CYSA+ STUDY SHEET · DOMAIN 2.0

Vulnerability Management

CompTIA Cybersecurity Analyst (CySA+) certification exam, CS0-004

26% of the exam · 4 exam objectives · CS0-004

Vulnerability Management is how an organization finds, analyzes and fixes weaknesses: planning and running the right kind of scan for each asset, reading the output of network, web, vulnerability, cloud and attack simulation tools, prioritizing findings by severity, likelihood and context before mitigating and validating them, and the control types, risk concepts, application security and third-party risk practices that frame the whole program.

You should be able to: A credentialed scan reports a Critical vulnerability on an isolated lab host and a High one on an internet-facing server listed as actively exploited, and the vendor has no patch for the High one yet. Which finding comes first, and what can the team do until a patch exists?

Every exam objective: the key point and the trap

2.1 Given a scenario, implement the appropriate vulnerability scanning method.

Scanning starts with an asset inventory: you cannot scan or prioritize what you do not know exists. The inventory records each asset's owner, location and value, and discovery scans keep it current.

Trap: Assuming one scan type fits everything. A credentialed active scan is accurate for servers but can crash fragile controllers, and a scanner blocked by a firewall reports filtered ports rather than the real state of the hosts behind it.

2.2 Given a scenario, analyze output from vulnerability assessment tools.

Network scanning and mapping: Angry IP Scanner is a lightweight graphical tool for finding live hosts and open ports; Masscan sweeps very large ranges for open ports at high speed by sending packets asynchronously.

Trap: Confusing tools that look alike. Prowler and ScoutSuite assess a deployed cloud account, while Checkov reads code before deployment; Nikto scans a web server, while Burp Suite and ZAP intercept and replay requests.

2.3 Given a scenario, analyze data to prioritize and mitigate vulnerabilities.

Prioritization criteria: exploitability (how easily it can be used), active exploitation reported by threat intelligence, asset value, impact if exploited, and whether a patch or other remediation is available.

Trap: Sorting only by CVSS severity. A lower-rated finding that is exposed and actively exploited usually outranks a higher-rated one on an isolated system.

2.4 Explain concepts related to control types, risks, and vulnerability management.

Control types describe what a control is: administrative (policies, procedures, training, personnel checks), technical (enforced by hardware or software, such as firewalls and encryption) and physical (fences, locks, guards).

Trap: Mixing up type and function. A firewall is a technical control that can be preventative; a guard is a physical control that can deter and detect. Answer the question asked: type or function.

Key terms

CVSS: Common Vulnerability Scoring System

PCI DSS: Payment Card Industry Data Security Standard

CIS: Center for Internet Security

OpenVAS: Open Vulnerability Assessment Scanner

ZAP: Zed Attack Proxy

BAS: Breach Attack Simulation

SAST: Static Application Security Testing

DAST: Dynamic Application Security Testing

SCA: Software Composition Analysis

SBOM: Software Bill of Materials

ExamDragon, examdragon.com/cysaplus. Independent exam preparation, written in our own words to the CS0-004 exam objectives. CompTIA and CySA+ are trademarks of CompTIA, Inc.