Unit – 1 | INT242 MCQs | www.geeksforcampus.com

1. What is the primary purpose of security roles in an organization?

A) To ensure compliance with industry regulations

B) To assign blame in case of a security breach

C) To manage and mitigate security risks

D) To increase employee workload

Answer: C) To manage and mitigate security risks

2. Which of the following is not a common information security role?

A) Security Analyst

B) Chief Financial Officer (CFO)

C) Security Engineer

D) Security Architect

Answer: B) Chief Financial Officer (CFO)

3. Which security control framework provides a comprehensive set of security controls for federal information systems and organizations?

A) ISO/IEC 27001

B) NIST Special Publication 800-53

C) COBIT

D) HIPAA

Answer: B) NIST Special Publication 800-53

4. What is the primary goal of threat actors in a cyber attack?

A) Financial gain

B) Political influence

C) Fame and recognition

D) All of the above

Answer: D) All of the above

5. Which threat actor type is typically motivated by political or ideological reasons?

A) Script Kiddies

B) Hacktivists

C) Insiders

D) Nation-State Actors

Answer: B) Hacktivists

6. Which attack vector involves exploiting vulnerabilities in software to gain unauthorized access?

A) Phishing

B) DDoS Attacks

C) SQL Injection

D) Social Engineering

Answer: C) SQL Injection

7. What is the primary source of threat intelligence?

A) Social Media

B) Government Agencies

C) News Websites

D) All of the above

Answer: D) All of the above

8. Which network reconnaissance tool is commonly used for discovering devices and services on a network?

A) Nmap

B) Wireshark

C) Metasploit

D) Burp Suite

Answer: A) Nmap

9. What is the main purpose of vulnerability scanning?

A) To exploit vulnerabilities

B) To identify and prioritize security weaknesses

C) To encrypt sensitive data

D) To block malicious traffic

Answer: B) To identify and prioritize security weaknesses

10. Which vulnerability scanning technique involves sending malformed data to a target to observe its response?

A) Black-box Testing

B) White-box Testing

C) Fuzzing

D) Brute Force Attack

Answer: C) Fuzzing

11. What is the primary goal of penetration testing?

A) To identify and mitigate vulnerabilities

B) To gather threat intelligence

C) To secure network infrastructure

D) To install security patches

Answer: A) To identify and mitigate vulnerabilities

12. Which social engineering technique involves impersonating someone with authority to gain access to sensitive information?

A) Phishing

B) Tailgating

C) Pretexting

D) Baiting

Answer: C) Pretexting

13. What are common indicators of malware-based attacks?

A) Slow network performance

B) Unexpected pop-up windows

C) Unauthorized file modifications

D) All of the above

Answer: D) All of the above

14. What is a common characteristic of ransomware?

A) Stealing sensitive data

B) Deleting files without warning

C) Encrypting files and demanding payment

D) Disabling antivirus software

Answer: C) Encrypting files and demanding payment

15. Which type of malware disguises itself as legitimate software?

A) Worm

B) Trojan Horse

C) Rootkit

D) Logic Bomb

Answer: B) Trojan Horse

16. Which of the following is not a social engineering technique?

A) Shoulder Surfing

B) Spear Phishing

C) Cross-Site Scripting (XSS)

D) Baiting

Answer: C) Cross-Site Scripting (XSS)

17. Which vulnerability type occurs when software developers inadvertently leave backdoors in their code?

A) Zero-Day Vulnerability

B) Design Flaw

C) Logic Error

D) Buffer Overflow

Answer: B) Design Flaw

18. What is a common method to protect against SQL injection attacks?

A) Using strong passwords

B) Encrypting network traffic

C) Input Validation

D) Updating antivirus software

Answer: C) Input Validation

19. Which type of penetration testing involves the tester having full knowledge of the target system?

A) White-box Testing

B) Black-box Testing

C) Gray-box Testing

D) Red Team Testing

Answer: A) White-box Testing

20. What is a common technique to mitigate the risk of phishing attacks?

A) Multi-factor Authentication

B) Installing firewalls

C) Disabling JavaScript

D) Using public Wi-Fi networks

Answer: A) Multi-factor Authentication

21. What is the primary purpose of a firewall?

A) To encrypt data transmissions

B) To prevent unauthorized access to or from a private network

C) To detect and remove malware

D) To store sensitive information

Answer: B) To prevent unauthorized access to or from a private network

22. Which social engineering technique involves creating a sense of urgency to prompt immediate action?

A) Phishing

B) Tailgating

C) Impersonation

D) Urgency Scam

Answer: D) Urgency Scam

23. Which type of malware spreads by attaching itself to executable files?

A) Virus

B) Worm

C) Trojan Horse

D) Rootkit

Answer: A) Virus

24. What is the primary objective of a rootkit?

A) To record keystrokes

B) To encrypt data

C) To gain unauthorized access and maintain control over a system

D) To delete files

Answer: C) To gain unauthorized access and maintain control over a system

25. Which vulnerability scanning technique involves analyzing the source code of an application?

A) Fuzzing

B) Static Analysis

C) Dynamic Analysis

D) Black-box Testing

Answer: B) Static Analysis

26. Which of the following is not a common penetration testing methodology?

A) White-box Testing

B) Gray-box Testing

C) Black-hat Testing

D) Red Team Testing

Answer: C) Black-hat Testing

27. What is a common indicator of a phishing email?

A) Typos and grammatical errors

B) Encrypted attachments

C) Short and concise message

D) Use of official company logo

Answer: A) Typos and grammatical errors

28.

Which type of malware spreads by replicating itself and spreading to other systems?

A) Virus

B) Worm

C) Trojan Horse

D) Rootkit

Answer: B) Worm

29. What is a common method to prevent malware infections?

A) Disabling antivirus software

B) Clicking on suspicious links

C) Regularly updating software and operating systems

D) Sharing passwords with coworkers

Answer: C) Regularly updating software and operating systems

30. Which of the following is not an example of a vulnerability type?

A) Buffer Overflow

B) Cross-Site Scripting (XSS)

C) Ransomware

D) SQL Injection

Answer: C) Ransomware

Unit – 2

1. What is the primary purpose of cryptographic ciphers?

A) To authenticate users

B) To ensure data integrity

C) To encrypt and decrypt data

D) To block network traffic

Answer: C) To encrypt and decrypt data

2. Which cryptographic mode of operation provides confidentiality and authentication?

A) ECB (Electronic Codebook)

B) CBC (Cipher Block Chaining)

C) CTR (Counter)

D) OFB (Output Feedback)

Answer: B) CBC (Cipher Block Chaining)

3. Which cryptographic weakness can occur if the same key is used to encrypt large amounts of data?

A) Brute Force Attack

B) Birthday Attack

C) Key Reuse

D) Differential Cryptanalysis

Answer: C) Key Reuse

4. What is a common use case for symmetric cryptography?

A) Digital Signatures

B) Public Key Encryption

C) Secure File Transfer

D) Secure Email Communication

Answer: C) Secure File Transfer

5. Which cryptographic technology is commonly used to secure internet communication?

A) SHA-1 (Secure Hash Algorithm 1)

B) AES (Advanced Encryption Standard)

C) DES (Data Encryption Standard)

D) RSA (Rivest-Shamir-Adleman)

Answer: B) AES (Advanced Encryption Standard)

6. What is the role of a certificate authority (CA) in the context of digital certificates?

A) To generate public-private key pairs

B) To issue and sign digital certificates

C) To authenticate users based on biometrics

D) To manage encryption keys

Answer: B) To issue and sign digital certificates

7. Which cryptographic concept is used to securely distribute public keys?

A) Key Escrow

B) Key Revocation

C) Key Exchange

D) Key Generation

Answer: C) Key Exchange

8. Which cryptographic use case is particularly vulnerable to man-in-the-middle attacks?

A) Secure Email Communication

B) Secure File Transfer

C) Digital Signatures

D) Public Key Encryption

Answer: D) Public Key Encryption

9. Which cryptographic weakness can occur if the encryption algorithm is susceptible to mathematical attacks?

A) Key Length

B) Key Reuse

C) Algorithmic Vulnerability

D) Quantum Cryptography

Answer: C) Algorithmic Vulnerability

10. What is the primary purpose of a digital certificate?

A) To encrypt data

B) To authenticate the identity of a user or entity

C) To generate public-private key pairs

D) To secure network traffic

Answer: B) To authenticate the identity of a user or entity

11. Which authentication design concept emphasizes the principle of "something you have"?

A) Biometrics Authentication

B) Knowledge-Based Authentication

C) Multi-Factor Authentication

D) Single Sign-On

Answer: A) Biometrics Authentication

12. What is a common example of knowledge-based authentication?

A) Typing a PIN number

B) Scanning a fingerprint

C) Swiping an access card

D) Speaking a passphrase

Answer: A) Typing a PIN number

13. Which authentication technology uses physical characteristics such as fingerprints or iris patterns?

A) Token-based Authentication

B) Biometrics Authentication

C) Knowledge-Based Authentication

D) Certificate-based Authentication

Answer: B) Biometrics Authentication

14. What is the primary advantage of biometrics authentication?

A) High level of security

B) Easy to remember passwords

C) Compatibility with legacy systems

D) Low cost of implementation

Answer: A) High level of security

15. Which authentication control is used to verify the integrity of digital certificates?

A) Certificate Revocation List (CRL)

B) Certificate Signing Request (CSR)

C) Certificate Authority (CA)

D) Certificate Pinning

Answer: A) Certificate Revocation List (CRL)

16. Which authentication technology generates a unique code that changes periodically?

A) One-Time Password (OTP)

B) Smart Card Authentication

C) Biometrics Authentication

D) Certificate-based Authentication

Answer: A) One-Time Password (OTP)

17. What is the primary purpose of a Certificate Signing Request (CSR)?

A) To request a digital certificate from a CA

B) To authenticate users based on biometrics

C) To encrypt data transmissions

D) To generate public-private key pairs

Answer: A) To request a digital certificate from a CA

18. Which authentication design concept emphasizes the principle of "something you know"?

A) Biometrics Authentication

B) Knowledge-Based Authentication

C) Multi-Factor Authentication

D) Single Sign-On

Answer: B) Knowledge-Based Authentication

19. Which authentication technology requires users to possess a physical device to gain access?

A) Biometrics Authentication

B) Token-based Authentication

C) Certificate-based Authentication

D) Knowledge-Based Authentication

Answer: B) Token-based Authentication

20. What is the primary role of a certificate authority (CA) in the context of PKI management?

A) To issue and manage digital certificates

B) To authenticate users based on biometrics

C) To encrypt data transmissions

D) To store encryption keys

Answer: A) To issue and manage digital certificates

21. Which authentication control is commonly used to mitigate the risk of password-based attacks?

A) Multi-Factor Authentication

B) Single Sign-On

C) Biometrics Authentication

D) Token-based Authentication

Answer: A) Multi-Factor Authentication

22. What is a common weakness associated with knowledge-based authentication?

A) Vulnerable to shoulder surfing attacks

B) Difficult to remember passwords

C) Requires expensive hardware

D) Susceptible to phishing attacks

Answer: D) Susceptible to phishing attacks

23. Which authentication technology relies on cryptographic keys stored on a physical device?

A) Token-based Authentication

B) Biometrics Authentication

C) Knowledge-Based Authentication

D) Certificate-based Authentication

Answer: A) Token-based Authentication

24. What is the primary purpose of Public Key Infrastructure (PKI)?

A) To manage biometric data

B) To authenticate users based on knowledge

C) To secure network communications using certificates

D) To encrypt data using symmetric keys

Answer: C) To secure network communications using certificates

25. Which authentication design concept emphasizes the principle of "something you are"?

A) Biometrics Authentication

B) Knowledge-Based Authentication

C) Multi-Factor Authentication

D) Single Sign-On

Answer: A) Biometrics Authentication

26. What is a common vulnerability associated with biometrics authentication?

A) Sus

ceptible to replay attacks

B) Difficult to implement

C) Requires specialized hardware

D) Vulnerable to false positives and false negatives

Answer: D) Vulnerable to false positives and false negatives

27. Which authentication control allows users to access multiple applications with a single set of credentials?

A) Multi-Factor Authentication

B) Single Sign-On

C) Biometrics Authentication

D) Token-based Authentication

Answer: B) Single Sign-On

28. What is the primary purpose of a digital certificate authority (CA)?

A) To issue and manage digital certificates

B) To authenticate users based on biometrics

C) To encrypt data transmissions

D) To store encryption keys

Answer: A) To issue and manage digital certificates

29. Which authentication technology relies on a unique physical characteristic of the user?

A) Token-based Authentication

B) Biometrics Authentication

C) Knowledge-Based Authentication

D) Certificate-based Authentication

Answer: B) Biometrics Authentication

30. What is the primary role of a certificate authority (CA) in the context of PKI management?

A) To issue and manage digital certificates

B) To authenticate users based on biometrics

C) To encrypt data transmissions

D) To store encryption keys

Answer: A) To issue and manage digital certificates

Unit – 3

1. Which of the following is a fundamental principle of secure network designs?

   A) Open access

   B) Least privilege

   C) Public key encryption

   D) Unencrypted transmissions

   Answer: B) Least privilege

2. What is the primary purpose of secure switching and routing protocols?

   A) To prevent unauthorized access to the network

   B) To optimize network performance

   C) To secure data during transmission

   D) To regulate internet traffic

   Answer: A) To prevent unauthorized access to the network

3. Which encryption protocol is commonly used to secure wireless networks?

   A) SSL (Secure Sockets Layer)

   B) TLS (Transport Layer Security)

   C) WEP (Wired Equivalent Privacy)

   D) PPTP (Point-to-Point Tunneling Protocol)

   Answer: B) TLS (Transport Layer Security)

4. What is the primary purpose of load balancers in a network infrastructure?

   A) To encrypt data transmissions

   B) To distribute network traffic evenly across servers

   C) To monitor network activity

   D) To prevent DDoS attacks

Answer: B) To distribute network traffic evenly across servers

5. Which network operations protocol is used to manage and monitor network devices?

A) SNMP (Simple Network Management Protocol)

B) DNS (Domain Name System)

C) FTP (File Transfer Protocol)

D) DHCP (Dynamic Host Configuration Protocol)

Answer: A) SNMP (Simple Network Management Protocol)

6. Which application protocol is commonly used for secure file transfer over a network?

A) HTTP (Hypertext Transfer Protocol)

B) SMTP (Simple Mail Transfer Protocol)

C) FTPS (File Transfer Protocol Secure)

D) Telnet

Answer: C) FTPS (File Transfer Protocol Secure)

7. Which remote access protocol is known for its strong encryption and authentication mechanisms?

A) RDP (Remote Desktop Protocol)

B) SSH (Secure Shell)

C) TFTP (Trivial File Transfer Protocol)

D) POP3 (Post Office Protocol version 3)

Answer: B) SSH (Secure Shell)

8. Which network security appliance is designed to monitor and control incoming and outgoing network traffic?

A) Firewall

B) Load Balancer

C) Proxy Server

D) Intrusion Detection System (IDS)

Answer: A) Firewall

9. What is the primary purpose of a proxy server in network security?

A) To encrypt data transmissions

B) To filter and cache web content

C) To balance network traffic load

D) To monitor network activity

Answer: B) To filter and cache web content

10. Which network security appliance is used to analyze and respond to security events in real-time?

A) Firewall

B) Intrusion Prevention System (IPS)

C) SIEM (Security Information and Event Management)

D) Proxy Server

Answer: C) SIEM (Security Information and Event Management)

11. Which network security appliance acts as an intermediary between internal and external networks?

A) Firewall

B) Intrusion Detection System (IDS)

C) Proxy Server

D) Load Balancer

Answer: C) Proxy Server

12. What is the primary purpose of an intrusion detection system (IDS)?

A) To prevent unauthorized access to the network

B) To monitor network traffic for suspicious activity

C) To encrypt data transmissions

D) To distribute network traffic evenly across servers

Answer: B) To monitor network traffic for suspicious activity

13. Which network security appliance is designed to prevent unauthorized access to a network while allowing legitimate traffic?

A) Firewall

B) Intrusion Detection System (IDS)

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: A) Firewall

14. What is the primary purpose of network security monitoring?

A) To encrypt data transmissions

B) To detect and respond to security incidents

C) To distribute network traffic evenly across servers

D) To manage network devices

Answer: B) To detect and respond to security incidents

15. Which network security appliance is used to balance traffic load across multiple servers to ensure optimal performance?

A) Firewall

B) Intrusion Prevention System (IPS)

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: D) Load Balancer

16. What is the primary role of a security information and event management (SIEM) system?

A) To prevent DDoS attacks

B) To monitor and analyze security events across the network

C) To encrypt network traffic

D) To manage authentication credentials

Answer: B) To monitor and analyze security events across the network

17. Which network security appliance is used to inspect network traffic for known vulnerabilities and exploits?

A) Firewall

B) Intrusion Prevention System (IPS)

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: B) Intrusion Prevention System (IPS)

18. What is the primary purpose of deep packet inspection (DPI) in network security?

A) To analyze and filter network traffic based on application content

B) To distribute network traffic evenly across servers

C) To encrypt data transmissions

D) To manage network devices

Answer: A) To analyze and filter network traffic based on application content

19. Which network security appliance is used to cache frequently accessed web content to improve performance and reduce bandwidth usage?

A) Firewall

B) Intrusion Detection System (IDS)

C) Proxy Server

D) Load Balancer

Answer: C) Proxy Server

20. What is the primary role of a security operations center (SOC) in network security?

A) To manage network devices

B) To monitor and respond to security incidents

C) To encrypt network traffic

D) To balance network traffic load

Answer: B) To monitor and respond to security incidents

21. Which network security appliance inspects incoming and outgoing network traffic based on a defined set of rules?

A) Firewall

B) Intrusion Prevention System (IPS)

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: A) Firewall

22. What is the primary role of network segmentation in secure network designs?

A) To encrypt data transmissions

B) To isolate sensitive resources from the rest of the network

C) To distribute network traffic evenly across servers

D) To manage network devices

Answer: B) To isolate sensitive resources from the rest of the network

23. Which network security appliance is used to detect and mitigate distributed denial-of-service (DDoS) attacks?

A) Firewall

B) Intrusion Prevention System (IPS)

C) SIEM (Security Information and Event Management)

D

) Load Balancer

Answer: B) Intrusion Prevention System (IPS)

24. What is the primary purpose of network address translation (NAT) in network security?

A) To encrypt data transmissions

B) To monitor and analyze security events

C) To translate private IP addresses to public IP addresses

D) To manage authentication credentials

Answer: C) To translate private IP addresses to public IP addresses

25. Which network security appliance is used to monitor and analyze network traffic for security events?

A) Firewall

B) Intrusion Detection System (IDS)

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: C) SIEM (Security Information and Event Management)

26. What is the primary purpose of a virtual private network (VPN) in network security?

A) To encrypt data transmissions over an insecure network

B) To distribute network traffic evenly across servers

C) To manage network devices

D) To prevent unauthorized access to the network

Answer: A) To encrypt data transmissions over an insecure network

27. Which network security appliance is used to authenticate and authorize users accessing a network remotely?

A) Firewall

B) VPN Concentrator

C) SIEM (Security Information and Event Management)

D) Load Balancer

Answer: B) VPN Concentrator

28. What is the primary role of network access control (NAC) in network security?

A) To monitor network traffic for security events

B) To authenticate and authorize devices connecting to the network

C) To manage network devices

D) To distribute network traffic evenly across servers

Answer: B) To authenticate and authorize devices connecting to the network

29. Which network security appliance is used to filter and inspect web traffic for malicious content and threats?

A) Firewall

B) Intrusion Prevention System (IPS)

C) Web Application Firewall (WAF)

D) Load Balancer

Answer: C) Web Application Firewall (WAF)

30. What is the primary purpose of a distributed denial-of-service (DDoS) mitigation appliance?

A) To encrypt data transmissions

B) To balance network traffic load

C) To detect and mitigate DDoS attacks targeting a network

D) To manage authentication credentials

Answer: C) To detect and mitigate DDoS attacks targeting a network

Unit – 4

Certainly! Here are 30 multiple-choice questions (MCQs) on various aspects of cybersecurity essential topics related to secure mobile solutions, secure application concepts, and data privacy and protection concepts, along with their answers:

1. What is the primary purpose of mobile device management (MDM) in cybersecurity?

A) To block all mobile device connections

B) To encrypt all mobile data transmissions

C) To remotely manage and secure mobile devices

D) To monitor mobile device battery levels

Answer: C) To remotely manage and secure mobile devices

2. Which secure mobile device connection protocol encrypts data transmitted between a mobile device and a server?

A) HTTP (Hypertext Transfer Protocol)

B) FTP (File Transfer Protocol)

C) SSH (Secure Shell)

D) Bluetooth

Answer: C) SSH (Secure Shell)

3. What are common indicators of application attacks?

A) Unusual network traffic patterns

B) Sudden increase in server load

C) Unexpected changes in application behavior

D) All of the above

Answer: D) All of the above

4. Which secure coding practice helps prevent SQL injection attacks?

A) Using input validation and parameterized queries

B) Storing sensitive data in plain text

C) Allowing unrestricted file uploads

D) Using weak encryption algorithms

Answer: A) Using input validation and parameterized queries

5. Which deployment concept automates the process of software deployment and configuration?

A) Continuous Integration (CI)

B) Agile Development

C) Waterfall Model

D) Spiral Model

Answer: A) Continuous Integration (CI)

6. What is the primary purpose of secure script environments?

A) To execute scripts without any restrictions

B) To provide a controlled environment for script execution

C) To allow scripts to access sensitive data

D) To increase script performance

Answer: B) To provide a controlled environment for script execution

7. What are common indicators of web application attacks?

A) Unusual user behavior patterns

B) Unexpected HTTP error codes

C) Presence of malicious scripts or code injections

D) All of the above

Answer: D) All of the above

8. Which data protection control ensures that only authorized individuals have access to sensitive data?

A) Encryption

B) Access Control

C) Data Masking

D) All of the above

Answer: B) Access Control

9. What is the primary purpose of privacy and data sensitivity concepts in cybersecurity?

A) To limit access to non-sensitive data only

B) To ensure compliance with privacy regulations

C) To collect as much user data as possible

D) To share data openly with third parties

Answer: B) To ensure compliance with privacy regulations

10. Which deployment concept emphasizes incremental and iterative development cycles?

A) Waterfall Model

B) Spiral Model

C) Agile Development

D) Rapid Application Development (RAD)

Answer: C) Agile Development

11. What is the primary purpose of data masking?

A) To encrypt sensitive data during transmission

B) To hide or obfuscate sensitive data in non-production environments

C) To authenticate users accessing sensitive data

D) To restrict access to sensitive data based on user roles

Answer: B) To hide or obfuscate sensitive data in non-production environments

12. Which deployment concept focuses on gathering user feedback and adapting to changing requirements?

A) Waterfall Model

B) Spiral Model

C) Agile Development

D) Rapid Application Development (RAD)

Answer: C) Agile Development

13. Which secure coding practice helps prevent cross-site scripting (XSS) attacks?

A) Encoding user input before rendering it in HTML

B) Storing sensitive data in plain text

C) Using weak passwords for authentication

D) Allowing unrestricted file uploads

Answer: A) Encoding user input before rendering it in HTML

14. What is the primary purpose of secure mobile device connections?

A) To transmit data without encryption

B) To prevent mobile devices from connecting to the internet

C) To ensure data confidentiality and integrity during transmission

D) To allow unrestricted access to mobile devices

Answer: C) To ensure data confidentiality and integrity during transmission

15. Which privacy and data sensitivity concept involves minimizing the collection of unnecessary user data?

A) Data Encryption

B) Data Minimization

C) Data Masking

D) Data Retention

Answer: B) Data Minimization

16. Which secure coding practice helps prevent buffer overflow attacks?

A) Using strong encryption algorithms

B) Limiting input length and validating input data

C) Ignoring input validation checks

D) Storing passwords in plain text

Answer: B) Limiting input length and validating input data

17. What is the primary purpose of deploying a secure script environment?

A) To execute scripts without any restrictions

B) To provide a controlled environment for script execution

C) To allow scripts to access sensitive data

D) To increase script performance

Answer: B) To provide a controlled environment for script execution

18. Which data privacy and protection control involves converting sensitive data into unreadable format?

A) Data Encryption

B) Access Control

C) Data Masking

D) Data Minimization

Answer: A) Data Encryption

19. Which deployment concept involves deploying software updates and patches continuously?

A) Waterfall Model

B) Spiral Model

C) Agile Development

D) Continuous Deployment

Answer: D) Continuous Deployment

20. What is the primary purpose of privacy and data protection controls in cybersecurity?

A) To collect as much user data as possible

B) To ensure compliance with privacy regulations and protect sensitive data

C) To share data openly with third parties

D) To restrict access to non-sensitive data only

Answer: B) To ensure compliance with privacy regulations and protect sensitive data

21. Which secure coding practice helps prevent injection attacks like SQL injection and command injection?

A) Using weak passwords for authentication

B) Using prepared statements with parameterized queries

C) Allowing unrestricted file uploads

D) Ignoring input validation checks

Answer: B) Using prepared statements with parameterized queries

22. What is the primary purpose of secure application concepts in cybersecurity?

A) To encourage the development of vulnerable applications

B) To protect applications from security vulnerabilities and attacks

C) To store sensitive data in plain text

D) To allow unrestricted access to application data

Answer: B) To protect applications from security vulnerabilities and attacks

23. Which deployment concept involves iterative development cycles with regular feedback from stakeholders?

A) Waterfall Model

B) Spiral Model

C) Agile Development

D) Rapid Application Development (RAD)

Answer: C) Agile Development

24. Which secure coding practice helps prevent authentication and session management attacks?

A) Storing session tokens in plain text

B) Using

weak encryption algorithms

C) Implementing secure session management mechanisms

D) Allowing unrestricted access to sensitive resources

Answer: C) Implementing secure session management mechanisms

25. What is the primary purpose of data privacy and protection concepts in cybersecurity?

A) To maximize the collection of user data

B) To ensure transparency in data handling practices

C) To restrict access to non-sensitive data only

D) To ignore privacy regulations

Answer: B) To ensure transparency in data handling practices

26. Which secure coding practice helps prevent insecure direct object references?

A) Using strong encryption algorithms

B) Implementing access controls and authorization checks

C) Ignoring input validation checks

D) Allowing unrestricted file uploads

Answer: B) Implementing access controls and authorization checks

27. What is the primary purpose of privacy and data sensitivity concepts in cybersecurity?

A) To allow unrestricted access to sensitive data

B) To maximize data collection without user consent

C) To protect the privacy and confidentiality of user data

D) To ignore data handling regulations

Answer: C) To protect the privacy and confidentiality of user data

28. Which deployment concept emphasizes delivering software in short, rapid cycles?

A) Waterfall Model

B) Spiral Model

C) Agile Development

D) Rapid Application Development (RAD)

Answer: C) Agile Development

29. Which secure coding practice helps prevent cross-site request forgery (CSRF) attacks?

A) Using weak authentication mechanisms

B) Implementing anti-CSRF tokens in web forms

C) Ignoring input validation checks

D) Allowing unrestricted file uploads

Answer: B) Implementing anti-CSRF tokens in web forms

30. What is the primary purpose of secure mobile solutions in cybersecurity?

A) To maximize mobile device vulnerabilities

B) To ensure data security and privacy on mobile devices

C) To encourage unrestricted mobile device connections

D) To ignore mobile security regulations

Answer: B) To ensure data security and privacy on mobile devices

Unit – 5

1. What is the primary goal of incident response procedures in cybersecurity?

A) To prevent all security incidents

B) To quickly detect and respond to security incidents

C) To ignore security incidents until they become critical

D) To assign blame for security incidents

Answer: B) To quickly detect and respond to security incidents

2. Which of the following is an appropriate data source for incident response?

A) Social media feeds

B) Security logs and event records

C) Public forums

D) Personal email accounts

Answer: B) Security logs and event records

3. What is the purpose of applying mitigation controls during incident response?

A) To ignore the incident and hope it goes away

B) To worsen the impact of the incident

C) To minimize the impact and prevent further damage

D) To blame other departments for the incident

Answer: C) To minimize the impact and prevent further damage

4. Which redundancy strategy is used to ensure continuous availability of critical systems?

A) Data replication

B) Data obfuscation

C) Data encryption

D) Data compression

Answer: A) Data replication

5. What is the primary purpose of implementing backup strategies in cybersecurity?

A) To complicate incident response procedures

B) To decrease the organization's data storage costs

C) To ensure data availability and recovery in case of incidents

D) To make it easier for attackers to access sensitive data

Answer: C) To ensure data availability and recovery in case of incidents

6. Which physical site security control is designed to prevent unauthorized access to physical facilities?

A) Intrusion Detection Systems (IDS)

B) Biometric authentication systems

C) Firewall appliances

D) Network firewalls

Answer: B) Biometric authentication systems

7. What is the primary goal of cyber security resilience strategies?

A) To make cyber security incidents more frequent

B) To increase the organization's vulnerability to cyber attacks

C) To improve the organization's ability to withstand and recover from cyber attacks

D) To blame external factors for cyber security incidents

Answer: C) To improve the organization's ability to withstand and recover from cyber attacks

8. Which physical host security control helps prevent unauthorized access to individual computing devices?

A) Data encryption

B) Password policies

C) Firewall rules

D) Cable locks

Answer: D) Cable locks

9. What is the primary purpose of redundancy strategies in cybersecurity?

A) To decrease system availability

B) To complicate incident response procedures

C) To ensure continuous availability of critical systems

D) To increase the organization's data storage costs

Answer: C) To ensure continuous availability of critical systems

10. Which backup strategy involves creating exact copies of data in real-time?

A) Incremental backup

B) Differential backup

C) Full backup

D) Continuous data protection

Answer: D) Continuous data protection

11. What is the primary purpose of physical site security controls?

A) To allow unrestricted access to physical facilities

B) To prevent unauthorized access to physical facilities

C) To increase the likelihood of cyber attacks

D) To complicate incident response procedures

Answer: B) To prevent unauthorized access to physical facilities

12. Which redundancy strategy involves using multiple internet service providers (ISPs) to ensure network connectivity?

A) Data replication

B) Network load balancing

C) Geographical redundancy

D) Redundant power supplies

Answer: B) Network load balancing

13. What is the primary purpose of implementing backup strategies?

A) To increase data storage costs

B) To make incident response procedures more complex

C) To ensure data availability and recovery in case of incidents

D) To decrease system availability

Answer: C) To ensure data availability and recovery in case of incidents

14. Which redundancy strategy involves storing data in multiple geographic locations?

A) Data replication

B) Network load balancing

C) Geographical redundancy

D) Redundant power supplies

Answer: C) Geographical redundancy

15. What is the primary purpose of cyber security resilience strategies?

A) To decrease the organization's ability to recover from cyber attacks

B) To increase the likelihood of cyber attacks

C) To improve the organization's ability to withstand and recover from cyber attacks

D) To blame internal factors for cyber security incidents

Answer: C) To improve the organization's ability to withstand and recover from cyber attacks

16. Which physical host security control involves limiting physical access to authorized personnel only?

A) Data encryption

B) Cable locks

C) Password policies

D) Biometric authentication systems

Answer: D) Biometric authentication systems

17. What is the primary purpose of implementing physical site security controls?

A) To increase the likelihood of physical breaches

B) To prevent unauthorized access to physical facilities

C) To complicate incident response procedures

D) To decrease system availability

Answer: B) To prevent unauthorized access to physical facilities

18. Which redundancy strategy involves having duplicate power sources to ensure continuous operation?

A) Data replication

B) Network load balancing

C) Geographical redundancy

D) Redundant power supplies

Answer: D) Redundant power supplies

19. What is the primary goal of incident response procedures?

A) To ignore security incidents until they become critical

B) To assign blame for security incidents

C) To quickly detect and respond to security incidents

D) To prevent all security incidents

Answer: C) To quickly detect and respond to security incidents

20. Which data source is not typically utilized for incident response?

A) Security logs and event records

B) Personal email accounts

C) Network traffic logs

D) Intrusion Detection System (IDS) alerts

Answer: B) Personal email accounts

21. What is the primary objective of applying mitigation controls during incident response?

A) To ignore the incident and hope it goes away

B) To worsen the impact of the incident

C) To minimize the impact and prevent further damage

D) To blame other departments for the incident

Answer: C) To minimize the impact and prevent further damage

22. Which redundancy strategy is used to ensure continuous availability of critical systems in different geographic locations?

A) Data replication

B) Network load balancing

C) Geographical redundancy

D) Redundant power supplies

Answer: C) Geographical redundancy

23. What is the primary purpose of cyber security resilience strategies?

A) To make cyber security incidents more frequent

B) To increase the organization's vulnerability to cyber attacks

C) To improve the organization's ability to withstand and recover from cyber attacks

D) To blame external factors for cyber security incidents

**Answer: C

Unit – 6

1. What is the primary objective of network security programming?

A) Data encryption

B) Prevention of unauthorized access

C) Software updates

D) Network monitoring

Answer: B) Prevention of unauthorized access

2. Which operating systems can Python be used on for network security programming?

A) Linux and macOS only

B) Windows only

C) Linux, macOS, and Windows

D) Linux only

Answer: C) Linux, macOS, and Windows

3. Which term refers to the fundamental unit of data transmission in computer networks?

A) Packet

B) Protocol

C) Socket

D) IP Address

Answer: A) Packet

4. In Python, what is the purpose of raw sockets?

A) To create encrypted connections

B) To bypass network security protocols

C) To access network interfaces at a low level

D) To increase network bandwidth

Answer: C) To access network interfaces at a low level

5. Which Python library is commonly used for socket programming?

A) PyCrypto

B) Requests

C) SocketIO

D) socket

Answer: D) socket

6. What functionality does the socket library provide in Python?

A) HTTP request handling

B) Sending and receiving data over network connections

C) GUI development

D) File manipulation

Answer: B) Sending and receiving data over network connections

7. What is the role of a server in client-server architecture?

A) Receives requests and sends responses

B) Initiates connections to clients

C) Executes client-side scripts

D) None of the above

Answer: A) Receives requests and sends responses

8. Which programming concept is essential for creating a port scanner in Python?

A) Multi-threading

B) Object-oriented programming

C) Recursion

D) Exception handling

Answer: A) Multi-threading

9. How does a port scanner program identify open ports on a target system?

A) By sending SYN packets and analyzing responses

B) By brute-forcing login credentials

C) By pinging the target system

D) By decrypting network traffic

Answer: A) By sending SYN packets and analyzing responses

10. What is the purpose of identifying live hosts over a network using Python?

A) To detect network vulnerabilities

B) To enumerate installed software

C) To determine network bandwidth

D) To perform load balancing

Answer: A) To detect network vulnerabilities

11. Which technique is commonly used to create a backdoor using Python?

A) Cross-site scripting

B) Remote code execution

C) SQL injection

D) Input validation

Answer: B) Remote code execution

12. What is the main functionality of a web crawler program in Python?

A) Extracting data from websites

B) Performing denial of service attacks

C) Encrypting web traffic

D) None of the above

Answer: A) Extracting data from websites

13. What is the purpose of a wireless packet sniffer in Python?

A) To encrypt wireless network traffic

B) To analyze and capture wireless network packets

C) To authenticate wireless clients

D) To establish secure connections

Answer: B) To analyze and capture wireless network packets

14. Which of the following is not a common security concern in network programming?

A) Man-in-the-middle attacks

B) Distributed denial of service (DDoS) attacks

C) Buffer overflows

D) Data compression

Answer: D) Data compression

15. Which Python module is used for creating HTTP servers?

A) http.server

B) socketserver

C) requests

D) urllib

Answer: A) http.server

16. What is the purpose of using encryption in network security programming?

A) To hide network traffic

B) To prevent unauthorized access

C) To compress data packets

D) To increase network speed

Answer: B) To prevent unauthorized access

17. Which Python module is used for handling JSON data?

A) jsonlib

B) jsonpickle

C) json

D) jsonparse

Answer: C) json

18. Which of the following is NOT a type of cyber attack?

A) SQL Injection

B) Algorithm

C) Phishing

D) Ransomware

Answer: B) Algorithm

19. Which of the following is NOT a commonly used encryption algorithm?

A) AES

B) RSA

C) MD5

D) ZIP

Answer: D) ZIP

20. What is the purpose of a salt in password hashing?

A) To add flavor to passwords

B) To enhance password security

C) To make passwords more memorable

D) To decrypt passwords

Answer: B) To enhance password security

21. Which of the following is NOT a security best practice for handling passwords?

A) Storing passwords in plaintext

B) Using a strong hashing algorithm

C) Implementing multi-factor authentication

D) Regularly updating passwords

Answer: A) Storing passwords in plaintext

22. What is the purpose of a firewall in network security?

A) To block unauthorized access to a network

B) To speed up network traffic

C) To encrypt data packets

D) To monitor network bandwidth

Answer: A) To block unauthorized access to a network

23. What is the primary function of an intrusion detection system (IDS)?

A) To prevent all cyber attacks

B) To detect and respond to cyber threats

C) To encrypt network traffic

D) To manage network resources

Answer: B) To detect and respond to cyber threats

24. What is the purpose of penetration testing in cybersecurity?

A) To encrypt sensitive data

B) To identify vulnerabilities in a system

C) To authenticate users

D) To manage network traffic

Answer: B) To identify vulnerabilities in a system

25. What is the difference between symmetric and asymmetric encryption?

A) Symmetric encryption uses a single key, while asymmetric encryption uses two keys.

B) Asymmetric encryption is faster than symmetric encryption.

C) Symmetric encryption is only used for text data, while asymmetric encryption is used for multimedia.

D) Asymmetric encryption is more secure than symmetric encryption.

Answer: A) Symmetric encryption uses a single key, while asymmetric encryption uses two keys.

26. Which cryptographic protocol is commonly used for securing web traffic?

A) SSH

B) HTTPS

C) FTPS

D) SFTP

Answer: B) HTTPS

27. Which of the following is NOT a common social engineering technique?

A) Phishing

B) Shoulder surfing

C) Firewall bypass

D) Impersonation

Answer: C) Firewall bypass

28. Which of the following is a type of malware that encrypts files and demands payment for decryption?

A) Trojan horse

B) Worm

C) Ransomware

D) Spyware

Answer: C) Ransomware

29. What is the purpose of a Virtual Private Network (VPN)?

A) To increase network speed

B) To provide secure remote access to a private network

C) To block access to certain websites

D) To compress network traffic

Answer: B) To provide secure remote access to a private network

30. What is the role of a Certificate Authority (CA) in the context of SSL/TLS?

A) To encrypt network traffic

B) To issue digital certificates to verify the identity of websites

C) To manage network resources

D) To authenticate users

Answer: B) To issue digital certificates to verify the identity of websites