TROY UNIVERSITY

COMPUTER SECURITY

CODE 04

MIDTERM QUIZ INFORMATION SECURITY

Time: 60 minutes

Question 1. A user enters a username to claim an identity. Which IAAA element is this?

A. Identification
B. Authentication
C. Authorization
D. Accounting

Question 2. Malware modifies the content of important files. Which CIA element is directly affected?

A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Question 3. In threat classification by impact, eavesdropping is an example of a:

A. Passive threat
B. Active threat
C. Corrective threat
D. Directive threat

Question 4. Organized cybercrime is usually motivated by:

A. Financial gain
B. Academic grading
C. User convenience
D. System usability

Question 5. Open-source supply chain infection occurs when:

A. Malicious code is inserted into an open-source project or dependency
B. A user enables MFA
C. Data is properly encrypted
D. Logs are stored correctly

Question 6. Data exfiltration means:

A. Destroying data so it cannot be recovered
B. Stealing data and transferring it to another party
C. Improving data access speed
D. Performing a legitimate backup

Question 7. The Kill Chain Model focuses on:

A. The stages of an attack from reconnaissance to final objectives
B. User interface design
C. Operating system permissions only
D. Classroom attendance scoring

Question 8. Complete Mediation in access control requires that:

A. Every access to every object should be checked
B. Only the first login should be checked

C. Administrators should never be checked
D. Users should define their own permissions

Question 9. Which of the following is a preventive control?

A. Firewall and strong authentication
B. Log monitoring
C. Backup restoration
D. User guidelines

Question 10. Regulatory compliance means:

A. The process of following relevant rules, regulations, or legal requirements
B. The process of deleting all old data
C. A type of cyberattack
D. A type of botnet

Question 11. Which IAM objective focuses on creating, maintaining, and deleting user identities?

A. Manage User Identities
B. Disable Authentication
C. Remove Access Control
D. Ignore Compliance

Question 12. Which authentication factor uses typing rhythm or mouse movement?

A. Something you know
B. Behavioral characteristics
C. Something you have
D. Plaintext password

Question 13. Which of the following is a disadvantage of biometric authentication?

A. It can change over time due to age or physical conditions
B. It is always free to deploy
C. It never requires hardware or sensors
D. It never has privacy concerns

Question 14. Account lockout or rate limiting helps protect against:

A. Unlimited password guessing attempts
B. Proper password hashing
C. Strong password generation
D. Secure password reset links

Question 15. What is the role of a pepper in password protection?

A. A public value stored with every user record
B. A secret value added to password hashing and stored separately
C. A replacement for all authentication factors
D. A user’s email address

Question 16. Which access control model is usually the most restrictive?

A. DAC
B. MAC
C. RBAC
D. Rule-Based Access Control

Question 17. In the Bell-LaPadula model, “No Read Up” means:

A. A lower-level subject cannot read a higher-level object
B. A higher-level subject cannot read a lower-level object
C. A subject cannot write any file
D. A subject can read everything

Question 18. Separation of Duties is designed to:

A. Allow one person to complete all critical transactions alone
B. Divide high-risk processes among multiple people
C. Remove audit trails
D. Give all users administrator rights

Question 19. Privileged Access Management focuses on protecting:

A. Ordinary files only
B. High-risk accounts such as administrators, root, or database admins
C. Public websites only
D. Guest Wi-Fi passwords only

Question 20. SAML 2.0 commonly uses which format to exchange authentication and authorization data?

A. XML
B. Plain text only
C. JPEG
D. CSV

Question 21. A stream cipher encrypts data:

A. One bit or character at a time
B. Only in 1 GB blocks
C. Only after creating a certificate
D. Only through a VPN

Question 22. A block cipher encrypts data:

A. By hiding it in unused file space
B. In fixed-size blocks
C. Without using any key
D. Only by using public certificates

Question 23. Which of the following is a common block cipher mode of operation?

A. CBC
B. DNS
C. HTML
D. SMTP

Question 24. What is Transparent Data Encryption mainly used for?

A. Encrypting and decrypting directly within the database engine
B. Signing mobile applications
C. Creating a VPN tunnel
D. Replacing all digital certificates

Question 25. A self-encrypting drive is an example of:

A. Hardware encryption
B. Metadata injection
C. A trust model
D. A downgrade attack

Question 26. What is the “zero-knowledge” principle in cloud encryption?

A. The cloud provider and encryption service cannot access the user's files
B. Everyone can read the encrypted data
C. The encryption key is stored publicly
D. The user does not need any key

Question 27. A standard hash used alone as an integrity check can fail because an attacker may:

A. Modify the message and recompute a new hash
B. Never see the message
C. Be unable to calculate any hash
D. Only attack hardware devices

Question 28. A MAC improves integrity checking by including:

A. A secret key
B. A public social media account
C. A larger file name
D. A digital camera

Question 29. A downgrade attack forces a system to:

A. Use weaker or older security protocols
B. Use stronger encryption
C. Delete its private key securely
D. Generate a certificate chain

Question 30. Post-quantum cryptography is designed to resist attacks from:

A. Quantum computers
B. USB drives
C. Acoustic leakage
D. Social media accounts

Question 31. Which malware category uses the infected host as a base to attack others?

A. Kidnap
B. Eavesdrop
C. Launch
D. Recovery

Question 32. A virus usually requires:

A. A host file to live in
B. A certificate authority
C. A secure cookie
D. A sandbox only

Question 33. In a botnet, the attacker who controls the network is called the:

A. Bot herder
B. Verifier
C. Patch manager
D. Cookie owner

Question 34. Command & Control infrastructure is used to:

A. Send instructions to infected zombie computers
B. Validate user input
C. Encrypt browser cookies
D. Restore a frozen system

Question 35. Vertical privilege escalation means:

A. Gaining higher-level permissions, such as user to administrator
B. Accessing another user's resources at the same permission level
C. Deleting browser history
D. Scanning files with antivirus

Question 36. Horizontal privilege escalation means:

A. Gaining access to another user's resources at the same privilege level
B. Becoming a root administrator
C. Encrypting all files
D. Blocking all network ports

Question 37. SSRF abuses a server's ability to:

A. Make requests to internal or unintended resources
B. Capture keystrokes
C. Encrypt the local disk
D. Generate antivirus signatures

Question 38. A replay attack involves:

A. Reusing intercepted communications later to impersonate a legitimate user
B. Installing software updates
C. Running a program in a sandbox
D. Checking file signatures

Question 39. HIDS mainly functions like a:

A. Security camera that monitors logs, file integrity, and suspicious activity
B. Physical door lock
C. Password manager
D. File compression tool

Question 40. Hardening endpoints means:

A. Reducing the system's attack surface and vulnerabilities
B. Installing all possible software
C. Allowing every port and protocol
D. Disabling all security tools

Question 41. Unauthorized information access occurs when a user:

A. Views sensitive data without the required "Need to Know" permission
B. Updates antivirus signatures
C. Uses a secure VPN
D. Applies router hardening

Question 42. Packet sniffing is used to:

A. Create VLANs
B. Block all traffic automatically
C. Capture network traffic for analysis
D. Remove unnecessary software

Question 43. A router can use ACLs to:

A. Replace all switches
B. Filter traffic based on IP addresses, ports, or protocols
C. Store website categories
D. Create honeynets

Question 44. A load balancer improves security partly because it can:

A. Disable all user accounts
B. Replace endpoint monitoring

C. Remove DNS entirely
D. Help detect and stop some attacks directed at servers or applications

---

Question 45. A reverse proxy mainly acts on behalf of:

A. Internal servers receiving requests from the Internet
B. Internal users visiting external websites
C. Personal laptops only
D. DNS clients only

Question 46. An IDS is different from an IPS because an IDS:

A. Blocks attacks inline by default
B. Deletes malicious packets automatically
C. Primarily alerts administrators about suspicious activity
D. Replaces the firewall entirely

Question 47. A honeynet is:

A. A single endpoint antivirus tool
B. A VLAN tagging protocol
C. A DNS resolver blocklist
D. Multiple honeypots linked together to simulate a network

Question 48. Web filtering can be based on:

A. Only physical cable length
B. Browser scanning, agent-based scanning, centralized proxy scanning, or cloud scanning
C. Only keyboard input
D. Only hard drive encryption