GSEC Exam Glossary

Find more at BareMetalCyber.com

1. **Access Control**
   Access control is how a system decides who can access a resource and what they are allowed to do once inside. On the exam, it shows up as choosing the right control type (preventive vs detective) and matching a scenario to the correct mechanism (for example, least privilege vs broad shared access).

2. **Accountability**
   Accountability means actions can be reliably tied back to a specific identity through logs, audit trails, and unique credentials. Exam questions often test whether a design supports traceability (for investigations and compliance) versus "everyone shares the same admin account," which breaks attribution.

3. **Active Directory (AD)**
   Active Directory is Microsoft's centralized identity and access system for Windows environments, managing users, groups, computers, and policy. On the exam, it matters when deciding between local controls and domain controls, and when interpreting how group membership and policy inheritance affect access.

4. **Advanced Encryption Standard (AES)**
   AES is a widely used **symmetric** encryption algorithm, meaning the same key is used to encrypt and decrypt data. On the exam, it commonly appears in decisions about protecting data at rest or in transit and recognizing that symmetric encryption is fast but depends heavily on secure key handling.

5. **Asymmetric Cryptography**
   Asymmetric cryptography uses a **public key** and a **private key** as a pair, enabling encryption, digital signatures, and key exchange. Exam scenarios often test when asymmetric methods are used (identity, trust, signing) versus when symmetric methods are used (bulk data encryption).

6. **Authentication**
   Authentication is proving an identity, such as verifying a user with a password, token, certificate, or multifactor method. On the exam, confusion traps are common: many scenarios fail because the identity was never strongly verified before access was granted.

7. **Authorization**
   Authorization is deciding what an authenticated identity is allowed to do, such as read a file, administer a service, or access a subnet. Exam questions frequently hinge on separating "who you are" (authentication) from "what you can do" (authorization), especially in role-based access control designs.

8. **Availability**
   Availability is keeping systems and data accessible to authorized users when needed, often discussed alongside confidentiality and integrity as part of the CIA triad. On the exam, availability shows up in choices like redundancy, patch timing, denial-of-service impacts, and how controls can unintentionally disrupt operations.

9. **Baseline**
   A baseline is an approved "known-good" reference state for configuration and security settings. The term can be used in different ways, but for GSEC it typically means a security configuration baseline used to detect drift, support audits, and speed recovery after changes.

10. **Bastion Host**
    A bastion host is a hardened, tightly controlled system placed at a network boundary to provide a controlled access point (often for administration). On the exam, it's a defensible network architecture concept: you're usually choosing it to reduce exposure, centralize logging, and limit pathways into sensitive segments.

11. **Botnet**
    A botnet is a group of compromised devices controlled by an attacker, often through a command-and-control channel. On the exam, it shows up in traffic-pattern recognition, denial-of-service scenarios, and choosing controls that reduce lateral spread and improve detection.

12. **Breach**
    A breach is a confirmed security incident where data, systems, or accounts are accessed or disclosed without authorization. Exam questions often test whether you can distinguish "suspicion" from "confirmed compromise," and what evidence moves an event into breach territory.

13. **Bring Your Own Device (BYOD)**
    BYOD is a policy model where employees use personal devices for work access, which introduces variability in patching, storage, and monitoring. On the exam, it

matters when choosing controls like mobile device management, segmentation, and data handling rules to reduce risk without assuming full device ownership.

14. **Business Continuity Plan (BCP)**
    A business continuity plan describes how an organization keeps critical functions running during and after disruption. On the exam, it often appears as a decision point between prevention and resilience, and it ties to concepts like acceptable downtime and alternate processing paths.

15. **Certificate Authority (CA)**
    A certificate authority is an entity that issues and signs digital certificates to bind identities to public keys. On the exam, the key idea is trust: if the CA is not trusted or is compromised, certificate-based authentication and secure communications can fail in subtle ways.

16. **Change Control**
    Change control is the process that governs how system changes are requested, approved, tested, implemented, and documented. On the exam, it shows up as "why did this outage or exposure happen," and the correct answer often involves approvals, rollback planning, and audit trails.

17. **Cipher**
    A cipher is an algorithm used for encryption and decryption, typically described as block ciphers or stream ciphers. On the exam, you're usually asked to match a scenario to an appropriate cipher type and avoid common mistakes like weak or outdated cryptography choices.

18. **Compensating Control**
    A compensating control is an alternative safeguard used when the primary control cannot be implemented as written, while still reducing risk to an acceptable level. On the exam, it appears in "constraint" scenarios, where you must pick a realistic alternative that addresses the same threat, not just any extra control.

19. **Confidentiality**
    Confidentiality means preventing unauthorized disclosure of data, whether in storage, processing, or transit. On the exam, it shows up in decisions about encryption, access rules, data classification, and "who should be able to see what" under least privilege.

20. **Containerization**
    Containerization packages an application and its dependencies into an isolated unit that shares the host operating system kernel. On the exam, it matters because isolation is not the same as a full virtual machine boundary, so you're often tested on risks like shared-kernel exposure, image provenance, and runtime permissions.

21. **Defense in Depth**
    Defense in depth is a strategy that uses multiple, overlapping layers of controls so one failure does not equal total compromise. On the exam, it often appears as picking a balanced set of controls across network, endpoint, identity, and monitoring rather than a single "silver bullet."

22. **Denial of Service (DoS)**
    A denial of service attack aims to make a system unavailable by exhausting resources like bandwidth, CPU, memory, or application threads. On the exam, you're typically tested on recognizing symptoms and choosing mitigations that fit the target layer, such as rate limiting, upstream filtering, or architectural redundancy.

23. **Detection**
    Detection refers to identifying security events through logs, alerts, signatures, behavioral signals, or anomaly patterns. On the exam, a frequent decision point is whether a control is actually detecting and producing usable evidence, or merely "hoping" someone notices a problem later.

24. **Digital Signature**
    A digital signature uses asymmetric cryptography to provide integrity and authenticity by proving that a message or file was signed by a private key holder. On the exam, it's commonly used to distinguish signing from encryption: signatures prove who and whether it changed, not secrecy.

25. **Domain Name System (DNS)**
    DNS translates human-readable names into IP addresses and underpins many security-relevant lookups. On the exam, it shows up in troubleshooting suspicious traffic, phishing indicators, and understanding how attacks like spoofing or tunneling can abuse DNS behavior.

26. **Encryption (at Rest / in Transit)**
    Encryption protects confidentiality by transforming data into ciphertext using a key. On the exam, "at rest" typically means stored data (disk, backups) while "in transit"

means data moving over networks, and questions often test choosing the correct control for the data's state and threat model.

27. **Endpoint Detection and Response (EDR)**
    EDR is a set of tools and processes that collect endpoint telemetry and support detection, investigation, and response actions. On the exam, it matters as a practical detection-and-evidence capability, especially when you need visibility into process activity, persistence, and lateral movement signals.

28. **Exploit**
    An exploit is code or a technique that takes advantage of a vulnerability to cause unintended behavior, such as running commands or escalating privileges. On the exam, it frequently appears in risk decisions about patching urgency, compensating controls, and distinguishing "vulnerability exists" from "active exploitation."

29. **Firewall**
    A firewall enforces traffic policy between networks or zones based on rules such as IPs, ports, protocols, and sometimes applications. On the exam, the common trap is assuming a firewall alone solves identity or application-layer problems; many questions test correct placement, least-allowed rules, and segmentation logic.

30. **Forensics**
    Forensics is the disciplined collection and analysis of digital evidence to understand what happened and support decisions or legal action. On the exam, it shows up in evidence handling choices, preserving logs and disk images, and avoiding actions that destroy timestamps or overwrite key artifacts.

31. **Governance**
    Governance is the oversight structure that sets direction, defines accountability, and ensures security decisions match risk tolerance and obligations. On the exam, it shows up in "who owns this decision" scenarios and in choosing policy-driven answers over ad hoc technical fixes.

32. **Hardening**
    Hardening is reducing attack surface by removing unnecessary services, tightening configurations, and enforcing secure defaults. On the exam, it's often tested as the "best first step" when a system is overly exposed, and as the difference between a functional setup and a defensible one.

33. **Hash Function**
    A hash function converts data into a fixed-length value used for integrity checks and comparisons. On the exam, it matters for verifying files, detecting changes, and understanding why hashes are not encryption and cannot be “decrypted” back into the original data.

34. **Incident Response**
    Incident response is the structured process for detecting, triaging, containing, eradicating, and recovering from security incidents. On the exam, it often tests sequencing: stabilize first, preserve evidence, communicate properly, and avoid “hero moves” that make the situation worse.

35. **Integrity**
    Integrity means data remains accurate, complete, and unaltered except by authorized change. On the exam, it shows up in controls like hashing, signatures, access restrictions, and change logging, especially where silent data manipulation is more damaging than downtime.

36. **Least Privilege**
    Least privilege means giving identities only the minimum permissions necessary to do their work, for the minimum time necessary. On the exam, it’s a common correct answer when reducing blast radius, limiting lateral movement, and preventing “everyone is admin” style failures.

37. **Log Management**
    Log management is collecting, normalizing, storing, and protecting logs so they are usable for detection and investigation. On the exam, it’s frequently a visibility-and-evidence topic: if logs aren’t complete, time-synced, and protected from tampering, detection and forensics break down.

38. **Malware**
    Malware is malicious software designed to disrupt, spy, steal, or gain control, including trojans, ransomware, and worms. On the exam, you’ll often need to identify likely malware behavior from symptoms and pick containment steps that reduce spread while preserving evidence.

39. **Multi-Factor Authentication (MFA)**
    MFA requires at least two different factor types, such as something you know plus something you have or are. On the exam, it’s a high-confidence control for reducing

account takeover risk, but questions may test realistic limitations like phishing-resistant factors versus basic one-time codes.

40. **Network Segmentation**
    Network segmentation divides networks into smaller zones with controlled traffic between them, limiting exposure and lateral movement. On the exam, it shows up in architecture choices, isolating high-value assets, and proving that “flat networks” increase the impact of a single compromise.

41. **Patch Management**
    Patch management is the process of testing, deploying, and tracking updates that fix vulnerabilities and bugs. On the exam, it’s commonly framed as a risk decision: prioritizing patches based on exposure and exploitability, and balancing speed with stability through controlled rollout.

42. **Phishing**
    Phishing is a social engineering attack that tricks users into revealing credentials, approving access, or running malicious content. On the exam, it often appears in email and web scenarios where the best answer combines user-facing controls (training, reporting) with technical controls (filtering, MFA, domain protections).

43. **Privilege Escalation**
    Privilege escalation is gaining higher permissions than intended, such as moving from a normal user to administrator or from one service context to another. On the exam, it’s a key attack path concept used to evaluate hardening, segmentation, and monitoring choices that would block or detect the step-up.

44. **Public Key Infrastructure (PKI)**
    PKI is the system of certificates, keys, authorities, and processes that enables trusted identity and encrypted communication at scale. On the exam, it matters for decisions about certificate trust chains, lifecycle management, and how authentication can rely on certificates rather than shared secrets.

45. **Risk Assessment**
    Risk assessment is evaluating threats, vulnerabilities, likelihood, and impact to prioritize controls and responses. On the exam, it shows up when a scenario forces tradeoffs, and the correct answer is often the one that reduces the highest risk first rather than the most visible issue.

46. **Security Information and Event Management (SIEM)**
    A SIEM centralizes logs and events, correlates signals, and supports alerting and investigation workflows. On the exam, it's tested as a detection and evidence tool: you may need to choose what to log, how to correlate, and why centralized visibility improves response.

47. **Threat Modeling**
    Threat modeling is systematically identifying what can go wrong, how it could happen, and what controls reduce the most important risks. On the exam, it appears as structured thinking: identifying assets, trust boundaries, and likely attacker paths rather than guessing controls randomly.

48. **Vulnerability**
    A vulnerability is a weakness that can be exploited to violate confidentiality, integrity, or availability. On the exam, it's important to separate a vulnerability (a condition) from an exploit (a technique) and from an incident (an outcome), because the correct actions differ.

49. **Vulnerability Scanning**
    Vulnerability scanning uses automated tools to identify known weaknesses and misconfigurations across systems. On the exam, common decision points include scan scope, credentialed vs non-credentialed scans, false positives, and why scanning is not the same as penetration testing.

50. **Zero Trust**
    Zero Trust is a security approach that treats every access request as untrusted until verified, emphasizing strong identity, least privilege, and continuous evaluation. On the exam, it often shows up as a modern framing for segmentation and access decisions, and the trap is assuming it is a single product rather than a design model.