) Credential replay → In this, stolen usernames and passwords are used to log in to systems or services. Gain unauthorised access to a specific service or account.

iv) Credential stuffing → ~~In this, stolen~~ It is an automated attack where attackers use stolen credential pairs from one data breach to try to log in to other services. Exploit password reuse ~~across~~ across multiple accounts & platforms.

7) List and discuss ~~briefly~~ briefly different types of segmentation techniques used in computer networking, to ~~segmentation~~ reduce the impact of potential breach.

Ans → i) Physical Segmentation → Uses separate physical hardware (like switches, routers, and cables) to isolate parts of a network.

Benefit → Complete isolation; highly secure.

Use case → Critical infrastructure systems; military networks.

ii) VLAN Segmentation → Creates logical segments within the same physical network using switches. Separates traffic between departments efficiently. Needs careful setup to avoid VLAN hopping attacks.

iii) Subnetting → Divides an IP network into smaller addressable sub-networks. Controls broadcast traffic and improves routing. Requires proper IP planning and router configuration.

iv) Firewall-Based Segmentation → Uses firewalls to control traffic between network zones. Allows granular access based on IPs, ports, or protocols. Effective but complex to manage at scale.

8) Name the two key factors required to be executed to satisfy the goal of access control mechanism associated with security issue in computer networking. Also differentiate between a file system Access Control List (ACL) and a network ACL being a part of access control mechanism.

Ans → Two key factors to satisfy Access Control Goals →

i) Authentication → Verifies the identity of the user or device attempting to access the system.

ii) Authorisation → Determines what actions or resources the authenticated entity is allowed to access.

Name: _____ Regd No: _____

Difference between File System ACL and Network ACL →

Feature	File System ACL	Network ACL
Purpose	Controls access to files and directories.	Control access to network resources
Scope	Operates at the OS-level	Operates at the network-level
Rules based on	User / group permissions	IP addresses, protocols, ports, traffic direction
Example	User can read but not modify a file	Block incoming traffic on port 80 from a subnet

9) List and highlight the use of key elements for a multiplayer strategy required to be implemented towards achieving effective network strategy.

Ans → i) Firewall → Filters incoming and outgoing traffic based on security rules. Prevents unauthorised access to or from a private network.

ii) Intrusion Detection and Prevention System (IDPS) → Monitors network traffic for suspicious activity and policy violations. Detects and blocks potential threats in real-time.

iii) Antivirus and Antimalware → Scans and removes malicious software from systems. Protects endpoints from viruses, ransomware, spyware, etc.

iv) Network Segmentation → Divides the network into isolated zones. Limits lateral movement during a breach and contains attacks.

v) Access Control → Ensures only verified users access specific systems or data. Prevents unauthorised access and enforces user priviledges.

vi) Encryption → Secures data in transit and at rest using cryptographic techniques. Maintains confidentiality and integrity of sensitive information.

10) Discuss the major benefits of infrastructure as code (IaC).

Ans → i) Speed & Efficiency → IaC automates the provisioning of infrastructure, drastically reducing the time required to set up and deploy environments.

ii) Consistency & Standardisation → By using code to define infrastructure, you avoid human errors & ensure every environment (dev, test, prod) is configured identically.

iii) Version Control & Auditability → Infrastructure definitions can be stored in version control systems enabling rollback, history tracking and collaborative changes.

iv) Scalability & Flexibility → IaC makes it easy to scale resources up or down automatically based on demand or predefined conditions.

Name: _____ Regd No: _____

11) Explain briefly the micro-services as a secured architecture listing out the key benefits of it.

Ans → Microservices architecture breaks down applications into small, independent services, each responsible for a specific functionality. These services communicate over secure APIs and are deployed independently, enhancing both scalability and security.

Key benefits →

i) Isolation of Services → A breach in one service doesn't affect others, limiting the blast radius of attacks.

ii) Smaller Attack Surface → Each service has a minimal, focused role, reducing exposed interfaces & vulnerabilities.

iii) Granular Access Control → Security policies and permissions can be enforced per service.

iv) Easier updates and patching → Security fixes can be applied to individual services without affecting the whole application.

12) Briefly explain the major security concerns associated with IOT devices.

Ans → i) Weak Authentication & Authorisation → Many IOT devices use default or hardcoded credentials, making them easy targets for unauthorised access.

ii) Lack of regular updates → IOT devices often lack firmware updates or patching mechanisms, leaving known vulnerabilities unaddressed.

iii) Unencrypted Communication → Data transmitted between devices and servers is sometimes unencrypted, exposing it to interception and tampering.

iv) Poor physical security → IoT devices deployed in public or uncontrolled environments are susceptible to physical tampering.

v) Insecure APIs → Improperly designed or exposed APIs can be exploited to gain unauthorised access or control.

vi) Device Hijacking and Botnets → Compromised IoT devices can be hijacked and used in large scale attacks, such as DDoS.

13) With the help of a suitable diagram, explain the function of each of the four Supervisory, Control and Data Acquisition (SCADA) system levels.

Ans → SCADA System levels →

i) Field Level (Level 0) - Sensors and Actuators

- Functions → This level includes physical devices like sensors and actuators that collect real-world data and execute control actions.
- Role → Interface with the physical process.

ii) Control Level (Level 1) - PLCs & RTUs.

- Functions → Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) gather

Name: _____ Regd No: _____

data from field data field devices and send control commands.

- Role → Real-time data acquisition and basic process control.

iii) Supervisory Level (Level 2) → SCADA Software/HMI

- Function → SCADA software and Human-Machines Interfaces (HMIs) display data, allow operator interaction, and send control commands.
- Role → Monitor and control process remotely.

iv) Enterprise Level (Level 3) → Data Management /IT systems

- Function → ~~SCADA software and Human-Machine~~ Stores historical data, generates reports & integrates with business systems.
- Roles → Long-term planning, performance analysis and enterprise integration.

Diagram →

Level 3: Enterprise Level
↑
Level 2: Supervisory Level
↑
Level 1: Control Level
↑
Level 0: Field Level

14) What is meant by attack surface in a network scenario? Explore briefly the key aspects of attack surfaces to need to be focused by a cyber-security proffesional.

Ans) The attack surface refers to all the possible points in a network or system where an unauthorised user can try to enter, extract data or cause harm. It includes all vulnerabilities, entry points, and interfaces that could be exploited.

Key aspects →

i) Network Attack Surface → a) Includes → open ports, unsecured APIs, communication protocols.
b. Monitor & limit exposed services, use firewalls and network segmentation.

ii) Software Attack Surface →

- Includes → Applications, operating system and services running on devices.
- Focus → Patch vulnerabilities, disable unused features, perform code reviews.

iii) Human/Physical Attack Surface →

- Includes → Social engineering, insider threats, physical access point.
- Focus → Employee training, access control, surveillance.

15) With the help of a suitable examples highlight the attributes associated with different categories of devices in the context of infrastructure security.

Ans → i) End-User Devices → • Examples → Laptops, desktops, mobile phones, tablets
• Attributes → i) Often mobile and exposed to public networks
ii) Require endpoint protection
iii) Susceptible to phising, malware, and user error

ii) Network Devices → • Examples → Routers, switches, firewalls, load balancers.
• Attributes → i) Control data flow across networks
ii) Critical for segmentation and traffic filtering
iii) Must be secured with strong credentials and firmware updates

iii) Server Devices → • Examples → Web servers, application servers, database servers.
• Attributes → i) Host critical applications and data
ii) Require patch management, secure configurations and monitoring
iii) Common targets for attacks like SQL injection or priviledge escalation.

iv) IOT Devices → • Examples → Smart cameras, thermostats, industrial sensors
• Attributes → i) Often have limited security features and computing power.
ii) Must be isolated or segmented from critical systems.
iii) Susceptible to hijacking and DDoS attacks.

16) List and define the various data types considered as a regulated data required to be protected from security beach in organisations.

Ans → i) Personally Identifiable Information → • Definition → Any Data that can be used to identify an individual. • Examples → Name, address, social security number, phone number, email
• Regulations → GDPR, CCPA, HIPAA (USA), etc.

ii) Protected Health Information → • Definition → Medical data linked to an individual's health status or health care services. • Examples → Medical records, prescriptions, insurance information.

iii) Payment Cared Information → • Definition → Sensitive data associated with credit or debit cared transactions. • Examples → Cared Numbers, CW codes, expiration dates.

iv) Financidl Data → • Definition → Information related to a person's or organisations financial activities. Examples → Bank account numbers, transaction details, tax information.

v) Confidential Business Information → • Definition → Proprietary organizational information not meant for public disclosure. • Examples → Product designs, source code, business strategies.

Name: _____ Regd No: _____

17) Justify that data classification seems to be important in organisations for giving safeguards to various data types from security breach. Also mention the key classification types of data sets available in organisations.

Ans → Data classification is a critical process that involves organising data into categorising based on its sensitivity, value, and regulatory requirements. This process is essential for implementing appropriate security controls and ensuring compliance with data protection laws.

Key Data Classification Types in Organisations →

Classification Type	Description
Public	Data that can be freely shared with the public without any risk.
Internal/Private	Data meant for internal use within the organisation; not for external sharing.
Confidential	Sensitive business data that could cause harm if disclosed.
Restricted / Highly confidential	Critical data whose unauthorised disclosure could result in severe financial, legal or reputational damage.

18) Explain the following methods that are meant for securing data from possible breaches during communication over a network. i) Geographic restriction ii) Hashing iii) Tokenisation iv) ~~Obsu~~ Obfuscation

Ans → i) Geographic Restriction → A security method that limits access to data or services based on the geographic location of the user or device. Reduces exposure to global cyberattacks & ensures compliance with regional data laws.

ii) Hashing → A one-way cryptographic function that ~~overwrites~~ converts data into a fixed-length string, which cannot be reversed to obtain the original data. Secures data by ensuring that even if intercepted, original data cannot be retrieved from the hash.

iii) Tokenisation → The process of replacing sensitive data with non-sensitive equivalents, which have no exploitable value outside a specific system. Prevents attackers from gaining access to real data even if the tokens are compromised.

iv) Obfuscation → Technique used to make data or code unreadable or harder to understand by transforming it into a complex or ambiguous form. Adds a layer of security by concealing the true meaning of the data, making it harder for attackers to interpret ~~to~~ or misuse it.

Name: _____ Regd No: _____

19) State the use of network load balancer that guarantees the availability of network to the host devices in a company even though the network carries high volume of traffic. Also differentiate the ~~load~~ basic two load balancer configurations active/active and active/passive.

Ans→ A Network Load Balancer is used to distribute incoming network traffic across multiple servers or resources in a balanced and efficient manner. It ensure →

- High Availability → Even under heavy traffic, the system remains accessible.
- Scalability → New servers can be added to handle increased load without downtime.
- Fault Tolerance → If one server fails, traffic is rerouted to others, minimizing service disruption.

Difference between Active/Active and Active/Passive Configurations →

Aspect	Active/Active Load Balancing	Active/Passive Load Balancing
Working nodes	All nodes actively handle traffic simultaneously.	One node is active, and other remain on standby
Performance	Offers better performance and resource utilization.	Lower resource utilization during normal operations.
Failover Handling	Load is automatically redistributed among all active nodes.	If the active node fails, a passive one takes over the full load.
Use case	Suitable for high demand, real time systems	Preferred for simpler, cost-sensitive setups requiring redundancy.

20) Name and illustrate briefly the scheduling techniques used by the load balancer to distribute the workload.

Ans→ i) Round Robin → Requests are distributed sequentially across all servers in a circular order.

Use case → Suitable when all servers have equal capacity.

ii) Least Connections → The request is sent to the server with the fewest active connections.

Use case → Ideal when session lengths vary or traffic is unpredictable.

iii) IP hash → A hash of the client's IP address determines which server recieves the request.

Use case → Useful for session persistence or user affinity.

iv) Weighted Round Robin → Servers are assigned a weight based on capacity; higher-weight servers get more requests.

Use case → Best for environments with servers of different capabilities.

v) Weighted Least Connections → Like least Connections but takes server weight into account when distributing traffic.

Use case → Suitable when handling mixed-performance servers.

Name: _____ Regd No: _____