Cyber Security Master Study Compilation

By: Charlotte Payan-Salcedo

Web & Application Attacks

Attack	What It Actually Is	Trigger Words
SQL Injection (SQLi)	Attacker injects malicious SQL to manipulate database queries	' OR 1=1--, “Authentication bypass”, “Unsanitized input”
CSRF	Tricks a logged-in user’s browser into sending unauthorized requests	“User session”, “Unauthorized action performed”
SSRF	Forces the server to send requests to internal or external resources	“Server fetches user URL”, “Access internal network”, “Metadata service”
LFI (Local File Inclusion)	Loads local files from the server filesystem	/etc/passwd, “Path manipulation”
RFI (Remote File Inclusion)	Loads malicious files from an external server	“Remote script execution”, “External file loading”

Quick differentiation:

- LFI = local system file
- RFI = remote attacker-controlled file

Malware & Advanced Threat Indicators

Term	What It Means	Trigger Words
Beaconing	Infected host communicates with C2 at regular intervals	“Periodic outbound traffic”, “Every 30 seconds”, “Callback”
Lateral Movement	Attacker moves within network to escalate access	“Pivot”, “Pass-the-hash”, “Move to file server”
APT (Advanced Persistent Threat)	Highly skilled, well-funded threat actor conducting long-term targeted attacks	“Nation-state”, “Long-term presence”, “Data exfiltration over months”

Threat Actors & Advanced Persistent Threats (APTs)

- **Threat Actor:** A person or entity responsible for an event identified as a security risk or incident.
- **APTs** (Advanced Persistent Threats): Well-funded, highly skilled attackers (often nation-states) that enter quietly and stay long-term to steal or manipulate data.
    - Goals: Real human adversaries with clear objectives like espionage, IP theft, or disruption.
    - Tactics: Use custom malware, zero-days, "living-off-the-land" tools, and careful cleanup to avoid detection.
- **Command and Control (C2):** The phase where an adversary establishes a communication channel with a successfully exploited target.
- Beaconing: A technique used by malware to maintain a covert communication channel with a C2 server.

The Response Teams

- **SOC (Security Operations Center):** A centralized team responsible for continuous monitoring, detection, analysis, and response to incidents.
- **CSIRT (Computer Security Incident Response Team):** The primary internal team for routine and non-emergency security incidents.
- **CERT (Computer Emergency Response Team):** A high-impact team for major/urgent incidents; they react, report trending threats, and relay info to law enforcement

OSSIM (Open Source Security Information Management)

An open-source SIEM platform **(AlienVault)** that collects and correlates security events.
Trigger: Open-source SIEM.

OSSTMM (Open Source Security Testing Methodology Manual)

A scientific methodology for full-spectrum security testing across People, Physical, and Network layers.
Trigger: Structured security testing framework.

Forensics & Legal Flow (The "Correct Order")

When an investigation starts, you must follow this exact sequence:

1. **Legal Hold:** Formal directive to preserve data; always the first move.
2. **Data Preservation:** Capturing evidence (e.g., using antistatic bags for hardware).
3. **Data Validation:** Ensuring the integrity/authenticity of the data.
4. **Data Analysis:** Investigating the evidence (e.g., via SIEM).

- **Chain of Custody:** The paper trail proving evidence was never tampered with.

Threat Intelligence & Attack Frameworks

Framework Comparison

- **Cyber Kill Chain:** 7-stage linear progression (Recon → Weaponization → Delivery → Exploitation → Installation → C2 → Actions).
- **Diamond Model:** Analytical and non-linear; maps the relationships between **Adversary, Infrastructure, Capability,** and **Victim**.
- **MITRE ATT&CK:** A massive knowledge base of real-world **Tactics (Why)** and **Techniques (How)**.

Threat Intelligence Standards

- **CybOX:** The **Data** (raw indicators like hashes).
- **STIX:** The **Language/Format** (gives data meaning).
- **TAXII:** The **Delivery/Transport** (moves the intel).

Detection Accuracy & Asset Value

Result Type	Meaning	Memory Aid
True Positive	**Correctly identifies a real threat.**	**Alert & Real**
False Positive	**Alert for a threat that doesn't exist.**	**Alert but Wrong**
True Negative	**Correctly identifies no threat is present.**	**Clean & Confirmed**
False Negative	**A real threat exists but tool missed it.**	**Missed it**

- **High Asset Value** (Critical): Compromise causes significant business/safety impact.
- **Low Asset Value:** "Nice to have" with minimal impact.

Exam Differentiation (High Yield)

• Nessus finds vulnerabilities — it does NOT exploit.
• Metasploit exploits to prove risk.
• SIEM (Splunk) analyzes logs — it does NOT automatically act.
• SOAR acts automatically.
• Snort/Suricata monitor traffic — they do not analyze host logs.
• Wireshark = raw packet detail, not alerting.
• Burp = web application testing only.

Fast Category Memory

Scanning → Nessus / Angry IP
Exploitation → Metasploit
Monitoring → Splunk / Snort / Suricata
Automation → SOAR
Web Testing → Burp Suite
Packet Analysis → Wireshark
Malware Analysis → Joe’s Sandbox

🧰 Cybersecurity Toolbelt

Tool	Category	Core Function (Exam Meaning)	Trigger Words / Memory Hook
Metasploit	Exploitation Framework	Validates vulnerabilities by safely launching exploits	"Proof of concept", "Exploit validation", Scan → Exploit
Splunk	SIEM	Collects, correlates, and analyzes logs across systems	"Log aggregation", "Correlation", The Big Picture
SOAR	Automated Response	Automates incident response actions using playbooks	"Automated containment", "Trigger playbook"
Snort	Network IDS (NIDS)	Detects malicious network traffic using signature rules	"Signature-based detection", Network Tripwire
Suricata	Network IDS/IPS	Similar to Snort; can detect and block traffic	"Inline IDS/IPS", Signature rules
Burp Suite	Web App Testing	Intercepts and manipulates web traffic for manual testing	"Intercept proxy", "Modify HTTP request"
Wireshark	Packet Analyzer	Captures and analyzes packet-level network traffic	"Deep packet inspection", Protocol analysis
Joe's Sandbox	Malware Analysis	Executes malware safely to observe behavior	"Dynamic analysis", "Behavior observation"
Nessus	Vulnerability Scanner	Identifies known vulnerabilities in systems	"Unpatched systems", "CVE detection"
Angry IP Scanner	Network Discovery	Quickly identifies live hosts on a network	"Who is alive?", Fast host discovery

Defensive Operations (SOC, SIEM, SOAR)

- **SOC (Security Operations Center):** A centralized team for continuous monitoring and incident response.
- **SIEM:** Collects and correlates logs from across the environment to detect incidents.
- **SOAR:** Automates incident response using **Playbooks** to reduce workload.
- **Webhooks:** An event-driven "Trigger" that sends real-time data between systems.
- **IDS (Intrusion Detection System):** Monitors activity and alerts, but **does not stop** the action.
    - **NIDS:** Network-based.
    - **HIDS:** Host-based.

Password Security & Cryptography

- **Rainbow Table Attack:** Using pre-computed hash tables ("Ready-made answers") to crack passwords.
    - **Vulnerable Hashes:** MD5, SHA-1, NTLM, LM.
- **Salting:** Adding random data before hashing to defeat rainbow tables.
- **Ephemeral Keys:** Temporary, one-session keys that provide perfect forward secrecy.

Infrastructure & Traffic Patterns

- **North-South Traffic:** Traffic moving between the Data Center and the Internet (passing the firewall).
- **East-West Traffic:** Traffic staying within the LAN or moving between internal Data Center systems.
- **Endpoint Sources:** Where traffic begins/ends (Workstations, Servers).
- **Intermediary Sources:** Devices traffic passes through (Routers, Firewalls, IDS).
- **Hybrid Cloud:** Balances security and scalability by keeping sensitive data private on-prem while using public cloud resources.

NIST Incident Response Lifecycle (SP 800-61)

Phase	What It Actually Means (Exam Language)	What You're Doing	Common Exam Clues
Preparation	Establish policies, tools, and procedures before an incident occurs	Create IR plan, define roles, deploy SIEM, harden systems, create playbooks, conduct training	"Before incident occurs", "Develop playbook", "Implement logging"
Detection & Analysis	Identify, validate, and determine scope of incident	Monitor alerts, analyze logs, confirm incident, determine affected systems, assign severity	"Alert triggered", "Suspicious traffic detected", "Determine scope"
Containment	Limit damage and prevent further spread	Isolate hosts, disable accounts, block IPs, segment network	"Stop the spread", "Prevent further damage", "Immediate next step"
Eradication	Remove root cause of incident	Remove malware, patch vulnerability, eliminate persistence mechanisms	"Remove malicious files", "Patch exploited service"
Recovery	Restore systems to normal operations	Rebuild systems, restore from backups, monitor for reinfection	"Restore services", "Return to production"
Post-Incident Activity (Lessons Learned)	Improve future response and update controls	Document findings, update policies, adjust controls, improve detection	"After-action report", "Improve future response"

Tool	Core Category	Primary Function (Exam Language)	Exam Trigger Phrases
Recon-ng	OSINT / Recon	Framework for collecting publicly available intelligence (domains, emails, usernames).	OSINT framework, public intelligence gathering
Aircrack-ng	Wireless Security	Captures wireless packets and cracks WEP/WPA keys; supports deauthentication attacks.	Wi-Fi capture, WPA cracking, deauth attack
Maltego	OSINT / Link Analysis	Visualizes relationships between entities (people, domains, IPs) for investigation.	Link analysis, relationship mapping
Cuckoo	Malware Analysis	Automated sandbox for dynamic malware analysis.	Malware sandbox, behavioral analysis
Nikto	Web Server Scanning	Scans web servers for outdated software, dangerous files, and misconfigurations.	Web server scanner, outdated software detection
OpenVAS	Vulnerability Management	Open-source vulnerability scanner that identifies known flaws.	Open-source scanner, vulnerability assessment
ScoutSuite	Cloud Auditing	Audits multi-cloud environments for security misconfigurations.	Multi-cloud audit, configuration review
Prowler	Cloud Security / CSPM	Assesses AWS/Azure/GCP environments against security best practices.	Cloud posture assessment, AWS audit
Pacu	Cloud Exploitation	AWS exploitation framework for testing cloud privilege escalation and lateral movement.	AWS exploitation, cloud privilege escalation
Arachni	Web App Scanning (DAST)	Dynamic Application Security Testing tool that scans web apps for vulnerabilities (SQLi, XSS).	DAST scanner, web app vulnerability scan
tcpdump	Packet Capture	Command-line packet analyzer that captures live network traffic (.pcap).	Packet capture, CLI sniffing, network traffic
GDB	Debugger / Exploit Dev	Debugger used to analyze program execution and memory behavior.	Reverse engineering, exploit development

🛠️ Security Architecture & Modern Infrastructure

Concept	Meaning	Exam Trigger Phrases
Zero Trust	"Never trust, always verify" across Identity, Devices, Networks, Apps, and Data.	**"I Do Not Accept Doubts"** (IDNAD).
SASE	Cloud-based architecture combining SD-WAN with security controls.	**Cloud + Network + Security**.
Microservices	**Containers** share a host OS kernel (e.g., Docker); **Virtualization** uses separate OS instances.	**Containers = Same OS**.
API	Structured app-to-app communication; minimizes human engagement.	**Programmatic exchange**.
Webhook	Automatic, event-driven data "push" (Trigger).	**Real-time notification**.

Frameworks & Compliance

- **CIS:** Focused on system **Hardening**, benchmarks, and "Quick Wins".
- **NIST:** US Government frameworks for **Risk Management** (RMF, CSF).
- **ISO (27001):** International **Global Standards** for security programs (Not free).
- **OWASP:** The go-to for **Web App** security and the "Top 10" risks.
- **SLO (Service Level Objective):** Metrics to determine if a project is worth doing and to meet leadership expectations.

Vulnerability Scanning Types

Scan Type	What It Does (Exam Meaning)	Trigger Words
Map Scan	Identifies live hosts, open ports, and services to understand network topology	“Discover hosts”, “Enumerate ports”, “Network layout”
Baseline Scan	Establishes a normal reference state for comparison over time	“Establish baseline”, “Compare against previous scan”
Agent-Based Scan	Uses installed agents on endpoints to report vulnerabilities directly	“Remote workforce”, “Dynamic IP”, “Off-network devices”
Internal Scan	Identifies vulnerabilities from inside the network	“Lateral movement risk”, “Insider threat exposure”
External Scan	Identifies vulnerabilities visible from the internet	“Public-facing systems”, “What attacker sees”
Fuzzing	Sends malformed or unexpected input to identify crashes or input validation flaws	“Application crash”, “Unexpected input testing”

Cloud Computing Models (CySA+ Focus)

Model	What It Means (Exam Language)	Trigger Words
Public Cloud	Shared infrastructure provided over the internet	AWS, Azure, GCP, Multi-tenant
Private Cloud	Cloud environment dedicated to a single organization	Single-tenant, Internal cloud
Hybrid Cloud	Combination of on-premises infrastructure and public cloud	Data center + cloud

Serverless (FaaS)	Cloud provider manages infrastructure; customer deploys code only	AWS Lambda, Event-driven compute

Exam trap:
Serverless does NOT mean “no servers.” It means the provider manages them.

Memory & Code Attacks

Term	What It Actually Means (Exam Language)	Trigger Words
Buffer Overflow	Writing more data into a buffer than it can hold, causing adjacent memory corruption	“Exceeds buffer size”, “Memory corruption”, “Improper bounds checking”
Stack Overflow	Overwrites return address in stack memory to hijack program execution	“Return pointer modified”, “Control flow hijacked”
Heap Overflow	Corrupts dynamically allocated memory to manipulate data or pointers	“Dynamic memory corruption”, “Heap manipulation”
SQL Injection (SQLi)	Injects malicious SQL into application queries to manipulate database operations	' OR 1=1--, “Authentication bypass”
ASLR	Randomizes memory addresses to reduce exploit predictability	“Memory randomization”, “Mitigation for overflow”

High-yield difference:
Stack = control flow takeover
Heap = data/pointer corruption

ASLR mitigates exploitation, not the vulnerability.

Syslog Severity Levels (0–7)

CySA expects you to know the numeric order.

Level	Name	Meaning
0	Emergency	System unusable
1	Alert	Immediate action required
2	Critical	Severe condition
3	Error	Operation failed
4	Warning	Potential issue
5	Notice	Significant but normal
6	Informational	Routine message
7	Debug	Detailed troubleshooting info

Memory Trick:
Lower number = more severe.

0 = worst.
7 = least severe.

Containment Hierarchy

When breach is confirmed:

1. Containment
2. Eradication
3. Recovery
4. Lessons Learned

If attack is ACTIVE → stop the damage first.

Examples:

Worm spreading → Isolate host
Data exfiltration → Block outbound traffic / shut service
Unauthorized login → Disable account

Interpreting CVSS v3.1 Strings

Example CVSS Vector

A CVSS vector looks like this:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Read it **left → right**. Each metric answers **one exam question**.

CVSS Vector Decoder —

Metric	What It Asks	Code in Yours	What That Code Means	Memory Shortcut
AV	How far is attacker?	**N**	Network (remote over internet)	**N** = Network = Remote
AC	How hard is exploit?	**L**	Low complexity (easy)	**L** = Low effort
PR	Login needed first?	**N**	None required	**N** = No login
UI	User must click?	**N**	No interaction needed	**N** = No click
S	Does it escape boundary?	**C**	Changed (breaks out / escalates impact)	**C** = Crosses boundary
C	Data exposure?	**H**	High (full data disclosure)	**H** = Huge leak
I	Data tampering?	**H**	High (full modification)	**H** = Hijacked data
A	System availability?	**H**	High (system down)	**H** = Halted system

---

Metric	Question It Answers	Codes	Meaning
AV (Attack Vector)	How far is attacker?	N	Network (remote)
		A	Adjacent (same network)
		L	Local
		P	Physical
AC (Attack Complexity)	How hard is exploit?	L	Low (easy)
		H	High (special conditions)
PR (Privileges Required)	Login required?	N	None
		L	Low
		H	High (admin/root)
UI (User Interaction)	User must act?	N	No
		R	Required
S (Scope)	Does impact escape boundary?	U	Unchanged
		C	Changed (crosses boundary)
C (Confidentiality)	Data exposed?	N	None
		L	Low
		H	High
I (Integrity)	Data modified?	N	None
		L	Low
		H	High
A (Availability)	System disrupted?	N	None
		L	Low
		H	High

One-Line Memory Hack

AV = Distance
AC = Difficulty
PR = Access
UI = Click needed?
S = Escape?
CIA = What breaks

If you can read that table smoothly, CVSS questions become free points.

CySA Exam Traps

• CVSS score ≠ exploitability
• Base score ≠ environmental score
• Scope **Changed** increases severity
• User Interaction **Required** lowers severity
• Availability **High** ≠ data breach (that's Confidentiality)

CVSS v3.x Scoring System

Score Range	Severity Rating	What It Means Operationally
0.0	None	No risk
0.1 – 3.9	Low	Minimal impact
4.0 – 6.9	Medium	Moderate risk
7.0 – 8.9	High	Serious risk
9.0 – 10.0	Critical	Immediate remediation required

Fast Memory Trick

0 = None
1–3 = Low
4–6 = Medium
7–8 = High
9–10 = Critical

Risk Treatment Strategies

Strategy	What It Means	Exam Trigger
Risk Acceptance	Acknowledge risk and do nothing	“Business decision to live with it”
Risk Mitigation	Reduce risk with controls	“Implement firewall / patch / MFA”
Risk Avoidance	Eliminate the risky activity	“Shut down service”
Risk Transference	Shift risk to third party	“Cyber insurance”, “Outsource”

Memory:
Accept = Live with it
Mitigate = Lower it
Avoid = Stop it
Transfer = Move it

Change Management & Patch Control

CySA LOVES process discipline.

If maintenance window closes before completion:
→ Stop
→ Roll back to last known good
→ Reschedule

Hard rule:
Untested patch in production = Reject

Change management =
Document → Approve → Test → Deploy → Validate → Rollback plan ready

Control Types (Classification Questions)

By Implementation Type

Control Type	Meaning	Example
Technical	Technology-enforced	Firewall, IDS, MFA
Operational	People/process actions	Security training, daily procedures
Managerial	Policies and governance	Risk decisions, security policy

By Function

Control Type	Purpose	Example
Preventive	Stop attack before it happens	Firewall, IPS
Detective	Identify after it happens	Logs, IDS
Corrective	Fix issue	Patch, restore backup
Compensating	Alternative control when ideal not possible	Extra monitoring
Responsive	React to incident	IR playbooks

Exam trap:
Training = Operational
Policy update = Managerial
Firewall = Technical Preventive

IDS vs IPS (Clear Separation)

	System Action
IDS	Detects & alerts only
IPS	Detects & blocks

NIDS = Network-based
HIDS = Host-based

Exam trap:
If question says “automatically blocks” → IPS

Log Type Identification (High Yield)

Log Type	What It Shows	When To Choose It
Authentication Log	Logins, failures, account lockouts	Brute force, account compromise
Application Log	App-specific errors/behavior	Strange app behavior
System Log	OS-level events	Service crash, system error
Security Log	Security events (Windows Event IDs)	Privilege escalation
Network Log	Traffic flow data	Beaconing, DDoS
Audit Log	User actions & changes	Data access tracking

If login problem → Authentication log
If malware callback → Network log
If app crashing → Application log

CVSS Score Types (Clarification)

Type	Meaning
Base Score	Intrinsic severity of vulnerability
Temporal Score	Adjusts for exploit maturity & fixes
Environmental Score	Adjusts for business impact

CySA mostly tests:
Base Score severity mapping.

Exploit Maturity vs Severity

CVSS 9.8 but no exploit available = still high severity
Exploit code publicly available = higher temporal score

**Do not confuse exploit availability with base severity*.

Data Sovereignty

Data governed by laws of the country where it is stored.

Trigger words:
GDPR
Cross-border storage
EU data residency

If question mentions geography + legal restrictions → Data Sovereignty

Data Exfiltration Indicators

- **Large outbound transfers**
- **Unusual hours**
- **Encrypted outbound to unknown IP**
- **High-volume DNS queries**
- **Sudden compression before transfer**

Incident Notification Order

When breach confirmed:

1. **Legal** (always first)
2. **Regulators** (if required by law)
3. **Law Enforcement** (criminal activity)
4. **Customers** (if impacted)
5. **Media** (after legal approval)

*Never public statement before Legal.

Zero-Day

Zero-Day = Vulnerability with no patch available.

Trigger:
“No vendor fix available”

Lateral Movement & Post-Compromise Techniques

Term	Definition (Exam Language)	Exam Trigger / Mnemonic
Lateral Movement	Attacker moves inside the network after initial compromise to access higher-value systems.	Internal spread, pivot, post-compromise movement
Pass-the-Hash (PtH)	Attacker uses a stolen password hash (e.g., NTLM) to authenticate without knowing the plaintext password.	NTLM/LM hash reuse, SAM dump, credential reuse
Living-off-the-Land (LOLBins)	Attacker uses legitimate built-in system tools (PowerShell, WMI, cmd, Bash) to avoid detection.	Built-in OS tools, “legitimate process,” low visibility
Privilege Escalation	Attacker gains higher-level permissions (e.g., standard user → admin) to expand access.	Elevated privileges, Domain Admin, high-privilege actions

Fast Mental Differentiation

Lateral Movement → Moving sideways inside network
Privilege Escalation → Moving upward in permissions
Pass-the-Hash → Reusing stolen hash to authenticate
LOLBins → Using trusted tools to stay stealthy

High-Yield Exam Connections

- Beaconing + internal pivot = likely lateral movement
- SAM database access → Pass-the-Hash setup
- PowerShell spawning suspicious processes → LOLBins
- Sudden admin account activity → Privilege escalation

Risk Terms (Often Confused)

Term	Meaning
Inherent Risk	Risk before controls
Residual Risk	Risk after controls
Risk Appetite	How much risk organization is willing to accept

East-West vs North-South

North-South = Internal ↔ Internet
East-West = Internal ↔ Internal

Worm spreading internally = East-West

Legal & Evidence

Legal Hold = ALWAYS first step in formal investigation
Chain of Custody = Proof evidence not altered
Data Validation = Integrity check (hash verification)

Attack Surface

Definition:
The total number of possible entry points an attacker can use to access a system.

Includes:

- Open ports
- Public-facing services
- APIs
- User accounts
- Cloud resources
- Exposed endpoints

Exam Trigger Words:
“Public exposure”, “Open services”, “Reduce exposure”, “External-facing systems”

Memory:
More exposure = bigger attack surface.

Attack Surface Reduction (ASR)

Definition:
The process of minimizing exposed services, ports, applications, and privileges to reduce opportunities for attack.

Examples:

- Disabling unused services
- Removing legacy protocols
- Least privilege enforcement
- Blocking macros

Exam Trigger Words:
“Reduce exposure”
“Disable unnecessary services”
“Minimize attack vectors”

Memory:
Less exposed = less exploitable.

End-of-Support (EOS) Risk

Definition:
Risk associated with software or hardware that no longer receives vendor updates or security patches.

Why It’s Dangerous:

- No future patches
- Known vulnerabilities remain exploitable
- Increased compliance risk

Exam Trigger Words:
“Unsupported OS”
“Legacy system no longer patched”
“Vendor discontinued updates”

If no patches are available and product is abandoned → EOS risk.

Signature-Based Detection vs Anomaly-Based Detection

Detection Type	How It Works	Strength	Weakness	Exam Trigger
Signature-Based	Matches activity against known patterns	Accurate for known threats	Cannot detect zero-day	“Known pattern”, “Signature rule”
Anomaly-Based	Detects deviations from baseline behavior	Can detect unknown threats	Higher false positives	“Behavior deviation”, “Baseline variance”

DAST vs SAST

Type	Full Name	What It Tests	When It Runs	Exam Trigger
SAST	Static Application Security Testing	Source code without running the app	During development	“Code review”, “White-box testing”
DAST	Dynamic Application Security Testing	Running application from outside	During runtime/testing	“Black-box testing”, “Running app scan”

Important:

- **Arachni = DAST**
- **DAST finds** runtime vulnerabilities (SQLi, XSS)
- **SAST finds** insecure coding flaws before deployment

Memory:
SAST = See Source
DAST = During execution

⚡ Quick Concept Map

Attack Surface → What is exposed
Attack Surface Reduction → How you shrink exposure
EOS → No more patches
Signature detection → Known bad
Anomaly detection → Weird behavior
SAST → Code scanning
DAST → Live app scanning

Secure SDLC (SSDLC)
Security integrated into every phase of development.

DevSecOps
Automated security testing integrated into CI/CD pipelines.

Command Injection
Attacker injects OS-level commands into application input.

Trigger:
“Execute system command”
“Shell spawned”
“; ls -la” type behavior

This ties directly to RCE.

Race Condition
Exploiting timing flaws where two operations occur simultaneously.

Trigger:
“TOCTOU” (Time-of-check to time-of-use)

Fuzzing
Automated testing method that sends random, malformed, or unexpected inputs to identify crashes and input-handling flaws.

Network Segmentation

Dividing network into isolated zones to limit lateral movement.

Trigger:

- “Limit blast radius”
- “Contain internal spread”

DLP (Data Loss Prevention)- Monitors and blocks sensitive data from leaving the organization.

MFA (Multi-Factor Authentication) -Requires two or more authentication factors. Look for on test (credential stuffing, Prevent account compromise)

Honeypots / Honeynets- Decoy system used to attract and monitor attackers. Look for on the test (Fake server, Attract attacker behavior)

File Integrity Monitoring (FIM)- Monitors changes to critical system files.

Baseline vs Benchmark
You define baseline scans, but not clearly:

Baseline = normal behavior reference
Benchmark = industry configuration standard **(CIS benchmark)**

Vulnerability Management Lifecycle

Stage	What Happens	Trigger Words
Discovery	Identify vulnerabilities via scan	“Scan results”
Assessment	Analyze severity (CVSS, impact)	“Risk scoring”
Prioritization	Rank by risk and business impact	“High-value asset first”
Remediation	Patch or mitigate	“Apply fix”
Verification	Rescan to confirm fix	“Confirm vulnerability resolved”

IoC (Indicator of Compromise) - Evidence that a system has been breached or is under attack.

Examples:

- Suspicious IP
- Unexpected outbound traffic
- Unknown file hashes
- Unusual login times

🔐 Secure Coding & Input Protection

Concept	What It Means (Exam Language)	What It Prevents	Exam Trigger Words
Input Validation	Ensuring all user input is properly sanitized and validated before processing.	SQLi, XSS, command injection	“Unsanitized input”, “Improper validation”
Parameterized Queries	Using placeholders in SQL queries instead of directly inserting user input.	SQL Injection	“Prepared statements”, “Bind variables”
Output Encoding	Encoding user-supplied data before displaying it in a browser.	Cross-Site Scripting (XSS)	“Encode output”, “HTML encoding”
Least Privilege	Running applications and services with the minimum permissions required.	Privilege escalation impact	“Minimal permissions”, “Restricted access”
Error Handling	Suppressing detailed system/database error messages from users.	Information disclosure	“Verbose error message”, “Stack trace exposed”
Code Injection	Injection of malicious code due to improper input handling.	SQLi, command injection	“Injected payload”, “Improper sanitization”
Command Injection	Injecting OS-level commands into application input fields.	Remote Code Execution (RCE)	“Execute system command”, “Shell spawned”
Buffer Overflow	Writing more data than a buffer can hold, causing memory corruption.	RCE, memory corruption	“Improper bounds checking”, “Exceeds buffer size”
ASLR	Randomizes memory addresses to reduce exploit reliability.	Predictable exploitation	“Memory randomization”
DEP (Data Execution Prevention)	Prevents execution of code in non-executable memory regions.	Code execution attacks	“Execution prevention in memory”

Fast Mental Flow

Root cause of most web attacks → Improper input validation
SQLi defense → Parameterized queries
XSS defense → Output encoding
RCE via memory → Buffer overflow
Exploit mitigation → ASLR + DEP

Network Attacks (DDoS & Related)

Attack	What It Means (Exam Language)	Trigger Words
DDoS (Distributed Denial of Service)	Overwhelms a target with traffic from multiple systems to make it unavailable.	"Botnet traffic", "Service unavailable", "Flood attack"
DoS	Single-source denial of service attack.	"Single IP flooding"
SYN Flood	Sends large numbers of TCP SYN requests without completing handshake.	"Half-open connections", "SYN queue exhaustion"
UDP Flood	Floods target with UDP packets to overwhelm bandwidth.	"High UDP traffic"
ICMP Flood (Ping Flood)	Sends excessive ICMP echo requests.	"Ping flood", "ICMP spike"
Amplification Attack	Uses third-party servers to amplify traffic (e.g., DNS, NTP).	"Reflection", "Amplified response"
DNS Amplification	Exploits open DNS resolvers to multiply traffic volume.	"Large DNS responses", "Spoofed source IP"

If question says:
"Service overwhelmed by traffic" → DDoS
"Half-open connections" → SYN flood

DDoS Mitigation & Traffic Protection Controls

Control	What It Does (Exam Language)	When It's Used	Exam Trigger Words
Rate Limiting	Limits number of requests allowed from a source within a time period.	API abuse, brute force, basic flood attempts	"Limit requests per second", "Throttle traffic"
Load Balancer	Distributes traffic across multiple servers to prevent overload.	High traffic environments, availability protection	"Distribute traffic", "Prevent single server overload"
CDN (Content Delivery Network)	Caches content across global servers to absorb and distribute traffic.	Large-scale DDoS protection, public websites	"Edge caching", "Global distribution", "Absorb traffic spike"
Blackholing	Drops all incoming traffic to a targeted IP to protect the network.	Severe DDoS when service sacrifice is acceptable	"Drop all traffic", "Null route"
Sinkholing	Redirects malicious traffic to a controlled server for analysis.	Botnet/C2 disruption, malware traffic	"Redirect malicious traffic", "Traffic analysis server"
Geo-blocking	Blocks traffic from specific geographic regions.	Region-specific attack sources	"Block traffic from country", "Regional restriction"
WAF (Web Application Firewall)	Filters and blocks malicious HTTP/HTTPS traffic at application layer.	Protecting web apps from SQLi, XSS, HTTP floods	"Application-layer filtering", "Protect web server"

Fast Mental Differentiation

Rate limiting → Slow them down
Load balancer → Spread the load
CDN → Absorb globally
Blackhole → Drop everything
Sinkhole → Redirect for analysis
Geo-block → Block by country
WAF → Filter web-layer attacks

Exam nuance:

- Blackholing sacrifices availability to protect infrastructure.
- Sinkholing is investigative.
- WAF protects Layer 7 (application layer).
- Load balancer improves availability but does not block malicious traffic by itself.

Command and Control (C2)

Concept	What It Means (Exam Language)	Exam Trigger Words
Command and Control (C2)	Communication channel established by an attacker to remotely control a compromised system.	“Callback traffic”, “Beaconing”, “Remote control server”
Beaconing	Periodic outbound communication from infected host to C2 server.	“Every 30 seconds”, “Regular interval traffic”
C2 Channel Types	Methods used to maintain communication.	HTTP/HTTPS, DNS tunneling, encrypted outbound traffic
Domain Generation Algorithm (DGA)	Malware generates random domain names to evade blocking.	“Random domain lookups”, “High DNS queries”
Fast Flux	Rapidly changing IP addresses tied to a malicious domain.	“Frequent DNS record changes”

What C2 Means in the Kill Chain

Cyber Kill Chain order:

Recon → Weaponization → Delivery → Exploitation → Installation → **C2** → Actions on Objectives

Important: C2 is the phase where the attacker has persistent control.

Egress Filtering

Filtering outbound traffic to prevent data exfiltration or C2 communication.

Trigger:“ **Block outbound to unknown IP”, “Prevent data exfiltration”**

Containment first during incident

Outbound block = Egress filtering
Internal spread = Segmentation issue
Sensitive data leaving = DLP
No alert but suspicion = Threat hunting
Unauthorized file change = FIM
Brute force logins = Lockout policy
Fake server = Honeypot

Detection Clues (High Yield)

- Outbound encrypted traffic to unknown IP
- Traffic at exact recurring intervals
- High-volume DNS queries
- Traffic to newly registered domains
- Connections to known malicious Ips

Disruption Methods

- Sinkholing
- Blocking outbound traffic
- DNS filtering
- Egress filtering
- Network segmentation

Fast Mental Map

C2 = Remote control channel
Beaconing = Periodic “phone home”
DGA = Random domain generation
Fast Flux = Rapid IP changes

If you see:
“Internal host communicating every 60 seconds to unknown IP”
That is beaconing → C2 activity.

✉ Email Security

Phishing Attacks

Attack	Meaning	Trigger Words
Phishing	Fraudulent email attempting credential theft.	“Fake login page”
Spear Phishing	Targeted phishing against specific individual.	“Personalized email”
Whaling	Targeting executives.	“CEO impersonation”
Smishing	SMS-based phishing.	“Text message scam”
Vishing	Voice-based phishing.	“Phone call scam”

Email Spoofing Protections

Control	What It Does	Trigger Words
SPF	Verifies sending mail server IP is authorized.	“Sender validation”
DKIM	Digitally signs email to ensure integrity.	“Email signature verification”
DMARC	Policy framework that enforces SPF/DKIM and reports failures.	“Reject spoofed mail”

Exam trap:

SPF = who can send
DKIM = message integrity
DMARC = policy + enforcement

Business Email Compromise (BEC)

Attacker impersonates trusted executive/vendor to request money transfer.

Trigger:
“Urgent wire transfer request”
“Finance department spoofed email”

Email Security Tools

- Secure Email Gateway (SEG)
- Sandboxing attachments
- URL rewriting
- Anti-spam filters

Email Indicators of Compromise

- Suspicious attachments (.zip, .exe, macro-enabled docs)
- Mismatched display name vs email address
- Urgent financial request
- Domain look-alike (typosquatting)

Email + Attack Pattern Link

Phishing → Credential theft
Credential theft → Lateral movement
Lateral movement → Privilege escalation
Privilege escalation → Data exfiltration

Account Lockout / Brute Force Protection

Concept	Definition	Trigger Words
Account Lockout Policy	Locks account after defined number of failed login attempts.	“Multiple failed logins”, “Brute force attack”
CAPTCHA	Prevents automated login attempts.	“Bot login attempts”

Risk Acceptance –
We know. We’re okay with it. **LIVE WITH IT**

Risk Mitigation –
Reduce it. (Add controls) **LOWER IT**

Risk Avoidance –
Stop doing it. (Eliminate activity) **LEAVE IT**

Risk Transference –
Shift it. (Insurance / third party) **MOVE IT**

Threat modeling =
Attack it.
Defend it.
Diagram it.

OWASP – Open Web Application Security Project
Focus: Web application security risks. (Top 10 Web Vulnerabilities Developer Guidance)

ISO – International Organization for Standardization
Global standards body. (ISO 27001 (Information Security Management Systems) not freely available-you have to pay for it.

CIS – Center for Internet Security
Provides security configuration benchmarks and controls. (Benchmarks, Controls)

PCI DSS – Payment Card Industry Data Security Standard
Standard for protecting credit card data.

NIST – National Institute of Standards and Technology-Cybersecurity Framework (CSF)

Federal guidance, Risk management framework, **Identify / Protect / Detect / Respond / Recover**

Operational –
PEOPLE*- People doing security.* Or security training(Procedures / daily actions)

Technical –
TECH *-Technology enforcing security.* (Hardware /Firewall, software controls)

Detective –
FIND *-Find it after it happens.* (Logs / alerts / monitoring)

Managerial –
POLICY*- Policies and* ***oversight****.* (Security, Policy, Governance/risk decisions)

Detective – Find it
Logs, alerts, IDS, monitoring.

Preventative – Stop it
Firewall, MFA, IPS, access controls.

Responsive – React to it
Playbooks, incident response procedures, containment actions.

Corrective – Fix it
Patch, restore, reimage, reset credentials.

Compensating – Cover it
Workaround when ideal control isn't possible.

🧠 Threat Actor Mapping

MOTIVATION	LIKELY ACTOR
FINANCIAL GAIN	Organized crime
POLITICAL AGENDA	Hacktivist
ESPIONAGE / INTELLIGENCE	Nation-state
INTERNAL GRIEVANCE	Insider

🏛️ Government Intelligence Sources

Scenario	Correct Source
Federal advisory / public alert	Government bulletin
CISA / DHS / FBI alert	Government advisory
Internal company discovery	Internal source
Incident response team	CERT / CSIRT

APIs (Application Programming Interfaces)

Structured way for applications to communicate programmatically. App-to-App communication. (You ask for the data) minimizes human engagement. **Existing product** toolkit for developers.

Webhooks

Automatic, event-driven data push to another system via HTTP. Real-time notification when something happens. It sends you data automatically.

Mitigation- Found Critical vulnerabilities and steps to resolve them. Detailed vulnerability reports include recommended mitigations, such as identifying a patch or describing a workaround. These mitigations from the security information and event management tool can help better secure a company's equipment.

Service-Level Objectives (SLOs) -Specific measurable performance targets for a service. How well, 99.9% uptime, Response time under 200ms, Recovery within 4 hours. Performance target / Availability metric.

Risk Scores - Numeric value representing the severity of a vulnerability or threat. Priority number, likelihood, impact, Exploitability EXAMPLE: CVSS score- Severity number, Prioritization

Configuration Management-Process of maintaining and controlling system settings and changes over time. primary control that ensures systems are consistently set up according to security and operational standards. By maintaining a known, compliant state across systems, administrators can prevent potential vulnerabilities due to misconfiguration or outdated setups.

The four core stages of incident response, based on the widely adopted NIST framework, are Preparation, Detection & Analysis, Containment, Eradication, & Recovery, and Post-Incident Activity,

Clean Chronological View (Operational Flow)

T0 – Detection
T1 – Incident Declaration
T2 – Scope Determination
T3 – Containment
T4 – Remediation / Respond to Recommendations
T5 – Recovery
T6 – Lessons Learned

Legal Hold- The first move This is a formal directive to preserve data because litigation, regulatory review, or investigation is anticipated.

Data validation- is a critical part of any investigation process and is used to ensure the integrity and authenticity of the data or evidence. However, it would typically come after a legal hold has been enacted, and the data has been preserved.

Data analysis- is an important step in the investigation but comes after the data has been legally held and validated.

Data preservation- is an essential component of the process to prevent any changes to the data during the investigation. But before this step, it is crucial to ensure a legal hold is in place to comply with legal requirements.

Final Order

1. Legal Hold
2. Data Preservation
3. Data Validation
4. Data Analysis

Chain of custody: Protecting the evidence - **paper trail that proves evidence was never tampered with**

Data preservation techniques -include bags with antistatic shielding to reduce the possibility of damaged or corrupted data on the electronic media by electrostatic discharge (ESD).

Data analysis-One feature of security information and event management (SIEM) tools is the ability to perform data and log analysis to detect and investigate security incidents.

Stakeholders in an incident — and this is about **who gets notified and when**

1. **Legal** (Internal Counsel) always first. Breach notification obligations, advise on liability, control communication language, invoke attorney-client privilege, legal guides -determine what you can say or can't say**, No public statements before Legal reviews them ever!**

2. **Regulators-** Notified if required by law. State Attorney General (U.S.), SEC (for public companies), HHS (**HIPAA** violations), FTC, GDPR supervisory authority (EU). Timing is often legally defined:72 hours under GDPR, varies by state breach laws. Failure to notify = fines

3. **Law enforcement-** contacted when criminal activity is confirmed, ransomware, data theft, Nation-state activity, financial fraud- FBI Cyber Division, Secret Service, financial crimes, local law enforcement

4. **Customers-** Notified when their data was exposed, credentials were compromised, service disruption affects them

Media -The media can make or break a company's reputation during an incident response. Staying ahead of salacious rumors can help mitigate the risk of damaging a reputation

Lessons learned -and after-action reports are valuable sources of information to identify recommended changes. It could be that the teams responsible for incident response were slow to act, made mistakes, or needed to be more coordinated.

ScoutSuite -Cloud security auditing tool -**Multi-cloud** configuration AWS, Azure

Prowler -AWS security auditing tool

Cuckoo-Malware sandbox

Pacu-AWS exploitation framework

☁️ Cloud Deployment Models

Model	What It Means (Exam Language)	Key Characteristics	Exam Trigger Words
Public Cloud	Shared cloud infrastructure operated by third-party provider (AWS, Azure, GCP).	Multi-tenant, internet-accessible	“Shared infrastructure”, “AWS resources”
Private Cloud	Cloud environment dedicated to a single organization.	Single-tenant, internal control	“Dedicated to one company”
Hybrid Cloud	Combination of on-premises infrastructure and public cloud working together.	Connected via VPN / Direct Connect	“Local data center + AWS”, “On-prem + cloud”
Community Cloud	Shared cloud used by organizations with similar compliance requirements.	Industry-specific sharing	“Healthcare shared environment”, “Government shared cloud”

🏗️ Cloud Service Models (Who Manages What?)

Model	You Manage	Provider Manages	Simple Memory	Example
IaaS	OS, apps, data	Hardware, storage, networking	Rent hardware	AWS EC2
PaaS	Apps, data	OS, runtime, infrastructure	Rent platform	Azure App Services
SaaS	Data only	Everything else	Rent software	Gmail, Microsoft 365
FaaS (Serverless)	Function code only	Infrastructure + scaling	Run code only	AWS Lambda

🧠 Cloud Stack Memory Ladder

IaaS → Hardware
PaaS → Platform
SaaS → Software
FaaS → Function

As you go down:
You manage less.
Provider manages more.

⚡ Serverless (FaaS) – Z.E.R.O Model

Letter	Meaning	What It Means
Z	Zero Management	No servers to patch or maintain
E	Elastic Scaling	Automatically scales up/down
R	Real-time Billing	Pay only when code runs
O	On-Demand	Runs only when triggered

Exam trap: Serverless doesn't mean no servers, It means providers manage them.

🏢 Virtualization vs Cloud (Often Confused)

Concept	Meaning	Trigger Words
Virtualization	Multiple virtual machines running on one physical host.	Hypervisor, VM, host OS
Cloud	On-demand access to shared computing resources over the internet.	Elastic, scalable, provider-managed

Virtualization = technology
Cloud = service delivery model

SASE (Secure Access Service Edge)

Concept	Meaning	Trigger Words
SASE	Cloud-based architecture combining SD-WAN with security services.	“Cloud + Network + Security”
Includes	Firewall-as-a-Service, SWG, CASB, Zero Trust	Remote workforce protection

Exam scenario:
Remote workforce + centralized cloud security → SASE.

Hybrid Cloud Scenario Recognition

If question says:
Company has:

- Local data center
- AWS/Azure resources
- Connected via VPN or Direct Connect

Answer → Hybrid Cloud.

Final Quick Recognition Grid

Public → Shared provider cloud
Private → Single organization
Hybrid → On-prem + cloud
Community → Industry-shared

IaaS → You manage OS
PaaS → You manage apps
SaaS → You manage data
FaaS → You deploy code only

SASE → Cloud-delivered network security

MITRE ATT&CK

Component	What It Means	Example	Exam Trigger Words
Tactic	The attacker's goal (the "why")	Lateral Movement	"What is the attacker trying to achieve?"
Technique	The method used (the "how")	Pass-the-Hash	"How was it done?"
Sub-Technique	More specific variation of technique	Pass-the-Hash via SMB	"Exact method variation"

Common MITRE Tactics (High-Yield)

Tactic	What It Means
Initial Access	How attacker got in
Persistence	How attacker stays in
Privilege Escalation	Gains higher permissions
Defense Evasion	Avoids detection
Credential Access	Steals credentials
Lateral Movement	Moves internally
Command & Control	Maintains remote control
Exfiltration	Steals data
Impact	Disrupts systems

Framework Comparison

Framework	Focus
Cyber Kill Chain	Attack stages
Diamond Model	Relationships between attacker & victim
MITRE ATT&CK	Specific attacker techniques

Fast Memory Formula

Tactic = Why
Technique = How
MITRE = Behavior mapping

If question says:
"Map detections to attacker behavior" → MITRE.

Cyber Kill Chain	Attack stages	Understanding attack progression
Diamond Model	Relationships between entities	Threat intel & attribution
MITRE ATT&CK	Specific techniques	Detection engineering & SOC mapping

Password Spraying: Trying one password against many accounts *"One password across many users"*
Credential Stuffing: Using breached username/password combos against other sites. *Reused credentials"*
Brute Force: Trying many passwords against one account. *"Multiple failed logins for same account"*
CASB (Cloud Access Security Broker)- Monitors and enforces security policies for cloud app usage. *"Shadow IT, Cloud data monitoring"*

EDR / XDR Explicitly

EDR = Endpoint Detection & Response
XDR = Extended Detection & Response (cross-domain)

Zero Trust: Never trust- always verify. Assume breach, Continuous authentication Micro-segmentation Identity-based access

Two-factor authentication- An identity verification method that requires **two different categories** of factors " Something you know " password", Something you have " token, phone, smart card" Something you are " biometric"

DNS-based Authentication of Named Entities (DANE) - provides a mechanism for verifying the authenticity of a server's Transport Layer Security (TLS) certificate

Sender Policy Framework (SPF) specifies **which mail servers are authorized** to send email for a domain. verifies the sender's authenticity of an email message. It helps

to prevent email spoofing by verifying the sending domain and authorizing the user to send messages from that domain**.**

🔐 **Public Key Infrastructure (PKI)-** provides a basic level of security for data in transitThe math and trust system behind secure communication Cryptographic trust framework

DomainKeys Identified Mail (DKIM)- DKIM verifies that the email was signed by the sending domain, the content wasn't altered in transit, and it uses cryptographic signatures in the email header. Good for validating that the domain authorized the message.

Sender Reputation Verification - If the sending IP/domain has a history of spam

Useful, but reputation ≠ authentication. A compromised legitimate domain could still have a good reputation.

DMARC (Domain-based Message Authentication- Reporting & Conformance- DMARC builds on SPF and DKIM. It verifies whether the domain passes authentication checks, and the message aligns with the domain policy. It specifically helps detect **spoofed or impersonated emails from recognized domains**.

TCPDump = tcpdump =
"Terminal Capture Packet Dump." Command-line packet sniffer. It captures and displays **live network traffic** on an interface. Captures packets in real time, filters traffic (IP, port, protocol,) writes captures to .pcap files, lets you analyze raw network behavior.
It operates at **Layer 2–4 mostly** (Ethernet, IP, TCP/UDP).

tcpdump -i <interface>

Captures everything on interface eth0 tcpdump -i eth0

Capture only traffic from an IP: tcpdump host 192.168.1.10

Capture traffic on port 80: tcpdump host 192.168.1.10

Capture only TCP:: tcpdump tcp

Save to file: tcpdump -i eth0 -w capture.pcap

Read from file:: tcpdump -r capture.pcap

Aircrack-ng - The **Wifi sniffer Captures "Air" packets & Cracks keys.**. Use it to sniff Wi-Fi, crack passwords, and kick devices off a network.

Recon-ng - The **Web Intelligence** King. It's a framework that gathers info from the public internet (OSINT) like emails, domains, and phone numbers.

Snort- The **Network Watchdog**. "Sniffs" the wire and barks at bad traffic.It is a "Packet-Sniffing" NIDS (Network Intrusion Detection System) that alerts you when it sees suspicious traffic based on rules.

Metasploit- [EXPLOIT]: The "Skeleton Key" for everything (Network, OS, Web) it is an all-purpose exploitation framework that can attack almost anything with a digital pulse. A framework used to launch **Exploits** against known vulnerabilities to prove you can get into a system. Metasploit is a widely used framework for penetration testing and exploiting vulnerabilities. It allows security professionals to test the security of a network by finding and exploiting vulnerabilities.

Burp Suite / OWASP ZAP: The "Scalpel" specifically for **Web Applications** only.

Splunk- is a **SIEM** (Security Information and Event Management). It collects data from *everywhere* (logs, traffic, apps) and lets you search through it like a Google for your network.

OpenVAS- is a vulnerability scanning tool that an analyst could use to identify potential vulnerabilities in a network. It is not for exploiting vulnerabilities.

Nessus: is a **Vulnerability Scanner**. It proactively "scans" your computers and servers to find out which ones are missing patches or have weak passwords.

Angry IP Scanner: A super-fast tool used for **Network Mapping**. It "pings" every IP address in a range to see who is awake and what their name is.

Wireshark- The world's most popular **Protocol Analyzer**. It doesn't just see traffic; it lets you "dissect" every single bit and byte inside a packet.

Traceroute (The GPS)- A command-line tool used to follow the **path** a packet takes from Point A to Point B. It shows every "hop" (router) along the way. On the Windows Command Prompt (**cmd**), the tool is called **tracert. If you are on a Windows CMD and tracert isn't giving you enough info, try pathping.**

While Linux and macOS use the full word traceroute, Windows shortens it. *If you type the wrong one on the exam, you'll lose the "simulation" point!*

Type this into the cmd line

tracert google.com

Distributed Denial-of-Service (DDoS) Attack -A DDoS attack is when many compromised systems (a botnet) flood a target with traffic to overwhelm it and make it unavailable. An unusual spike in network traffic could indicate a DDoS attack.

Ping Sweep (The Doorbell)- Sends ICMP Echo Requests (pings) to a **range** of IP addresses. **Goal:** To see which computers are "alive" (turned on). **Trigger:** "Who is home?" / Discovery.

Port Scan (The Door Handle)- Checks a **single** IP address for open communication "ports" (like 80 for web, 21 for FTP). **Goal:** To see what services/apps are running on that specific machine. **Trigger:** "Is the web server open?" / Enumeration.

TCP Sweep (The Handshake)- A "Ping Sweep" for networks that block standard pings. It sends a **TCP SYN** packet to a common port (like 80 or 443) across many IPs. **Goal:** Finding "alive" hosts when ICMP is disabled. **Trigger:** "Bypassing Firewall" / Reliability.

UDP Sweep (The Message in a Bottle)- Sends UDP packets to common ports (like DNS 53 or SNMP 161) across many IPs. **Goal:** Finding hidden services that don't use TCP. **Trigger:** "Finding non-standard services" / Slow & Unreliable (since UDP doesn't "handshake").

Man-in-the-middle (MitM) — The Eavesdropper

A hacker sticks themselves between you and the person you're talking to (like your bank). They see everything you send and can even change the data before it reaches the destination. (To spy or Modify Traffic)

SQL Injection (SQLi) — The Database Backdoor

A hacker types "database commands" into a web form (like a username box). If the website isn't protected, it sends those commands to the database, letting the hacker see or delete all the data. (to steal or change Data)

Input validation / Database leak / ' OR 1=1 --.

Cross-Site Request Forgery (CSRF) — The Identity Thief

The hacker tricks your browser into doing something on a website where you're already logged in (like clicking a link that secretly "transfers money" from your bank account). To force an action by a user.

Beaconing — The "Phone Home"

After a computer is infected, the malware sends a signal back to the hacker's server at regular intervals (like every 30 seconds) to ask for new instructions.

C2 (Command & Control) / Heartbeat / Regular intervals. Update the malware/c2

NMAP: tool is for network exploration and security auditing, open ports, services and service enumeration.

🕵️ **Maltego**

Maltego = OSINT + relationship mapping tool.

Maltego is an OSINT and link analysis tool that gathers publicly available data and visualizes relationships between entities in a graphical format.

Burp Suite (Community Edition) — The Web Scalpel

"Custom Web Application" and **"Comprehensive Testing** Burp Suite is an **Interception Proxy**. It sits between your browser and the website you're testing. It lets you "pause" a request, change the data (like changing a price from $100 to $1), and then send it to the server.+1 **Web Apps / SQLi / XSS / Manual Testing**.

OWASP Zed Attack Proxy (ZAP) is an **open-source web application security testing tool** used to find vulnerabilities in web apps.

It's built and maintained by **OWASP**.

Nikto is an open-source **Web Server Scanner**. Unlike Burp Suite (which is a "manual scalpel" for web apps), Nikto is an "automatic shotgun" that fires thousands of tests at a web server to find dangerous files, outdated software, and misconfigurations across multiple sites

Wazuh is a free, open-source **XDR (Extended Detection and Response)** and **SIEM** platform. Think of it as the "Security Bodyguard" for your individual computers (endpoints) and your cloud environment. It doesn't just watch the network; it watches the *insides* of your servers.

Prowler is an open-source security tool specifically designed for **Cloud Security Posture Management (CSPM)**. It focuses on AWS, Azure, and Google Cloud (GCP) to ensure your cloud "house" is locked up tight and follows best practices.

The **GNU Debugger (GDB)** is the industry-standard tool for "cracking open" a program while it's running to see exactly what's happening inside the code. In cybersecurity, it's a favorite for **Reverse Engineering** and **Exploit Development**.

Pacu — The Cloud Attacker

If **Prowler** is the "Cloud Inspector," **Pacu** is the "Cloud Burglar." It is an open-source **AWS exploitation framework** (built by Rhino Security Labs) used to test how an attacker could move through your Amazon cloud environment.

Tenable.io — The Corporate Scanner

Tenable.io is the **Cloud-based version of Nessus**. While "Nessus Professional" is a tool for one person, **Tenable.io** is a massive platform for a whole company to manage their "Vulnerability Management" program.

Suricata — The Network Sentinel

Suricata is a high-performance **IDS/IPS** (Intrusion Detection/Prevention System). It is the modern rival to **Snort**. It watches network traffic in real-time and alerts you (or blocks the traffic) if it sees a known attack pattern.

Arachni is a high-performance, open-source **Web Application Security Scanner (DAST)**. It's essentially a "bot" that crawls through a website, finds every page, link, and form, and then automatically tests them for security vulnerabilities like SQL injection or Cross-Site Scripting (XSS).

Regular expressions -are a powerful tool for defining and searching for specific patterns in text data. "Search Pattern" on steroids. It is a specialized string of characters used to find, manage, and manipulate text based on specific "shapes" of data rather than exact words.

Python — The Automation Master

Python is the "Language of Cybersecurity." It is a high-level, general-purpose programming language known for being easy to read. Analysts use it to automate repetitive tasks, parse complex logs, and even write custom exploits.

Shell Scripts — The OS Whisperer

A Shell script (like **Bash** on Linux or **PowerShell** on Windows) is a list of commands that the Operating System executes in order. It’s used to talk directly to the computer’s "engine."

JavaScript — The Web's Engine (and Weapon)

JavaScript is the language that makes websites interactive. In security, analysts study it to understand how **Cross-Site Scripting (XSS)** works or how a malicious website might steal a user's session.

XML (eXtensible Markup Language)

XML uses **tags** (like <tag>data</tag>) to define structure. It is the "grandfather" of data formats—highly structured, very strict, but a bit "wordy" (verbose).

JSON (JavaScript Object Notation) JSON is the modern standard for web APIs. It uses **Key-Value pairs** and curly braces {}. It is much lighter and faster to read for both humans and computers than XML.

CSV (Comma-Separated Values) -CSV is the simplest format. It’s just plain text where each line is a record and each piece of data is separated by a **comma**.

YAML (Yet Another Markup Language) YAML is designed to be **extremely human-readable**. It relies on **indentation** (spaces) rather than tags or braces. It is the go-to format for "Configuration Files" (like for Docker or Kubernetes).

When an **application** is behaving strangely or producing "unexpected output," the most direct evidence of what is happening inside its "brain" is the **Application Log**.

When a SIEM alerts you to a sudden spike in **"high-privilege actions,"** it usually means an attacker has successfully gained access and is now trying to create a "permanent" home for themselves. Creating a new, hidden administrator account is the classic way hackers maintain **persistence**.

When a security analyst spots **"abnormal behavior"** in a system, they are by definition identifying an **anomaly**. In the world of cybersecurity, an anomaly is anything that deviates from the established "baseline" of what is considered normal or expected.

Remote Code Execution: An attacker runs their own code on the target system remotely. What attacker gets: Full System Control (Worst case)
RCE: Run Code Everywhere

Cross-Site Request Forgery (CSRF)— (**Tricks the User**) tricks a Logged-in users browser into sending an unauthorized request to a site they trust.

The attacker doesn't steal credentials; they abuse an existing session
CSRF- *Click stuff Request forged*

Server-Side Request Forgery (SSRF) (Tricks the Server)

Attacker forces a **server** to make unauthorized requests on their behalf.

Instead of the attacker sending the request directly, the **vulnerable server sends it**.

Trigger words on exam:
"Server fetches URL provided by user"
"Access internal resources"
"Cloud metadata exposure"
"Backend request manipulation"

Quick difference from CSRF:
CSRF = tricks the **user's browser**
SSRF = tricks the **server itself**

If you see "internal network access via web app," think SSRF immediately.

Directory Traversal: (../escapethe_folder) Accessing files outside the intended directory by manipulating paths (eg.,../)
What the attacker gets: Config files, passwords, system files

Think ?page=http://evil.com/shell.php. This is high-risk because it leads directly to Remote Code Execution (RCE) by pulling in outside code.

Local File Inclusion (LFI)- (**Loads files Internally**) Forcing a web app to read or execute a file already sitting on the **local** server.

Think /etc/passwd. The attacker uses a "Directory Traversal" trick (like ../../) to trick the app into showing sensitive system files

Remote File Inclusion (RFI)— (**Loads files Externally**) Forcing a web app to load a malicious file from a third-party or remote server.

SQL Injection (SQLi)— (**Talks directly to the Database**) Inserting malicious SQL code into input fields to manipulate or steal data from the back-end database. Think ' OR 1=1 --. SQLi = Database data theft.
What attacker gets: Data theft, login bypass, data deletion

Address Space Layout Randomization (ASLR) (Memory Randomization Defense) Security control that **randomizes memory locations** of system and application processes to prevent attackers from predicting where code executes.

Time Synchronization: Ensures all devices, systems & applications on a network use the same precise time. NTP is easy as 1-2-3 Network timed protocol

Log Ingestion: Process of collecting, transmitting, parsing and storing logs into a centralized system (usually a SIEM)

Threat Actors & Advanced Persistent Threats (APTs)

- **Threat Actor:** A person or entity responsible for an event identified as a security risk or incident.
- **APTs (Advanced Persistent Threats):** Well-funded, highly skilled attackers (often nation-states) that enter quietly and stay long-term to steal or manipulate data.
    - **Goals:** Real human adversaries with clear objectives like espionage, IP theft, or disruption.
    - **Tactics:** Use custom malware, zero-days, "living-off-the-land" tools, and careful cleanup to avoid detection.
- **Command and Control (C2):** The phase where an adversary establishes a communication channel with a successfully exploited target.
- **Beaconing:** A technique used by malware to maintain a covert communication channel with a C2 server.

---

2. Threat Intelligence Frameworks

- **CybOX (Cyber Observable eXpression):** Describes the **Data**—raw technical indicators like file hashes and registry keys.
- **STIX (Structured Threat Information eXpression):** The **Language/Format** used to give the data meaning and structure.
- **TAXII (Trusted Automated eXchange of Intelligence Information):** The **Delivery/Transport** method used to move intel between systems.

---

3. Vulnerability Management & Scanning

- **Attack Surface:** Points where a network or application receives external inputs that are potential exploit vectors.
- **Vulnerability Scan Report:** Essential inclusions are the **Affected Hosts** and the **Risk Score**.
- **Agent-Based Scanning:** Ideal for geographically diverse workforces with dynamic IPs to reduce network traffic.
- **Baseline Scan:** Capturing "Normal First" behavior to spot future anomalies.
- **Internal Scan:** Performed from "inside" to find vulnerabilities an insider could exploit.
- **Fuzzing:** Sending random/malformed input to an application to trigger crashes ("Break it with junk").
- **End of Support (EOS):** When a product no longer receives patches, it creates critical vulnerabilities.

Recovery Metrics

RTO = Recovery Time Objective
RPO = Recovery Point Objective

Defensive Operations (SOC, SIEM, SOAR)

- **SOC (Security Operations Center):** A centralized team for continuous monitoring and incident response.
- **SIEM:** Collects and correlates logs from across the environment to detect incidents.
- **SOAR:** Automates incident response using **Playbooks** to reduce workload.
- **Webhooks:** An event-driven "Trigger" that sends real-time data between systems.
- **IDS (Intrusion Detection System):** Monitors activity and alerts, but **does not stop** the action.
    - **NIDS:** Network-based.
    - **HIDS:** Host-based.

🔐 Data Protection & Cryptography

📦 Data States

Data State	What It Means	Protection Method	Exam Trigger Words
Data at Rest	Stored data (disk, database, backups)	Disk encryption, database encryption	“Stored on server”, “Database protection”
Data in Transit	Data moving across network	TLS, HTTPS, VPN	“Secure transmission”, “Encrypt traffic”
Data in Use	Data actively being processed in memory	Access controls, memory protection	

Memory:
Rest = stored
Transit = moving
In Use = being processed

🔐 Encryption & Cryptography Types

Type	What It Means	Key Feature	Exam Trigger Words
Symmetric Encryption	Uses one shared key for encryption & decryption	Fast, efficient	“Shared secret key”
Asymmetric Encryption	Uses public/private key pair	Key exchange, digital signatures	“Public key”, “Private key”
Hashing	One-way function to verify integrity	Cannot be reversed	“Verify integrity”, “Password storage”

Memory:
Symmetric = Same key
Asymmetric = Key pair
Hash = No reverse

Public Key Infrastructure (PKI)

Component	Purpose	Exam Trigger Words
PKI	Framework that manages digital certificates & trust	“Certificate authority”, “Trust model”
Certificate Authority (CA)	Issues and validates certificates	“Trusted issuer”
Digital Certificate	Binds public key to identity	“TLS certificate validation”

PKI = The trust system behind TLS/HTTPS.

RAID vs Backup (Critical Distinction)

Concept	What It Does	What It Does NOT Do	Exam Trap
RAID	Provides redundancy & availability	Does NOT protect against deletion or ransomware	“High availability”
Backup	Copies data for recovery	Does NOT provide live redundancy	“Restore after loss”

Memory:
RAID = uptime
Backup = recovery

If ransomware encrypts files:
RAID won’t save you.
Backup will.

Quick Recognition Map

Encrypt stored data → Data at rest
Encrypt traffic → Data in transit
Verify password integrity → Hash
Key exchange → Asymmetric
Fast bulk encryption → Symmetric
Trust certificates → PKI
Prevent downtime → RAID
Recover deleted data → Backup

Fast Exam Memory Rules

Rest → Encrypt disk
Transit → Encrypt traffic
In Use → Protect memory

Symmetric → Fast
Asymmetric → Key exchange
Hash → No reverse

PKI → Trust system for certificates

RAID → Prevent downtime
Backup → Recover lost data

If ransomware hits:
RAID fails you.
Backup saves you.

📊 MTTR vs MTBF (Combined Table)

Metric	Full Name	What It Measures	Formula	Higher Is Better?	Exam Trigger Words	What It Tells You
MTTR	Mean Time To Respond (sometimes Mean Time To Repair in other contexts — read carefully)	How quickly incidents are handled and contained	Total response time ÷ Number of incidents	❌ No (lower is better)	"Response speed," "containment time," "incident handling efficiency"	How fast your team reacts
MTBF	Mean Time Between Failures	How reliable a system is before failing again	Total uptime ÷ Number of failures	✅ Yes (higher is better)	"System reliability," "stability," "failure rate reduction"	

Plain English:
How long does the system run before it breaks again?

Exam trap:
MTBF applies to repairable systems.
MTTF (Mean Time To Failure) is for non-repairable systems.

🏢 Hot Site vs Warm Site vs Cold Site

Feature	Hot Site	Warm Site	Cold Site
Equipment	Fully configured	Partially configured	Empty facility
Data	Real-time replicated	Periodic backups	No current data
Staff Ready?	Yes	Some setup required	No
Recovery Time (RTO)	Minutes to hours	Hours to days	Days to weeks
Cost	$$$$ (Most expensive)	$$$	$ (Cheapest)
Best For	Critical systems	Important systems	Low-priority systems

Plain English Breakdown

Hot Site
Plug and play. Power goes out at HQ, flip the switch, you're live.

Warm Site
Hardware exists, but you need to restore data and configure before going live.

Cold Site
Basically an empty building with power and networking. Bring everything yourself.

Exam Pattern Recognition

If question says:

- "Immediate failover required" → Hot site
- "Moderate cost but reasonable recovery time" → Warm site
- "Budget constraints, long RTO acceptable" → Cold site
- "Improve reliability metric" → MTBF
- "Improve incident response time" → MTTR

🔁 Failover vs Failback

Feature	Failover	Failback
What It Is	Switching operations to a backup system	Returning operations to the original primary system
When It Happens	During outage or failure	After primary system is restored
Automatic or Manual?	Often automatic	Often manual or controlled
Goal	Maintain availability	Restore normal operations
Exam Trigger Words	"Automatic switchover," "secondary site activated."	"Return to primary," "restore original configuration"

Plain English

Failover = "Primary died, go to backup."
Failback = "Primary fixed, go back home."

Exam trap: Failover is not permanent migration. It's temporary continuity.

💉 Tabletop Exercise vs Simulation Test

Feature	Tabletop Exercise	Simulation Test
Type	Discussion-based	Operational / Live-action
Systems Affected	No real systems touched	Systems may be actively tested
Real Downtime?	No	Possibly
Realistic Pressure?	Low	High
Cost	Low	Higher
Purpose	Validate plans on paper	Validate plans under realistic conditions
Exam Trigger Words	"Walkthrough," "discussion," "policy review"	"Live test," "real-time scenario," "operational validation"

What This Means
Tabletop = "Let's sit in a room and talk through what we would do."
Simulation = "Let's actually simulate the attack or outage."

Exam trick:
If no real systems are affected → Tabletop.
If systems are actively tested → Simulation.

🔐 Windows Security Event IDs for CySA+

Event ID	What It Means	What To Look For	Exam Pattern
4624	Successful logon	Logon Type, Account Name, Source IP	Normal activity unless unusual time/location
4625	Failed logon	Failure reason, Source IP, repeated attempts	Brute force if repeated
4672	Special privileges assigned	Admin-level login	Privilege escalation indicator
4688	New process created	Suspicious executable launched	Malware execution
4768	Kerberos TGT requested	Initial domain authentication	Domain login activity
4769	Kerberos service ticket	Accessing network service	Lateral movement clue

```
Event ID: 4625

Account: admin

Source IP: 192.168.1.45

Attempts: 30 within 2 minutes
```

That = brute-force attack.

🖥️ Windows Security Logs

Field	What It Means	What To Watch For	Attack Indicator
Event ID	Type of activity	4624, 4625, 4672, 4688	Brute force, privilege escalation
Account Name	User involved	Admin account used oddly	Lateral movement
Logon Type	How login occurred	Type 3 = Network login	Remote access
Source IP	Where request came from	External or unusual internal IP	Attack source
Failure Reason	Why login failed	Bad password vs locked account	Password spray

🌐 Apache / Web Server Access Logs

```
192.168.1.10 - - [10/Feb/2026:14:32:10] "GET /admin HTTP/1.1" 404 512
```

Field	Meaning	What To Watch	Attack Indicator
IP Address	Client IP	Many requests from one IP	Scanning
Method	GET / POST	POST to login pages	Credential attack
URL Path	Resource accessed	/admin, /etc/passwd	Directory traversal
Status Code	Server response	200, 404, 500	404 spikes = recon
User-Agent	Browser type	curl, python script	Automation

Common Status Codes:

- **200** = Success
- **403** = Forbidden
- **404** = Not found (scanning indicator)
- **500** = Server error

🔥 Firewall Logs

```
DENY TCP 192.168.1.5:445 → 10.0.0.10:22
```

Field	Meaning	What To Watch	Attack Indicator
Action	Allow or Deny	Many denies	Scan or brute force
Protocol	TCP / UDP / ICMP	Port 22, 3389, 445	Targeted service
Source IP	Origin	External IP hitting many ports	Port scan
Destination Port	Service	3389 = RDP, 22 = SSH	Remote access attempt

🛡️ IDS / IPS Logs (Snort Style)

```
Csharp
```

```
[1:1000001:0] ET SCAN Nmap Scripting Engine User-Agent
```

Field	Meaning	What To Watch	Attack Indicator
Signature ID	Rule triggered	Known exploit signatures	Malware / scan
Classification	Type of attack	Attempted Admin	Privilege escalation
Source IP	Attacker	Internal vs external	Compromised host
Destination IP	Target	Sensitive server	Targeted attack

📡 NetFlow Logs

Field	Meaning	What To Watch	Attack Indicator
Source IP	Origin	One host sending large data	Exfiltration
Destination IP	Target	Unknown external IP	C2
Bytes Sent	Volume	High outbound traffic	Data theft
Duration	Length of session	Long persistent sessions	Beaconing

Linux Syslog

Example:

nginx

```
Failed password for root from 192.168.1.50 port 22 ssh2
```

Field	Meaning	What To Watch	Attack Indicator
Username	Targeted account	root attempts	Privilege attack
Source IP	Origin	Repeated attempts	Brute force
Port	Service used	22 = SSH	Remote login attack

SIEM Correlation Output

Field	Meaning	What To Watch	Attack Indicator
Alert Name	Type of event	“Multiple failed logins”	Brute force
Severity	Risk level	High severity	Immediate action
Time Range	Attack timing	Rapid attempts	Automation
Affected Assets	Systems hit	Critical server	Targeted attack

20 Common Ports You Must Know

Cyber Edition

FTP **TCP 21** File Transfer Protocol	**SSH** **TCP 22** Secure Shell for secure login	**Telnet** **TCP 23** Remote login (unsecured)	**SMTP** **TCP 25** Simple Mail Transfer Protocol	**DNS** **TCP/UDP 53** Domain Name System queries
DHCP Server **UDP 67** Dynamic Host Configuration Protocol	**DHCP Client** **UDP 68** Dynamic Host Configuration Protocol	**HTTP** **TCP 80** Hypertext Transfer Protocol	**POP3** **TCP 110** Post Office Protocol V3	**NTP** **UDP 123** Network Time Protocol
NetBIOS **TCP 139** NetBIOS service	**IMAP** **TCP 143** Internet Message Access Protocol	**HTTPS** **TCP 443** Secure HTTP (SSL/TLS)	**SMB** **TCP 445** Server Message Block protocol	**Oracle DB** **TCP 1521** Oracle DB communication port
MySQL **TCP 3306** MySQL database communication	**RDP** **TCP 3389** Remote Desktop Protocol	**PostgreSQL** **TCP 5432** PostgreSQL database communication	**LDAP** **TCP/UDP 389** Lightweight Directory Access Protocol	**SNMP** **UDP 161** Simple Network Management Protocol

CySA+ Log Recognition Cheat Sheet

1️⃣ SQL Injection (Web Server Log – Apache Style)

```
192.168.1.50 - - [16/Feb/2026:10:00:01 -0500] "GET /login.php?user=admin' OR
'1'='1' --&pass=test HTTP/1.1" 200 512 "-" "Mozilla/5.0"
```

Give-away:

```
' OR '1'='1' --
```

Answer:
SQL Injection (Authentication bypass attempt)

2️⃣ Local File Inclusion / Directory Traversal

```
192.168.1.50 - - [16/Feb/2026:10:05:22 -0500] "GET
/view.php?file=../../../../etc/passwd HTTP/1.1" 200 1245 "-" "Mozilla/5.0"
```

Give-away:

```
../../../../etc/passwd
```

Answer:
Local File Inclusion (Directory Traversal)

3️⃣ Command & Control (Beaconing – Firewall/NetFlow Style)

```
Feb 16 10:00:00 FW1 ALLOW TCP 10.0.0.5:49532 -> 54.23.1.2:443 bytes=512

Feb 16 10:00:30 FW1 ALLOW TCP 10.0.0.5:49532 -> 54.23.1.2:443 bytes=512

Feb 16 10:01:00 FW1 ALLOW TCP 10.0.0.5:49532 -> 54.23.1.2:443 bytes=512

Feb 16 10:01:30 FW1 ALLOW TCP 10.0.0.5:49532 -> 54.23.1.2:443 bytes=512
```

Give-away:

```
   Exact 30-second interval, Identical packet size, Same destination IP
```

Answer:

C2 Beaconing

4️⃣ Brute Force (Linux SSH Log)

```
Feb 16 10:15:01 server sshd[1234]: Failed password for root from 192.168.5.10 port 49822 ssh2

Feb 16 10:15:02 server sshd[1234]: Failed password for root from 192.168.5.10 port 49823 ssh2

Feb 16 10:15:03 server sshd[1234]: Failed password for root from 192.168.5.10 port 49824 ssh2

Feb 16 10:15:04 server sshd[1234]: Failed password for root from 192.168.5.10 port 49825 ssh2
```

Give-away:

```
Rapid repeated failures, Same username, Same source IP
```

Answer:

Brute Force Attack

5️⃣ Cross-Site Scripting (Web Log – Reflected XSS)

```
192.168.1.50 - - [16/Feb/2026:10:20:11 -0500] "GET /search?q=<script>alert('XSS')</script> HTTP/1.1" 200 742 "-" "Mozilla/5.0"
```

Give-away:

```
<script>alert('XSS')</script>
```

Answer:

Reflected XSS

***CySA+ 2026 Pro-Tips:**

On the exam, if you see **"Parameterized Queries"** or **"Stored Procedures,"** the answer is almost always **SQLi**. If you see **"Anti-CSRF Tokens"** or **"SameSite Cookies,"** the answer is **CSRF**.

1. SIEM vs. SOAR— (Know the Difference)

SIEM is for **Watching** (Logs, alerts, dashboards). **SOAR** is for **Acting** (Playbooks, automation, API integration).

- *Exam Tip:* If the question asks how to **remediate faster**, pick **SOAR**.

2. The "CVSS" Score— (Prioritize the Fix)

CVSS 9.0+ is Critical. **7.0–8.9** is High.

- *Exam Tip:* If you have 5 vulnerabilities, **always** fix the Critical/High ones on "External/Public" servers first.

3. Nmap Flags— (The "Big Three")

- -sS: **Stealth** (Half-open) scan. Fast and quiet.
- -sV: **Version** detection. Tells you exactly what's running.
- -O: **OS** fingerprinting. Tells you the operating system.

4. "The Log" is King— (Evidence Hunt)

If a user is locked out, check **Authentication Logs**. If a web server is slow, check **HTTP Access Logs**. If a database is leaked, check **SQL/Audit Logs**.

5. False Positives— (The Analyst's Nightmare)

A **False Positive** is a "Fire Alarm" going off when there is **no fire**.

- *Exam Tip:* The fix is usually **Tuning** the alert or adjusting the "Threshold" in the SIEM.

6. Beaconing— (Spotting Malware)

(Traffic at regular intervals) If you see a internal IP hitting an external IP every **exactly** 30 seconds, it's a **C2 (Command & Control) Beacon**.

- *Exam Tip:* Look for "heartbeat" patterns in network logs.

7. Isolated vs. Segmented— (Containment)

Isolation = Pull the plug (Disconnect the host). **Segmentation** = Put it in a digital cage (VLAN/Sandbox).

- *Exam Tip:* If a worm is spreading, **Isolate** immediately.

8. Data Sovereignty— (Where is the Data?)

(Legal/Geography stuff) If the question mentions **GDPR** or data stored in another country, the answer is **Data Sovereignty**.

9. Risk Labels— (Impact vs. Likelihood)

Inherent Risk: The risk *before* you do anything. **Residual Risk:** The risk *leftover* after you put in a firewall/control.

- *Exam Tip:* You can never have **Zero** Residual Risk.

10. The "Best" Answer— (Read Carefully)

CySA+ loves asking for the **"Next step"** or **"First step."**

- *First step:* Usually **Identification** (confirming the hit).
- *Next step:* Usually **Containment** (stop the bleeding).

11. The "Containment" Hierarchy—

(Stop the Bleed First) When an incident is confirmed, your priority is always to **contain** before you **analyze**.

- **Worm/Virus spreading?** Isolate the host from the network immediately.
- **Data being exfiltrated?** Shut down the specific service or port.
- **Unauthorized Login?** Disable the user account.
- *Exam Tip:* If the question asks for the "Next Step" after confirming an active breach, look for the answer that **minimizes the damage** (Isolation/Containment) before you worry about "Investigation" or "Recovery."