Exam Code: 312-39

Total Questions: 125

Questions

1) Which principle ensures users only have the permissions necessary for their role?
   A) Separation of duties
   B) Principle of least privilege
   C) Need-to-know
   D) Role aggregation

2) In SIEM, which of the following best describes “normalization”?
   A) Encrypting log data
   B) Converting diverse log formats to a common schema
   C) Aggregating alerts into incidents
   D) Deleting duplicate logs

3) Which TCP flag combination completes the 3-way handshake?
   A) SYN, ACK
   B) FIN, ACK
   C) RST
   D) PSH, URG

4) What’s the primary purpose of a host-based IDS (HIDS)?
   A) Monitor network packets only
   B) Inspect host-level events and integrity (files, registry)
   C) Block DDoS traffic
   D) Replace endpoint antivirus entirely

5) Which hashing algorithm is considered insecure due to collision attacks?
   A) SHA-256
   B) MD5
   C) SHA-3
   D) BLAKE2

6) When investigating Windows systems, which log contains process creation events if enabled?
   A) Application log
   B) Security log (with process creation auditing)
   C) System log
   D) Setup log

7) What is the best definition of “indicator of compromise” (IOC)?
   A) A prevention control
   B) Artifacts or observables that indicate a security breach
   C) A documented policy
   D) A firewall rule

8) Which phase of incident response focuses on preserving evidence and collecting artifacts?
A) Preparation
B) Containment
C) Identification
D) Eradication

9) In threat modeling, which technique enumerates what could go wrong by walking through the attacker's perspective?
A) STRIDE
B) PASTA
C) OWASP Top 10
D) CVSS

10) What does the acronym MITRE ATT&CK; primarily provide?
A) A vulnerability scanner
B) A taxonomy of adversary tactics, techniques, and procedures (TTPs)
C) A firewall vendor
D) Encryption standards

11) Which port is default for HTTPS?
A) 80
B) 443
C) 22
D) 3389

12) In digital forensics, “chain of custody” documents:
A) Who had access to the evidence and when
B) Encryption keys used on the evidence
C) The network topology
D) The vulnerability scanner output

13) Which Windows artifact records the last run executables and some path info (user-specific)?
A) Prefetch files
B) /var/log/messages
C) /etc/passwd
D) binary logs

14) For detecting DNS tunneling, which metric is most useful?
A) High UDP port 53 query volume with long/encoded query names
B) Low TTL on DNS responses
C) High ICMP echo requests
D) Large TCP three-way handshakes

15) In Splunk, what does the search command index= specify?
A) Time range
B) Data source (logical bucket) to search
C) Field extraction rules
D) Alert thresholds

16) Which of the following is a false positive?
A) An actual breach
B) Legitimate activity incorrectly flagged as malicious

C) Confirmed malware
D) Verified data exfiltration

17) What is pivoting in post-exploitation?
A) Shutting down compromised hosts
B) Using a compromised host to reach other network segments
C) Encrypting files for ransom
D) Reloading signatures in antivirus

18) The NIST incident severity that requires immediate enterprise-wide notification is best described as:
A) Low—local impact
B) High—widespread critical impact
C) Informational only
D) Deprecated

19) What does CVE stand for?
A) Common Vulnerabilities and Exposures
B) Critical Vendor Exam
C) Certified Vulnerability Enumeration
D) Common Virus Event

20) Which log source would you query to find VPN connection times for a user?
A) DNS logs
B) VPN concentrator or firewall authentication logs
C) DHCP server logs only
D) Web server access logs

21) What's the main difference between black-box and white-box penetration testing?
A) Tools used
B) Knowledge of internal design: black-box has none, white-box has full details
C) Time required only
D) Black-box is only physical tests

22) Which Linux directory stores system logs by default?
A) /etc/logs
B) /var/log
C) /home/logs
D) /usr/bin/logs

23) Which artifact helps identify user interactive logon on Windows (i.e., GUI login)?
A) Event ID 4624 with Logon Type 2 or 10 (interactive or remote interactive)
B) Event ID 6008 only
C) Task Scheduler logs only
D) Windows Defender events only

24) In network forensics, what does PCAP refer to?
A) Packet capture file format
B) Policy compliance audit protocol
C) Privileged access control policy
D) Port classification analysis program

25) Which attack exploits a race condition in file handling to gain privilege?
A) SQL injection
B) Time-of-check to time-of-use (TOCTOU)
C) Cross-site scripting
D) ARP spoofing

26) What is the main objective of log retention policies?
A) Reduce storage to zero
B) Preserve logs long enough for compliance, investigations, and forensic analysis
C) Delete logs daily automatically
D) Encrypt all logs with the same symmetric key forever

27) Which protocol is used to securely transfer files and provides interactive shell access?
A) FTP
B) SFTP (over SSH)
C) HTTP
D) TFTP

28) Which of the following is a common indicator of ransomware activity?
A) Sudden mass file renaming with unusual extensions and presence of ransom note files
B) Increased DNS queries only
C) Low CPU usage
D) Clean event logs with no changes

29) What does a SIEM correlation rule do?
A) Only archive logs
B) Identify relationships between disparate events to produce alerts
C) Replace endpoint agents
D) Generate SSL certificates

30) When triaging an alert, what’s the FIRST action?
A) Delete logs to hide evidence
B) Validate the alert and determine scope/impact (identify false positives)
C) Reinstall OS
D) Publicly disclose incident

31) Which technique is used to map lateral movement using event logs?
A) Counting opened web pages only
B) Analyzing authentication events across hosts for abnormal patterns
C) Only checking firewall rules
D) Disabling SMB entirely

32) What is YARA commonly used for?
A) Packet capture analysis
B) Writing rules to identify malware by patterns in files/memory
C) Managing certificates
D) DNS resolution

33) Which file system journal artifact can help determine file modification timelines on Linux?
A) /etc/passwd
B) ext4 journal and filesystem metadata (mtime/ctime/atime)
C) Windows Registry

D) Registry hives

34) Which metric in risk assessment measures likelihood and impact?
A) KPI only
B) Risk score derived from probability × impact
C) Uptime
D) Latency

35) Which type of backup is quickest to restore but requires most storage?
A) Incremental
B) Full backup
C) Differential
D) Snapshotless

36) What is a “honeypot” used for in defensive operations?
A) To accelerate production services
B) Deceive and monitor attackers by providing an attractive but isolated target
C) Encrypt data at rest
D) Replace firewalls

37) Which Windows location stores scheduled task definitions?
A) C:\Windows\System32\Tasks and Task Scheduler library (XML)
B) /etc/cron.d
C) /var/spool/cron
D) C:\Windows\Temp only

38) A blind SQL injection means:
A) Attacker retrieves full database schema directly
B) Attacker cannot see query output directly and infers via side effects
C) Database is encrypted
D) Injection is only in logs

39) Which of these is an example of host hardening?
A) Enabling unnecessary services
B) Disabling unused services and applying patches
C) Using default credentials on all systems
D) Disabling logging entirely

40) In a SOC, what is “mean time to detect” (MTTD)?
A) Time to patch a system
B) Average time from compromise to detection
C) Time to hire staff
D) Time to decrypt data

41) What does “defense in depth” mean?
A) Single control for all threats
B) Multiple layered controls across network, host, and application
C) No security controls at all
D) Security through obscurity only

42) Which Windows artifact often holds pre-authentication cached credentials?
A) SAM (Security Account Manager) database (offline)
B) /etc/shadow
C) Lsass.exe dump (in-memory secrets)
D) system32/driver files only

43) SSH brute-force attempts are best detected by:
A) Excessive failed authentication attempts from same IP or user over time
B) Low disk usage
C) Unchanged password policies
D) High GPU usage

44) What is the difference between vulnerability assessment and penetration testing?
A) None—identical
B) Assessment finds and rates vulnerabilities; pentest actively exploits weaknesses to access systems
C) Pentest is only automated scans
D) Assessment is destructive always

45) Which of following best describes a SOCKS proxy used by attackers?
A) DNS server replacement
B) A transport-layer proxy enabling TCP/UDP traffic relay for anonymizing attacker connections
C) A malware family name
D) A Windows service

46) For cloud logs collection, which service provides centralized logging in AWS?
A) Amazon S3 only
B) Amazon CloudWatch Logs and AWS CloudTrail for activity auditing
C) Route 53 only
D) IAM alone

47) What is “pivot” in threat hunting context?
A) Ignoring low-signal alerts
B) Using one observable to expand to related artifacts and hosts to map the attack surface
C) Restarting logs
D) Encrypting hunt data

48) Which of these is a reliable way to detect fileless malware?
A) Only scanning files on disk
B) Monitoring suspicious memory behavior, PowerShell command lines, and parent-child process relationships
C) Rebooting daily
D) Clearing logs regularly

49) In privilege escalation on Windows, exploiting weak service permissions targets:
A) Read-only files only
B) Services that run as SYSTEM with writable binary paths or registry keys
C) Browser cookies only
D) Network printers only

50) Which Nmap flag runs a stealth SYN scan (on privileged port)?
A) -sT
B) -sS
C) -A

D) -O

51) What is the main purpose of anomaly detection in SIEM?
A) Generate random alerts
B) Identify deviations from established baseline behavior that may indicate compromise
C) Replace signature detection entirely
D) Delete old indices

52) Which logging practice makes forensic analysis easier?
A) Storing logs only on the local host without forwarding
B) Centralizing logs to a write-once secure location with synchronized timestamps
C) Overwriting logs weekly
D) Encrypting logs with unknown keys only

53) XSS (cross-site scripting) primarily attacks:
A) Web server file systems only
B) Users by injecting scripts into web pages viewed by victims
C) Network routers only
D) VPN tunnels only

54) Which technique best uncovers insider threat data exfiltration over allowed channels?
A) Ignoring large uploads
B) User behavior analytics (UBA) and DLP policies to detect abnormal data movement patterns
C) Removing email entirely
D) Only using antivirus

55) What is a “memory artifact” useful in forensic analysis?
A) A text file on desktop only
B) Volatile data like process lists, network connections, and loaded DLLs captured from RAM
C) Printer queue entries only
D) Router config snapshots only

56) Which control reduces risk by splitting duties between multiple people?
A) Single sign-on
B) Separation of duties (SoD)
C) Default admin account use
D) Shared credentials

57) Which analysis technique reconstructs the timeline of system events?
A) Static code analysis only
B) Timeline analysis (correlating timestamps from multiple sources)
C) Only checking antivirus logs
D) Random sampling of packets

58) What’s the typical goal of attackers using “living-off-the-land” (LotL) techniques?
A) Use native tools to avoid detection and persist without dropping malware files
B) Only use new zero-day malware
C) Rely on hardware rootkits only
D) Use only external USB devices

59) Which technique helps ensure integrity of log files during forensic collection?
A) Copy files without checksums
B) Compute and record cryptographic hashes (e.g., SHA-256) before and after transfer
C) Edit logs to remove noise
D) Email logs to personal accounts

60) In an incident response runbook, a “playbook” is:
A) Unrelated marketing material
B) A standardized sequence of actions for specific incident types to ensure consistent response
C) A password list
D) A performance benchmark

61) Which of these indicates possible ARP spoofing on a LAN?
A) Stable, single MAC per IP mapping always
B) Multiple MAC addresses seen for the same IP or gratuitous ARP announcements
C) No ARP entries at all
D) Unchanged routing tables only

62) What is the primary risk of using SMBv1 on networks?
A) Faster file transfer
B) Known vulnerabilities (e.g., WannaCry exploited SMBv1) and lack of security features
C) Improved security
D) Lower latency only

63) Which forensic artifact can reveal previously typed commands on Linux?
A) ~/.bash_history
B) Windows Event ID 4624
C) C:\Windows\Temp only
D) /etc/shadow only

64) What’s the best defense against credential stuffing attacks?
A) Disable MFA
B) Enforce MFA, rate-limit login attempts, and detect anomalous IP/logins
C) Store passwords in plain text
D) Reuse weak passwords across users

65) Which of the following is evidence of data staging before exfiltration?
A) Files moved to uncommon directories or compressed archives near exfil times
B) Increased CPU but no file changes
C) Only DNS lookups
D) IR staff inactivity

66) What is the purpose of an EDR (Endpoint Detection & Response) agent?
A) Replace network firewalls only
B) Monitor endpoints for suspicious activities, enable response and isolation
C) Function as a backup engine only
D) Provide only antivirus definitions

67) Which file format is commonly used to share threat intelligence (structured IOCs)?
A) CSV only
B) STIX/TAXII for structured threat intel sharing
C) EXE only

D) PNG only

68) What does the term “persistence” refer to in attacker lifecycle?
A) Initial access only
B) Techniques used to maintain foothold across reboots and time (services, scheduled tasks, registry run keys)
C) Only data exfiltration steps
D) Password resets

69) Which of these is the best method to detect exfiltration over encrypted channels?
A) Ignore encryption and assume safe
B) Look at metadata: volume, timing patterns, destination reputations, and DLP heuristics
C) Only block TLS entirely
D) Only rely on signatures

70) In OSINT for investigations, which source is most useful for resolving IP ownership?
A) WHOIS and RIR databases (ARIN, RIPE)
B) /etc/hosts only
C) Local password files
D) BIOS settings

71) Which cryptographic primitive provides non-repudiation?
A) Symmetric encryption only
B) Digital signatures (asymmetric cryptography)
C) Cleartext passwords
D) Simple checksums

72) Which Windows event indicates a user account was locked out?
A) Event ID 4625 for failed login reasons with lockout info or 4740 for account lockout
B) Event ID 6005 always
C) Event ID 1000 only
D) Event ID 1102 only

73) What is a “false negative” in detection?
A) Benign activity flagged malicious
B) A malicious activity that goes undetected
C) Duplicate alerts
D) An alert that was correctly triaged

74) Which technique is used to persist web shells on compromised web servers?
A) Remove all files
B) Embedding backdoor PHP/ASP scripts in webroot or tampering with .htaccess to route to payloads
C) Only changing DNS servers
D) Using only Windows services

75) What log source is most useful to investigate email-based phishing?
A) Web server only
B) Email gateway/MTAs and mail logs (headers, recipients, sending IPs)
C) DHCP logs only
D) Printer logs only

76) Which action is a priority in containment for a compromised host suspected of data exfiltration?
A) Wipe the disk immediately
B) Isolate the host from the network (but preserve volatile data if needed)
C) Immediately power off without capturing memory
D) Delete all event logs

77) What is the main advantage of forward deployment of sensors (e.g., NetFlow, packet capture) across network segments?
A) Increases single point of failure
B) Better visibility into lateral movement and segmentation bypass attempts
C) Decreases storage needs only
D) Replaces endpoint agents

78) Which of the following is a reliable way to TTP-map a malware sample?
A) Only check file size
B) Perform static analysis (strings, imports) and dynamic analysis (sandbox behavior) to map techniques to ATT&CK;
C) Run it on production without safety
D) Only check filename

79) Which method ensures log timestamps from different devices align for correlation?
A) Random time settings
B) Synchronize clocks using NTP and record timezone details
C) Use local timezone only without sync
D) Disable timestamps entirely

80) Which Windows registry key is commonly abused for persistence at user logon?
A) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B) /etc/init.d only
C) /var/tmp only
D) Boot.ini only

81) What is the principle behind “defanging” indicators in reports?
A) Make IOCs executable
B) Alter IOCs (e.g., 1.2.3[.]4) to prevent accidental activation when sharing intelligence
C) Encrypt IOCs with secret keys
D) Publish raw malware binaries openly

82) For packet capture analysis, which tool provides deep protocol inspectors and GUI?
A) Notepad
B) Wireshark
C) Telnet only
D) FTP client

83) Which of these indicates command-and-control (C2) beaconing behavior?
A) Random one-off connections only
B) Periodic outbound connections to an external host at regular intervals with small payloads
C) Only internal DNS lookups to local DC
D) One-time large download only

84) Which approach best reduces the blast radius of compromised credentials?
A) Use static shared admin credentials everywhere

B) Implement privileged access management (PAM) and session isolation/just-in-time access
C) Only disable logging
D) Increase password re-use

85) Which of the following is true about TLS certificate pinning?
A) It prevents all network attacks always
B) It binds an application to a specific certificate/public key to prevent MitM with rogue certs
C) It disables encryption
D) It’s only used for FTP

86) What’s the primary role of a SOC playbook for malware containment?
A) Provide ad-hoc steps each time with no structure
B) Provide structured steps: isolate host, collect volatile data, analyze, eradicate, and recover
C) Immediately post to social media
D) Destroy all backups

87) Which Linux command shows network connections and associated processes?
A) ls -la
B) ss or netstat -tunap
C) chmod 777 only
D) passwd only

88) Which artifact helps detect scheduled persistence on Linux?
A) crontab entries and systemd unit files
B) Windows Registry only
C) SAM database only
D) %APPDATA% only

89) What is the best initial indicator to suspect supply chain compromise?
A) Unexpected changes/behavior in a vendor-supplied application after an update
B) Same behavior as before updates
C) Only internal caching issues
D) Disk space increase only

90) Which of these is a proactive threat hunting hypothesis example?
A) “All systems are safe”
B) “There are instances of PowerShell-based credential dumping used in our estate”
C) “Never look at logs”
D) “Only check backups”

91) Which control detects abnormal privilege escalation attempts?
A) Application whitelisting only
B) Monitoring changes to privileged group membership and suspicious service/registry modifications
C) Removing logging only
D) Only scanning ports

92) Which Windows event indicates system time was changed?
A) Event ID 4616 (system time change)
B) Event ID 100 only
C) Event ID 6006 only
D) Event ID 1102 only

93) What is the function of a WAF (Web Application Firewall)?
A) Replace OS firewall only
B) Filter and monitor HTTP/S traffic to identify and block web application attacks (e.g., SQLi, XSS)
C) Only speed up web pages
D) Convert HTTP to FTP

94) Which indicator suggests a brute-force SSH attack in logs?
A) Single successful connection only
B) Numerous failed authentication attempts across multiple usernames/IPs in a short time
C) High disk I/O only
D) No authentication attempts at all

95) In threat intelligence, what distinguishes tactical intel from strategic intel?
A) Tactical is long-term; strategic is immediate
B) Tactical focuses on operational indicators and immediate detection, strategic focuses on trends and policy-level implications
C) They are identical always
D) Tactical is only marketing

96) Which method helps identify suspicious PowerShell usage?
A) Disabling PowerShell logging
B) Enabling Module Logging, Script Block Logging, and monitoring parent-child process chains and encoded commands
C) Only scanning for .exe files
D) Only check disk signatures

97) What is the purpose of an “incident post-mortem”?
A) Erase all evidence
B) Analyze causes, actions taken, lessons learned, and update controls/runbooks to prevent recurrence
C) Only assign blame publicly
D) Ignore the incident completely

98) Which artifact is useful to detect lateral movement over SMB?
A) Windows Security Event 4624/4625 (auth events) and SMB session logs (server-side) showing access to remote shares
B) DNS logs only
C) BIOS logs only
D) Printer spool only

99) Which type of analysis is safe to run malware dynamically?
A) On production servers
B) In an isolated sandbox/lab with network containment and monitoring
C) Directly on user laptops
D) On Internet-connected enterprise machines without controls

100) Which metric measures how quickly systems are restored after an incident?
A) MTTD only
B) Mean Time to Recovery (MTTR)
C) CPU utilization only
D) Number of alerts only

101) What is the typical use of NetFlow records in detection?
A) Store user passwords
B) Analyze flow-level metadata (source/dest, volume, ports, timestamps) for unusual traffic patterns
C) Replace file system logs entirely
D) Only for performance tuning

102) Which control helps against supply-side attacks on package managers?
A) Using unauthenticated repos only
B) Enforcing package signing verification and reproducible builds from trusted sources
C) Blindly installing all packages
D) Disabling verification in production

103) Which Windows log indicates firewall policy changes?
A) Event logs in the Security or System channel (Windows Firewall operational logs) and Group Policy change events
B) /var/log/messages only
C) /etc/fstab only
D) Task Scheduler only

104) What is the main function of Data Loss Prevention (DLP) systems?
A) Prevent disk fragmentation only
B) Detect and prevent unauthorized transfer of sensitive data across channels (email, web, removable media)
C) Manage backups only
D) Replace anti-malware engines only

105) Which artifact helps forensic investigators identify USB device history on Windows?
A) Registry entries (USBSTOR), SetupAPI logs, and Windows Event logs about device connection
B) /etc/usb only
C) Browser cookies only
D) DNS cache only

106) What is “credential dumping”?
A) Deleting credentials intentionally
B) Extracting stored credentials/hashes from system memory or files (e.g., LSASS, SAM) for lateral movement
C) Frequent password changes only
D) Backup of passwords only

107) Which detection reduces risk from phishing via email attachments?
A) Disable email scanning
B) Sandboxing attachments, content disarm and reconstruction (CDR), and attachment scanning with detonation in safe environment
C) Allow all attachments without scanning
D) Only check SPF records

108) Which Windows event shows that the system audit policy was changed?
A) Event ID 4719 (System audit policy change)
B) Event ID 4624 only
C) Event ID 6005 only
D) Event ID 7036 only

109) What’s the difference between IDS and IPS?
A) IDS blocks; IPS only monitors

B) IDS detects and alerts; IPS detects and can proactively block traffic inline
C) IDS is only for endpoints, IPS for network only
D) There is no difference

110) Which data element is most reliable as a unique file identifier?
A) File name only
B) Cryptographic hash (SHA-256) of the file contents
C) File size only
D) File creation time only

111) Which protocol is vulnerable to downgrade attacks when not properly configured?
A) Plain HTTP (no encryption) and older TLS versions (e.g., TLS 1.0) if negotiation allows downgrades
B) ICMP only
C) SMTP only
D) FTP in passive mode only

112) Which sign suggests an attacker used scheduled tasks for persistence?
A) No scheduled entries at all
B) Newly created scheduled tasks with unusual triggers or unknown executables, or tasks created around compromise time
C) Only legitimate task entries updated daily
D) Only DNS queries changed

113) Forensic collection of volatile memory should be done:
A) After powering off immediately
B) As soon as possible, before reboot, to capture processes, network connections, and credentials in RAM
C) Never — RAM is useless
D) Only after formatting disk

114) What is a “kill chain” model used for?
A) Only to schedule backups
B) Describe attack stages (reconnaissance to actions on objectives) to plan detections and defenses
C) Encrypt logs automatically
D) Replace patching schedules

115) Which approach improves detection of polymorphic malware?
A) Only rely on static hashes
B) Behavior-based detection, sandboxing, and heuristics rather than static signatures alone
C) Only check filename patterns
D) Only use email filters

116) What is the key benefit of using application allowlisting?
A) It allows any application
B) It restricts execution to approved applications, dramatically reducing unauthorized code execution risk
C) It slows down updates only
D) It removes auditing capabilities

117) Which evidence is critical to prove data exfiltration over HTTP?
A) Only server uptime logs
B) Web proxy logs, packet captures, and timestamps showing large POSTs/uploads to external domains/IPs
C) Only antivirus logs

D) Only DNS cache entries

118) Which Windows process often houses credentials and has been targeted for dumping?
A) explorer.exe only
B) lsass.exe (Local Security Authority Subsystem Service)
C) calc.exe only
D) cmd.exe only

119) What is the main goal of “red team” exercises relative to SOC?
A) To provide only compliance paperwork
B) Simulate realistic attacks to test SOC detection and response capabilities
C) Replace SOC staff entirely
D) Only test physical security doors

120) Which approach should you use when sharing sensitive IOC lists with external parties?
A) Publish raw hashes to public forums immediately
B) Defang indicators, share via secure channels, and apply appropriate access controls and NDAs if needed
C) Email them in plain text to everyone
D) Post them on social media

121) Which of the following is a common sign of credential reuse across services?
A) Unique passwords for each account always
B) Multiple compromised accounts traced back to one plaintext password found in breached data
C) Only one account compromised ever
D) No use of two-factor auth anywhere ever

122) In incident response, what is the role of a “war room”?
A) Place to store archived logs never used
B) Centralized space (virtual/physical) where responders coordinate, communicate, and make decisions during an incident
C) Only for PR announcements
D) A place to destroy evidence

123) Which of the following best detects living-off-the-land persistence using WMI?
A) Only check for file hashes on disk
B) Monitor WMI consumers/subscriptions and abnormal WMI activity along with parent processes creating WMI entries
C) Ignore WMI entirely
D) Reboot systems daily without logging

124) What does the GDPR require related to breach notifications (in general terms)?
A) No requirement to report breaches
B) Notify supervisory authority within 72 hours of becoming aware of a personal data breach (subject to conditions)
C) Publish breaches on social media immediately only
D) Always keep breaches secret indefinitely

125) Which of the following is a defensible step when encountering ransomware in production?
A) Pay ransom without question always
B) Isolate affected systems, preserve backups, collect forensic data, and determine scope before any payment decisions

C) Immediately delete all backups to save space
D) Reboot all systems without investigation

Answer Key

1) B. Principle of least privilege minimizes rights to necessary ones, reducing attack surface.
2) B. Normalization maps heterogeneous logs into a uniform structure for searching and correlation.
3) A. The server responds with SYN+ACK to client SYN; client sends ACK to complete handshake.
4) B. HIDS inspects local events and file/registry integrity for compromises.
5) B. MD5 is vulnerable to collisions and should not be used for integrity/security.
6) B. Security log with auditing (Event ID 4688) records process creation when enabled.
7) B. IOCs (hashes, IPs, filenames) point to potential compromise.
8) B. Containment often includes preserving evidence and controlled collection.
9) A. STRIDE helps identify threats from attacker-centric categories (Spoofing, Tampering, etc.).
10) B. ATT&CK; catalogs TTPs to map detections and red-team scenarios.
11) B. HTTPS uses TCP port 443.
12) A. Chain of custody records handlers and timestamps to maintain evidence integrity.
13) A. Prefetch (on Windows) caches exe run info and can show run counts/timestamps.
14) A. DNS tunneling often sends many encoded/long queries to exfiltrate data.
15) B. index= limits the search to a specific indexed dataset.
16) B. False positive = benign activity mistakenly labeled malicious.
17) B. Pivoting leverages an initial foothold to access otherwise inaccessible systems.
18) B. High-severity incidents cause widespread critical impacts and need immediate escalation.
19) A. CVE is the standard identifier for publicly known vulnerabilities.
20) B. VPN/authentication logs contain session start/end and user details.
21) B. White-box tests start with full internal knowledge; black-box simulates external attacker.
22) B. Standard syslogs stored under /var/log.
23) A. Logon Type differentiates interactive (2) and remote interactive/remote desktop (10).
24) A. PCAP stores captured network traffic for analysis.
25) B. TOCTOU uses timing between check and use to manipulate resources.
26) B. Policies balance retention for legal/compliance needs and forensic purposes.
27) B. SFTP works over SSH and is secure for file transfer and shell interactions.
28) A. Mass encryption and ransom notes are hallmarks of ransomware.
29) B. Correlation links multiple events to detect complex behaviors.
30) B. Initial triage confirms legitimacy and scope before larger actions.
31) B. Correlating authentication and process events reveals lateral movement.
32) B. YARA helps detect malware via signature-like rules.
33) B. ext4 journals and timestamps show file metadata changes.
34) B. Risk scoring combines probability and impact to prioritize mitigation.
35) B. Full backups store everything and are fastest to restore but use the most space.
36) B. Honeypots lure attackers to observe TTPs and gather IOCs.
37) A. Task definitions are in the Tasks folder and Task Scheduler library.
38) B. Blind SQLi extracts data indirectly via boolean/time-based responses.
39) B. Hardening reduces attack surface by patching and disabling unnecessary services.

40) B. MTTD measures detection speed and is key SOC metric.

41) B. Layered defenses increase resilience to breaches.

42) A. SAM stores hashed local credentials; Lsass stores in-memory secrets — careful: question targets SAM for cached creds.

43) A. Repeated failed auth attempts indicate brute-force.

44) B. Assessments identify; pentests attempt exploitation to show impact.

45) B. SOCKS proxies relay arbitrary traffic and help attackers route covert communications.

46) B. CloudWatch collects logs/metrics; CloudTrail records API activity.

47) B. Pivoting expands investigation from an initial IOC to related entities.

48) B. Fileless malware resides in memory and uses command interpreters; monitor behaviors and process trees.

49) B. Writable service binaries/registry allow attackers to replace service executables and gain SYSTEM.

50) B. -sS performs SYN (stealth) scan, sending SYN and not completing handshake.

51) B. Anomaly detection finds unusual patterns not covered by signatures.

52) B. Centralized, tamper-resistant logs with time sync facilitate investigations.

53) B. XSS injects client-side scripts to compromise users or sessions.

54) B. UBA and DLP detect deviations and prevent exfiltration over permitted channels.

55) B. Memory reveals running processes, network connections, and in-memory malware.

56) B. SoD prevents fraud by requiring multiple actors for sensitive tasks.

57) B. Timelining orders events from logs/artifacts to model attack progression.

58) A. LotL uses legitimate system tools (PowerShell, WMI) to blend in and evade detection.

59) B. Hashing verifies files weren’t modified during collection/transfer.

60) B. Playbooks guide responders through repeatable remediation steps.

61) B. ARP spoofing shows inconsistent IP-to-MAC mappings.

62) B. SMBv1 contains lengthy-known weaknesses and should be disabled.

63) A. Bash history stores executed shell commands (if not cleared).

64) B. MFA and rate-limiting mitigate credential stuffing and account takeover.

65) A. Staging often includes compression or aggregation to prepare for exfil.

66) B. EDR provides detection, investigation, and response on endpoints.

67) B. STIX/TAXII is a standard for sharing structured threat intel.

68) B. Persistence mechanisms ensure attackers maintain access.

69) B. Metadata and behavior analysis can flag exfil over encrypted channels.

70) A. WHOIS and RIR data help map IP ownership and registration info.

71) B. Digital signatures bind identity to a message, supporting non-repudiation.

72) A. 4740 is account lockout; 4625 records failed logons.

73) B. False negatives mean threats slip past detection controls.

74) B. Web shells hide in webroots and can be triggered via HTTP requests.

75) B. Mail logs and gateway data show sender, path, and payload details.

76) B. Isolation stops further exfil while preserving evidence for analysis.

77) B. Distributed sensors provide granular visibility into internal traffic.

78) B. Combined static and dynamic analysis reveals TTPs for mapping to ATT&CK.;

79) B. NTP sync ensures accurate cross-device correlation.

80) A. Run keys execute programs at user logon and are commonly abused.
81) B. Defanging prevents accidental clicks/queries when sharing threat intel.
82) B. Wireshark inspects packet contents and protocols with a GUI.
83) B. Regular, small, periodic connections are classic C2 beacons.
84) B. PAM limits credential exposure and provides auditing.
85) B. Pinning restricts trust to specific certificates/keys, reducing MitM risks.
86) B. Playbooks standardize response to reduce errors and speed recovery.
87) B. ss/netstat reveal sockets and PID/process info.
88) A. Cron and systemd units are common persistence vectors on Linux.
89) A. Unexpected behavior following a vendor update can signal supply-chain tampering.
90) B. Hypotheses like this guide hunts for specific TTPs and artifacts.
91) B. Alerting on group membership and service changes flags potential privilege escalation.
92) A. 4616 logs time changes (which attackers may manipulate to cover tracks).
93) B. WAFs analyze and block malicious web traffic at application layer.
94) B. Patterned failed attempts indicate brute-force activity.
95) B. Tactical intel supports detection; strategic informs long-term decisions.
96) B. Enhanced PowerShell logging and behavior analytics detect abuse.
97) B. Post-mortems drive improvements and knowledge sharing.
98) A. Auth events and SMB logs show remote access patterns.
99) B. Sandboxes isolate malware to observe behavior safely.
100) B. MTTR tracks time to restore services after incidents.
101) B. NetFlow gives metadata for traffic analysis and anomaly detection.
102) B. Signature verification and trusted sources mitigate package tampering.
103) A. Firewall and policy changes show in system/security logs and group policy channels.
104) B. DLP enforces policies to stop sensitive data exfiltration.
105) A. USBSTOR and SetupAPI record device connection history.
106) B. Credential dumping harvests secrets for use in attacks.
107) B. Sandboxing and CDR help identify malicious attachments.
108) A. 4719 logs changes to audit policy (a possible attacker cover-up).
109) B. IDS alerts; IPS sits inline and may block malicious flows.
110) B. Hashes uniquely identify file content (barring collisions).
111) A. Weak/old TLS and unencrypted HTTP allow downgrade or interception.
112) B. Unusual scheduled tasks are classic persistence indicators.
113) B. Memory must be captured before power state changes to preserve volatile evidence.
114) B. Kill chains map attacker stages to identify defensive interventions.
115) B. Behavioral detection detects variants that evade static signatures.
116) B. Allowlisting prevents unapproved binaries from running.
117) B. Proxy/PCAP and timing show actual data transfer to remote hosts.
118) B. LSASS stores authentication tokens and credentials—target for credential dumpers.
119) B. Red teams emulate adversaries to validate defenses and SOC performance.
120) B. Secure sharing and defanging protect both parties and prevent accidental misuse.

121) B. Reuse leads to multiple accounts compromised from a single leaked credential.

122) B. War rooms centralize incident coordination and communication.

123) B. WMI persistence uses consumers/subscriptions; monitoring their creation reveals misuse.

124) B. GDPR generally requires a 72-hour notification to authorities when personal data is breached.

125) B. Containment, evidence preservation, and assessment are necessary before deciding on remediation or payment.