TROY UNIVERSITY

COMPUTER SECURITY

CODE 03

MIDTERM QUIZ INFORMATION SECURITY

Time: 60 minutes

Question 1. Availability in the CIA Triad means that:

A. Data must not be viewed by unauthorized users
B. Systems and information must be accessible to authorized users when needed
C. Users do not need authentication
D. Data does not need backups

Question 2. In the CNSS/McCumber Cube, “Technology, Policy & Procedures, Education & Awareness” belong to which dimension?

A. Security Goals
B. Information States
C. Security Measures
D. Threat Actors

Question 3. Poor security awareness is best described as a:

A. Weakness
B. Threat
C. Security asset
D. Cryptographic method

Question 4. A DoS or DDoS attack mainly affects which CIA element?

A. Confidentiality
B. Availability
C. Identification
D. Non-repudiation

Question 5. Hacktivists are usually motivated by:

A. Ideology, beliefs, or political/social causes
B. System maintenance
C. Data backup
D. Performance optimization

Question 6. An attack surface is:

A. A channel, platform, or entry point that attackers may target
B. A security patch
C. A human resource policy
D. An offline backup

Question 7. A zero-day vulnerability is dangerous because it:

A. Has already been patched for years
B. May be exploited before public knowledge or available fixes
C. Only affects printed documents
D. Cannot cause damage

Question 8. LINDDUN is most suitable for analyzing:

A. Privacy risks in systems handling personal data
B. CPU speed problems

C. Systems with no users
D. File naming conventions

Question 9. Fail-safe defaults usually recommend that systems should:

A. Allow all access when an error occurs
B. Deny by default and allow only explicitly permitted access
C. Disable all logging
D. Skip security checks

Question 10. Which of the following is an example of a directive control?

A. Security policies and user guidelines
B. IDS alerts
C. Backup restoration
D. Firewall filtering

Question 11. Which of the following is a core component of IAM?

A. Identity Management
B. Video editing
C. Graphic design
D. File compression only

Question 12. Which of the following is an identifier?

A. Username
B. Firewall rule
C. Encryption key length
D. Audit policy

Question 13. Multi-Factor Authentication requires:

A. Two or more forms of verification
B. Only one password
C. Only one username
D. No identity verification

Question 14. A One-Time Password is:

A. A password reused for many years
B. A unique password valid for a single login session or transaction
C. A password stored in plaintext
D. A password that never expires

Question 15. What is the main principle for password recovery mechanisms?

A. Recovery should be weaker than login authentication
B. Recovery should not be weaker than the authentication mechanism
C. Recovery should always send plaintext passwords by email
D. Recovery should never notify users

Question 16. An Access Control List stores permissions primarily by:

A. Object
B. Weather condition
C. Password age
D. Biometric trait

Question 17. A capability list stores permissions primarily by:

A. Subject
B. Data center temperature
C. Password complexity
D. Encryption algorithm only

Question 18. The Biba model mainly protects:

A. Confidentiality
B. Integrity
C. Availability
D. Password length

Question 19. Which model is most flexible and can combine attributes such as role, location, time, and device?

A. DAC
B. MAC
C. ABAC
D. Bell-LaPadula

Question 20. What does log integrity mean?

A. Logs should be easy for attackers to delete
B. Logs should be protected from tampering
C. Logs should never be collected
D. Logs should only store usernames

Question 21. A substitution cipher works by:

A. Rearranging the positions of letters only
B. Replacing one character with another based on a rule or key
C. Deleting all vowels from a message
D. Hiding data inside image metadata only

Question 22. A permutation cipher works by:

A. Rearranging characters while keeping the characters themselves the same
B. Replacing every letter with a number
C. Encrypting only hard drives
D. Creating public certificates

Question 23. A secure hash should produce:

A. Variable output length for every input
B. The same fixed-size output regardless of input size
C. The original message after hashing
D. A private key

Question 24. Which statement about hashes is correct?

A. A tiny change in input should produce a very different hash
B. Hashes are designed to be easily reversed
C. Two different files should always have the same hash
D. Hashing requires a public-private key pair

Question 25. Hybrid encryption usually combines:

A. Symmetric encryption speed with asymmetric key exchange/protection
B. Only steganography and compression
C. Only plaintext and cleartext
D. Only hashing and deletion

Question 26. Why are digital signatures usually created from a message digest instead of the full message?

A. To reduce computational overhead and avoid signing large messages directly
B. To remove integrity protection

C. To make the message public
D. To avoid using private keys

Question 27. End-to-end encryption means that plaintext is available:

A. At every intermediate server
B. Only at the sender and receiver endpoints
C. Only at the router
D. Only at the cloud provider

Question 28. IPsec Tunnel Mode encrypts:

A. Only the application password
B. The entire IP packet, including data and headers
C. Only the username
D. Only the file name

Question 29. A collision attack attempts to find:

A. Two different inputs with the same hash result
B. A faster Internet connection
C. A stolen physical key
D. A hidden image file

Question 30. PKI is a framework used to manage:

A. Digital certificates and public keys
B. Only physical locks
C. Only file compression
D. Only password length

Question 31. Which malware type silently monitors browsing, system usage, and personal habits?

A. Spyware
B. Worm
C. Logic bomb
D. Buffer overflow

Question 32. Fileless malware is difficult to detect because it:

A. Operates in RAM or uses trusted system tools instead of files on disk
B. Only appears as a printed document
C. Always has a clear file signature
D. Cannot use PowerShell or WMI

Question 33. Bloatware can be a security risk because it:

A. May contain vulnerabilities or even malicious components
B. Always improves endpoint security
C. Prevents all malware infections
D. Removes unused ports automatically

Question 34. A rootkit is mainly designed to:

A. Hide itself and other malware from users and security tools
B. Encrypt files for backup
C. Block all cookies
D. Validate web input

Question 35. Which is an Indicator of Attack?

A. Impossible travel login
B. Normal scheduled backup

C. Valid software signature
D. Successful patch installation

Question 36. A NULL pointer dereference may cause:

A. A program crash or immediate exit
B. Stronger authentication
C. More secure cookies
D. Automatic encryption

Question 37. A race condition occurs when:

A. Two tasks try to use the same resource at the same time
B. A user enters a strong password
C. A system updates antivirus signatures
D. A browser sends secure cookies over HTTPS

Question 38. CSRF tricks a victim’s browser into:

A. Sending an authenticated request to a trusted site without the user’s intention
B. Encrypting the local hard drive
C. Installing official patches
D. Scanning a USB drive

Question 39. VirusTotal is useful because it:

A. Uses multiple antivirus engines to scan files or URLs
B. Removes the need for all endpoint protection
C. Guarantees that every file is safe
D. Disables browser protections

Question 40. Secure cookies are designed to be sent:

A. Only over HTTPS encrypted requests
B. Only through SMS
C. Only through FTP
D. Only in plaintext HTTP

Question 41. Ping of Death works by sending:

A. A normal DNS query
B. A fake MAC address
C. A VLAN trunk packet
D. An oversized ICMP packet

Question 42. A Teardrop attack causes problems by sending:

A. Valid HTTPS requests only
B. Overlapping IP fragments that the target cannot reassemble properly
C. Secure VPN packets
D. Normal ARP replies

Question 43. In firewall rule actions, “Deny” usually means:

A. Traffic is logged but not stopped
B. Traffic bypasses the firewall
C. Matching traffic is explicitly blocked
D. All traffic is encrypted

Question 44. A Next-Generation Firewall commonly combines traditional firewall functions with:

A. Only password management
B. Only physical access control
C. Only file compression
D. Deep packet inspection, IPS, and application-level inspection

---

Question 45. Unified Threat Management is commonly useful for smaller businesses because it:

A. Requires no security policies at all
B. Combines firewall, antivirus, antispam, and content filtering in one system
C. Only protects one computer
D. Works only as a honeypot

Question 46. DNS filtering blocks access by:

A. Encrypting every webpage
B. Changing VLAN IDs
C. Refusing to resolve malicious or unapproved domains
D. Replacing all web filters

Question 47. In Zero Trust Architecture, the Policy Enforcement Point is responsible for:

A. Writing malware signatures
B. Enforcing the access decision
C. Performing DNS amplification
D. Creating MAC addresses

Question 48. An air-gapped network is:

A. Physically isolated from other networks or the Internet
B. A public guest Wi-Fi network
C. A DNS filter
D. A cloud scanning service

Question 49. L2TP is usually paired with IPsec because L2TP alone:

A. Blocks all malware
B. Performs deep packet inspection
C. Provides web filtering
D. Does not provide encryption or protection by itself

Question 50. A DNS amplification DDoS attack uses open DNS resolvers to:

A. Improve DNS reliability
B. Reduce traffic volume
C. Amplify traffic toward the victim
D. Create VLAN trunks