Glossary-CEH

🔐 Core Security Concepts

- **CIA Triad**: Confidentiality, Integrity, Availability – the foundation of InfoSec.
- **Authenticity**: Data is from a verified, trusted source.
- **Non-repudiation**: Ensures actions cannot be denied later.
- **Auditing & Accountability**: Tracking user activities.
- **Threat**: Potential cause of harm.
- **Vulnerability**: Weakness in a system.
- **Exploit**: Code/method that takes advantage of a vulnerability.
- **Payload**: Malicious part of an exploit.
- **Risk**: Likelihood and impact of a threat exploiting a vulnerability.

🧠 Hacking Terminology

- **Hack Value**: Perceived prestige of compromising a system.
- **Zero-Day**: Vulnerability unknown to the vendor, with no fix yet.
- **Daisy Chaining**: Using one compromised system to access others.
- **Doxing**: Public exposure of someone's personal info.
- **Pivoting**: Moving laterally within a network after access.
- **EISA**: Framework to align business and security architecture.

🧑‍💻 Types of Hackers

- **White Hat**: Ethical hacker with permission.
- **Black Hat**: Malicious hacker.
- **Gray Hat**: Hacks without permission but not for evil.

- **Script Kiddie**: Uses tools/scripts without deep knowledge.
- **Hacktivist**: Hacks for social/political causes.
- **State-Sponsored**: Backed by a nation.
- **Suicide Hacker**: Doesn’t care about consequences.
- **Cyberterrorist**: Uses cyberattacks to spread fear.

🛠️ Common Tools

- **Nmap**: Port scanner and host discovery.
- **Nessus**: Vulnerability scanner.
- **OpenVAS**: Open-source vulnerability scanning tool.
- **Nikto**: Web server scanner.
- **Metasploit**: Pen testing and exploit development framework.
- **Splunk**: SIEM platform for log management.
- **ArcSight**: Enterprise SIEM solution.
- **ELK Stack**: Elasticsearch, Logstash, Kibana – open-source SIEM suite.

🌐 Protocols & Attacks

- **MITM**: Intercepting communications between two parties.
- **ARP Spoofing**: Faking MAC addresses to mislead network devices.
- **DNS Poisoning**: Redirecting DNS queries to malicious sites.
- **DoS/DDoS**: Overloading systems to make them unavailable.
- **SQL Injection**: Injecting SQL code via input fields.
- **XSS**: Injecting malicious scripts into web pages.
- **Buffer Overflow**: Overwriting memory to execute arbitrary code.
- **Brute Force**: Trying many passwords until one works.
- **Social Engineering**: Tricking people into giving access.

- **Phishing**: Fake emails or websites to capture credentials.

🔎 Phases of Ethical Hacking

1. **Reconnaissance** – Info gathering (Passive/Active)
2. **Scanning** – Port and vulnerability detection
3. **Gaining Access** – Exploiting vulnerabilities
4. **Maintaining Access** – Backdoors, trojans
5. **Covering Tracks** – Log deletion, obfuscation

🏗️ Security Architecture & Access Models

- **MAC**: Mandatory Access Control – based on labels.
- **DAC**: Discretionary Access Control – owner decides access.
- **RBAC**: Role-Based Access Control – access based on roles.
- **Least Privilege**: Only give needed permissions.
- **Separation of Duties**: Split roles to reduce risk.

🔍 Vulnerability & Threat Databases

- **CVE**: Common Vulnerabilities and Exposures – public list.
- **CVSS**: Scores vulnerabilities by severity.
- **NVD**: US government vulnerability database.

📄 Risk Management & Threat Modeling

- **Identify → Assess → Respond → Monitor → Report**
- **Risk Matrix**: Likelihood vs. impact visualization.
- **Threat Modeling**: Analyzing app risks step-by-step.
- **Attack Vector**: Path used by an attacker.

🔐 IAM (Identity and Access Management)

- **Identification**: Claiming an identity (e.g., username).
- **Authentication**: Verifying identity (password, biometric).
- **Authorization**: Granting access to resources.
- **Accounting**: Logging actions for audits (non-repudiation).

Authentication Factors:

- Something you know (password)
- Something you have (token)
- Something you are (biometric)
- Something you do (signature)
- Somewhere you are (location)

🔄 Incident Response Process

1. **Preparation** – Setup roles and tools
2. **Detection & Analysis** – IDS, SIEM, reports
3. **Containment** – Isolate systems
4. **Eradication & Recovery** – Remove threats and restore
5. **Post-Incident** – Documentation, learning, reporting

Forensic Tools: Logs, memory dumps, packet captures

🧪 Penetration Testing

- **Black Box**: No prior knowledge
- **White Box**: Full knowledge
- **Gray Box**: Partial knowledge

Phases:

1. Preparation

2. Assessment
3. Post-Assessment

🧾 Laws & Standards

- **HIPAA**: Health data privacy law
- **SOX**: Corporate financial transparency law
- **PCI-DSS**: Protects credit card data
- **FISMA**: Federal agency info security standards
- **GDPR**: EU data privacy regulation
- **COBIT**: IT governance framework
- **ITIL**: Best practices for IT service management
- **OSSTMM**: Open-source testing methodology
- **NIST 800-53**: Security control framework for federal IT
- **DMCA**: US copyright protection law
- **GLBA**: Protects consumer financial data

🧯 Controls & Countermeasures

- **Preventive**: Stop events (firewalls, access controls)
- **Detective**: Identify incidents (IDS, logs)
- **Corrective**: Fix damage (patching, reconfiguring)
- **Deterrent**: Discourage attempts (signs, warnings)
- **Compensating**: Alternatives when primary controls fail
- **Defense in Depth**: Multiple layered defenses

🧰 SIEM Concepts

- **Aggregation**: Collecting logs from multiple sources

- **Correlation**: Analyzing relationships between events
- **Normalization**: Standardizing log formats
- **Alerts**: Notifications of suspicious behavior
- **WORM**: Write Once Read Many – log integrity

💾 Backup & Recovery

- **Cold Site**: Basic infrastructure, slow recovery
- **Warm Site**: Equipment ready, data brought in
- **Hot Site**: Fully mirrored site, real-time sync

📑 Security Policies & Documentation

- **Policy**: High-level rules (e.g., Acceptable Use)
- **Procedure**: Step-by-step instructions
- **Guideline**: Suggested practices

Policy Types:

- **Promiscuous**: No restrictions
- **Permissive**: Allow all but block known risks
- **Prudent**: Block most, allow some with logging
- **Paranoid**: Block everything

🎯 Social Engineering / Psychological Attacks

- **Phishing**: Sending fraudulent emails pretending to be legitimate to steal sensitive data.
- **Spear Phishing**: Targeted phishing directed at a specific individual or organization.
- **Whaling**: Phishing that targets high-level executives ("big fish").

- **Vishing**: Voice phishing over phone calls.
- **Smishing**: SMS/text message phishing.
- **Pretexting**: Creating a fake scenario to trick someone into revealing information.
- **Impersonation**: Pretending to be someone trusted to gain unauthorized access.
- **Shoulder Surfing**: Watching someone’s screen or keystrokes to gather info.
- **Dumpster Diving**: Retrieving discarded documents to gather sensitive data.
- **Tailgating**: Entering a secure area by closely following an authorized person.
- **Piggybacking**: Gaining entry with the consent of an authorized person.
- **Quid Pro Quo**: Offering a benefit in exchange for information.

🌐 Network Attacks & Info Gathering

- **Sniffing**: Intercepting network traffic to gather unencrypted data.
- **Spoofing**: Faking the identity of a device or user (IP, MAC, email).
- **Snooping**: Unauthorized access to someone's data, files, or systems.
- **Pharming**: Redirecting a website’s traffic to a fake website to steal data.
- **Session Hijacking**: Taking over a session by stealing session tokens.
- **DNS Spoofing / Poisoning**: Altering DNS records to redirect traffic to malicious sites.
- **ARP Spoofing**: Associating attacker’s MAC address with IP of a trusted host.
- **MAC Spoofing**: Changing the MAC address to bypass access controls.
- **Wardriving**: Searching for Wi-Fi networks while driving around.
- **Bluejacking**: Sending unsolicited messages over Bluetooth.
- **Bluesnarfing**: Unauthorized access to data via Bluetooth.

🧠 Other Useful Recon/Attack Terms

- **OSINT (Open Source Intelligence)**: Gathering public info from the internet.
- **Footprinting**: Mapping a target's network or systems.
- **Enumeration**: Extracting usernames, machine names, shares, etc.
- **Banner Grabbing**: Collecting service banners to determine software versions.
- **Port Scanning**: Discovering open ports and services on a target system.
- **Network Mapping**: Visualizing a network's structure and components.
- **MITM (Man-in-the-Middle)**: Intercepting and altering communications between parties.
- **Replay Attack**: Re-sending captured data packets to trick the system.
- **Clickjacking**: Tricking users into clicking something different than they think.
- **Typosquatting**: Registering domain names similar to legitimate ones to mislead users.

🧠 Advanced Threat & Malware Terms

- **Polymorphic Malware**: Malware that constantly changes its code to evade detection.
- **Fileless Malware**: Lives in memory and avoids writing files to disk.
- **Logic Bomb**: Malicious code that triggers on specific conditions.
- **Command and Control (C2)**: Server used by attackers to control compromised systems.
- **Rootkit**: Hides the presence of malicious activity on a system.

📱 Modern & Emerging Threats

- **Rogue Access Point**: Unauthorized Wi-Fi AP set up to lure users.
- **Evil Twin**: A fake Wi-Fi AP mimicking a legitimate one.
- **Drive-by Download**: Malware installed without user's knowledge via compromised sites.

- **IoT Exploits**: Attacks targeting smart devices like cameras, thermostats, etc.

🌐 Cloud & Virtualization

- **Hyperjacking**: Attacking the hypervisor layer in a virtualized system.
- **VM Escape**: Breaking out of a virtual machine to control the host.
- **Cloud Hopper**: APT targeting cloud service providers to attack customers.
- **Shadow IT**: Unauthorized IT systems used within an organization.

🔐 Authentication & Cryptography

- **Rainbow Tables**: Precomputed hash tables used for cracking passwords.
- **Salting**: Adding random data to passwords before hashing to prevent rainbow table attacks.
- **Pass the Hash**: Using stolen hash values to authenticate without cracking them.
- **Kerberoasting**: Extracting service tickets in Kerberos to brute-force passwords offline.
- **Credential Stuffing**: Using leaked username/password combos to breach other services.

🤔 Leftover / Rarely Asked But Known Terms

These are **super rare**, but here's a few more if you want to go nuclear on prep:

- **Watering Hole Attack**: Infecting a site commonly visited by the target.
- **Click Fraud**: Repeatedly clicking ads to drain competitor ad budgets.
- **Typosquatting**: Registering misspelled domain names.
- **Shimming**: Exploiting code between hardware and software (e.g., USB skimmers).
- **Side-Channel Attack**: Using physical observations (timing, power, EM leaks) to extract secrets.

- **Transitive Trust**: Trust inherited through a chain of systems (used in AD exploitation).
- **Zombie**: A compromised system used in botnets.
- **Hoax**: A fake virus alert that tricks users into causing harm.
- **Nonce**: Random number used only once (often in cryptographic communication).