CYBERQUIZZER CHEAT SHEET

The Cyber Kill Chain

Exams rarely ask you to define a phase — they describe an attacker action and ask **which phase is this?** Below: the seven phases, then 21 scenarios mapped to them.

Scan to drill this sheet

01 Recon	02 Weaponize	03 Delivery	04 Exploit	05 Install	06 C2	07 Actions
Research and select the target **Defend:** monitor for scanning	Pair an exploit with a payload **Defend:** threat intel only	Transmit the weapon to the target **Defend:** mail filtering, training	Trigger the code on the victim system **Defend:** patching, EDR	Establish persistence on the host **Defend:** FIM, app allow-listing	Open a channel back for remote control **Defend:** egress & DNS analysis	Achieve the goal — exfiltrate, encrypt, destroy **Defend:** DLP, immutable backups

Scenario → phase

Cover the right-hand column and work down. These are how the question is actually asked.

ATTACKER IS…	PHASE	ATTACKER IS…	PHASE
Scraping LinkedIn for names and job titles	**Reconnaissance**	Adding a Run key to survive reboot	**Installation**
Nmap scanning a public IP range	**Reconnaissance**	Creating a hidden local admin account	**Installation**
Harvesting emails from the company site	**Reconnaissance**	Installing a backdoor RAT on the host	**Installation**
Embedding a macro into a decoy invoice	**Weaponization**	Malware beaconing out every 60 seconds	**Command & Control**
Building a malicious PDF for a known CVE	**Weaponization**	Tunnelling commands over DNS TXT	**Command & Control**
Packing a trojan to evade signatures	**Weaponization**	Registering a domain the implant calls	**Command & Control**
Emailing the attachment to 40 staff	**Delivery**	Copying the customer DB off-network	**Actions on Objectives**
Dropping infected USBs in the car park	**Delivery**	Encrypting shares, leaving a ransom note	**Actions on Objectives**
Compromising a site the target visits	**Delivery**	Deleting backups and wiping event logs	**Actions on Objectives**
The victim opens it; the macro runs	**Exploitation**	Moving laterally to the domain controller	**Actions on Objectives**
Buffer overflow in an unpatched service	**Exploitation**	Escalating from user to SYSTEM	**Exploitation**

Where people lose the mark

Three distinctions that decide most kill-chain questions.

Delivery vs Exploitation

Delivery is **sending** it. Exploitation is the code **running**. The phishing email arriving is Delivery; the click that fires the macro is Exploitation.

Exploitation vs Installation

Exploitation gets code running **once**. Installation makes it **survive a reboot** — persistence is the tell.

Recon vs Weaponization

Both happen before contact. Recon **gathers information**; Weaponization **builds the tool**. Neither touches your network — so neither is detectable there.

Reading the chain won't stick — turn it into instinct.

Drill scenario-to-phase questions until the answer is automatic. Ten minutes a day, free forever, no card.

cyberquizzer.com/go/killchain-sheet

Framework: Lockheed Martin Cyber Kill Chain® · Updated August 2026

© CyberQuizzer