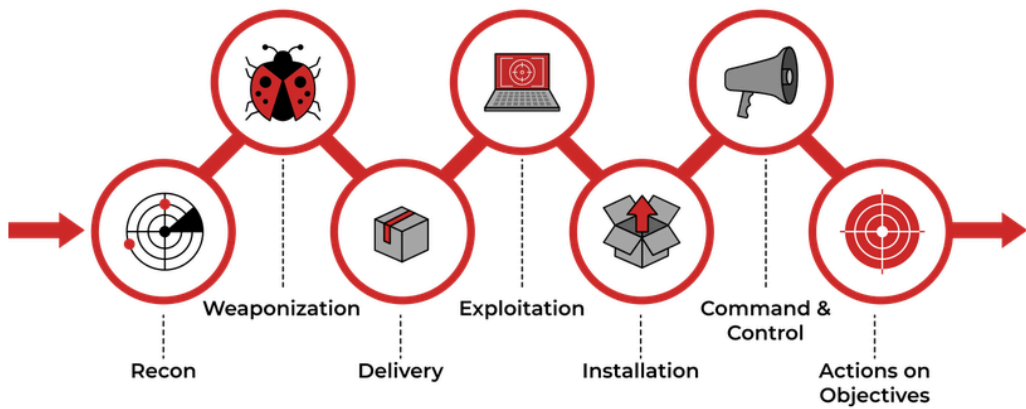


Ethical Hacking and Cyber Kill Chain Methodologies

Phase	Description	Technique Used	Example	Real-life Example
Reconnaissance	Gathering info about the target system to identify potential vulnerabilities	Google Dorking,WHOIS lookups,DNS enumeration,social engineering tactics	Searching Google for exposed admin pages or checking WHOIS data to find owner details	Watching a house from the street to learn when owners are out, checking social media to see vacation posts
Scanning	Using tools to identify vulnerabilities in the target systems through various scans	Network mapping,port Scanning, Vulnerability scanning	Running nmap to find open ports and services on a target IP	Walking up to doors and windows to see which ones are unlocked or have weak locks
Gaining Access	Attempting to exploit identified vulnerabilities to gain unauthorized access to the system	SQL injection,Buffer overflow attacks,phishing attacks	Using sql injection on a login page to bypass authentication	Picking an unlocked door or convincing a neighbor you're a delivery person to get inside
Maintaining Access	Establish a persistent connection to the compromised system to assess the duration of undetected access.	Installing rootkits,creating hidden user accounts,tunneling	Installing a backdoor to reconnect later without detection	Hiding a spare key under a plant or leaving a window slightly ajar so you can return later.
Clearing Tracks Clearing Tracks	Removing traces of the hacker's activities from system logs to avoid detection	Modifying log files,deleting evidence, clearing bash history	Deleting access logs to hide login attempts.	Wiping fingerprints, moving items back to their original places

				or deleting CCTV footage
--	--	--	--	-----------------------------

CYBER KILL CHAIN METHODOLOGY



Phase	Description	Technique Used
Reconnaissance	Attackers gather info about the target to identify vulnerabilities. This includes studying public data, websites and social media.	Scanning for open ports, Collecting data on employees, Identifying security measures
Weaponization	The attacker creates a malicious payload paired with an exploit that targets identified vulnerabilities	Developing malware, Combining payloads with exploits
Delivery	The malicious payload is	Sending phishing emails,

	transmitted to the target through various methods such as phishing emails, malicious links, or USB drives	Utilizing compromised websites for downloads
Exploitation	Successful delivery, the attacker exploits a vulnerability in the target's system to execute the payload and gain access.	Triggering malware, Exploiting software vulnerabilities
Installation	The attacker installs malware on the victim's system to establish a foothold, allowing for persistent access in the future	Installing backdoors, Setting up remote access tools
Command and Control	The attacker establishes a command and control channel to remotely manipulate the compromised system without detection	Creating communication channels, sending commands to the installed malware
Actions on objectives	Finally the attacker carries out their primary goal, which may include data theft, system disruption, or other malicious activities	Data exfiltration encrypting files for ransom, disrupting services