SECURITY+ STUDY SHEET · DOMAIN 2.0

Threats, Vulnerabilities, and Attacks

CompTIA Security+ certification exam, SY0-801 (V8)

24% of the exam · 6 exam objectives · SY0-801

Domain 2 is the largest share of the exam (24%). It asks you to describe who attacks and why, how attacks get in, what makes a system vulnerable, how to read the signs of an attack in logs and behaviour, and which threats come with the use of AI. Most questions give a short situation and ask you to name the threat, vector, vulnerability or attack it shows.

You should be able to: Logs show one password tried once against hundreds of accounts. Is this brute force or password spraying, and what single control would most reduce the chance it succeeds?

Every exam objective: the key point and the trap

2.1 Explain characteristics of threats and vulnerabilities.

Risk from a threat combines likelihood (how probable it is) with impact (how much harm it causes).

Trap: Treating the CVSS base score as the whole of prioritization, or mixing up CVE (the name) with CVSS (the score).

2.2 Describe common threat actors and motivations.

Actors listed: crime syndicate or organized crime, terrorist, unskilled attacker, hacktivist, insider, accidental or unintentional, competitor and state-sponsored.

Trap: Naming the actor from the technique alone. Data theft can be a competitor, an insider or a state; the motivation and attributes decide.

2.3 Describe threat vectors and sources.

Message-based vectors are email, Short Message Service (SMS), Rich Communication Services (RCS), instant messaging and collaboration tools; image-based ones are quick response (QR) codes, embedded content and CAPTCHA.

Trap: Confusing the vector (how the attack arrives) with the attack itself, for example naming a QR code sticker as a malware type instead of an image-based vector.

2.4 Explain types of vulnerabilities and attack surfaces.

Unsupported products get no more vendor fixes; unpatched systems have fixes available that are not applied; obsolete and unmanaged systems lack upkeep and oversight.

Trap: Treating unsupported and unpatched as the same thing. Unpatched means a fix exists; unsupported means none will come.

2.5 Given a scenario, analyze indicators of malicious activity.

Malware listed: ransomware, Trojan, worm, spyware, adware, virus, rootkit, keylogger, logic bomb and fileless malware.

Trap: Mixing up password spraying and brute force, or the social engineering channels: smishing is text, vishing is voice, quishing is a QR code.

2.6 Summarize threats and vulnerabilities associated with artificial intelligence (AI) usage.

Prompt injection plants instructions in input the model processes; jailbreaking persuades a model to bypass its own safety rules.

Trap: Treating prompt injection, jailbreaking and poisoning as the same thing. They differ in who supplies the input and at which stage.

Key terms

APT: Advanced Persistent Threat

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System

DDoS: Distributed Denial of Service

LLM: Large Language Model

MFA: Multifactor Authentication

NFC: Near-field Communication

RCS: Rich Communication Services

TOC: Time-of-check

TOU: Time-of-use

ExamDragon, examdragon.com/secplus. Independent exam preparation, not affiliated with or endorsed by CompTIA; written in our own words to the SY0-801 exam objectives. CompTIA and Security+ are trademarks of CompTIA, Inc.