CompTIA Security+ SY0-701 Common Attacks Cheat Sheet

secplusmastery.com

Malware, social engineering, and common attacks, each defined in one line. A free study resource.

Know the attack by its description. Malware is malicious software, social engineering manipulates people, and the rest target passwords, networks, and applications.

Malware types

Malicious software, grouped by how it spreads and what it does.

Virus Malicious code that attaches to a file or program and needs user action to run and spread.

Worm Self-replicates and spreads across networks on its own, with no host file or user action.

Trojan Disguised as legitimate software but carries hidden malicious functionality, often a backdoor.

Ransomware Encrypts the victim's files and demands payment for the decryption key.

Spyware Secretly gathers information about a user and their activity.

Keylogger Records keystrokes to capture passwords, messages, and other typed data.

Rootkit Hides its presence and maintains privileged, often kernel-level, access to the system.

Logic bomb Dormant code that triggers when a condition, such as a specific date, is met.

Bot / botnet A compromised device under remote control; many together form a botnet used for DDoS or spam.

RAT Remote Access Trojan. Gives an attacker full remote control of the infected host.

Fileless malware Runs in memory using legitimate tools such as PowerShell, leaving little or nothing on disk.

Social engineering

Attacks that manipulate people rather than technology to gain access or information.

Phishing Fraudulent email that tricks users into revealing data or clicking a malicious link.

Spear phishing Phishing tailored to a specific individual using personal or work details.

Whaling Spear phishing aimed at senior executives, the high-value targets.

Vishing Voice phishing carried out over a phone call.

Smishing Phishing carried out over SMS text messages.

Pretexting Inventing a believable scenario or persona to extract information.

Pharming Redirecting users from a legitimate site to a fake one, often by poisoning DNS.

Baiting Luring a victim with something enticing, such as a malware-laden USB drive left in a parking lot.

Tailgating Following an authorized person through a secure door without authenticating.

Shoulder surfing Observing someone enter credentials or sensitive data nearby.

Dumpster diving Recovering sensitive information from discarded trash or documents.

Watering hole Compromising a website the target group is known to visit so victims infect themselves.

Business email compromise Impersonating an executive or vendor to authorize fraudulent payments or wire transfers.

Other common attacks

Password, network, and application attacks you should recognize on the exam.

Brute force Systematically trying every possible password combination until one works.

Password spraying Trying a few common passwords across many accounts to avoid lockouts.

Credential stuffing Reusing username and password pairs leaked from one breach against other sites.

DDoS A distributed denial-of-service floods a target from many hosts until it is unavailable.

On-path (MITM) Secretly intercepting and relaying traffic between two parties who think they are direct.

Replay Capturing valid data such as a session token and resending it to impersonate the user.

DNS poisoning Corrupting DNS records or cache to redirect users to malicious sites.

SQL injection Inserting crafted SQL into an input so the database runs it, exposing or altering data.

Cross-site scripting (XSS) Injecting scripts into a trusted site so they run in other visitors' browsers.

Privilege escalation Exploiting a flaw to gain higher permissions than were originally granted.