Back to PenTest+

PenTest+ Study Notes

Comprehensive study guide for CompTIA PenTest+ PT0-003

Domain 1: Security Operations (33%)

Key Topics:

- SIEM (Security Information and Event Management) configuration and correlation rules
- Security orchestration, automation, and response (SOAR) platforms
- Endpoint detection and response (EDR) and extended detection and response (XDR)
- Threat intelligence platforms (TIP) and STIX/TAXII standards
- Network traffic analysis — NetFlow, PCAP, packet capture tools
- Threat hunting methodologies and hypothesis-driven investigation
- Identity and access management (IAM) monitoring — privileged access, MFA
- Cloud security monitoring — CWPP, CSPM, and cloud audit logs
- Attack frameworks: MITRE ATT&CK, Cyber Kill Chain, Diamond Model

SIEM & Log Analysis:

Log Sources: Effective SIEM use requires ingesting Windows Event Logs (Security, System, Application), syslog from network devices, web server access logs, firewall logs, and DNS query logs. Normalizing these into a common schema enables correlation.

Correlation Rules: SIEM correlation rules detect patterns — e.g., multiple failed logins followed by a successful login from the same source IP within 5 minutes = potential brute force success. Tuning rules reduces false positives.

Threat Hunting: Proactive threat hunting uses hypotheses based on threat intelligence (e.g.,

C2, Exfiltration, and Impact. PenTest+ analysts map detections to ATT&CK IDs (e.g., T1059 = Command and Scripting Interpreter).

Domain 2: Vulnerability Management (30%)

Key Topics:

- Vulnerability scanning tools — Nessus, Qualys, OpenVAS, Rapid7 InsightVM
- CVSS v3.1 — Base, Temporal, and Environmental metrics scoring
- CVE, NVD, and vulnerability databases
- EPSS (Exploit Prediction Scoring System) for exploitation probability
- Patch management lifecycle and prioritization frameworks
- Asset discovery and inventory management
- Configuration management and security baselines (CIS Benchmarks, DISA STIGs)
- Container security scanning — image vulnerabilities, registry scanning
- Web application vulnerability scanning (OWASP Top 10, DAST/SAST)

CVSS Scoring:

Base Score Metrics: Attack Vector (Network, Adjacent, Local, Physical), Attack Complexity (Low/High), Privileges Required, User Interaction, Scope (Changed/Unchanged), Confidentiality/Integrity/Availability Impact. Base scores range 0.0–10.0.

Temporal Metrics: Exploit Code Maturity, Remediation Level, Report Confidence. These adjust the base score based on current exploitation activity — a Critical with Proof-of-Concept exploit is higher priority than one with Unproven exploit code.

Prioritization: PenTest+ analysts combine CVSS scores with asset criticality, exposure (internet-facing vs. internal), and threat intelligence (CISA KEV catalog) to prioritize remediation. A CVSS 7.5 on an internet-facing critical asset outranks CVSS 9.8 on an isolated dev server.

Domain 3: Incident Response & Management (20%)

- Digital forensics fundamentals — chain of custody, evidence preservation

- Memory forensics, disk forensics, and network forensics
- Malware analysis — static analysis, dynamic analysis, sandboxing
- Root cause analysis (RCA) and lessons-learned process
- Containment strategies: network isolation, account disablement, firewall rules
- Tabletop exercises and IR plan testing

IR Lifecycle Deep Dive:

Detection & Analysis: Alert triage begins with validating the alert (true positive vs. false positive), then scoping the incident — how many systems are affected, what data may be at risk, lateral movement indicators? SIEM, EDR, and threat intelligence are used together.

Containment: Short-term containment (isolating affected hosts, blocking C2 IPs) preserves evidence while limiting damage. Long-term containment may involve patching, credential rotation, and reimaging while business operations continue on clean systems.

Post-Incident Activity: The lessons-learned meeting (held within 2 weeks of resolution) identifies process gaps, detection failures, and control improvements. Outputs: updated playbooks, new detection rules, revised asset inventories, and management reports.

Domain 4: Reporting & Communication (17%)

Key Topics:

- Security metrics and KPIs — MTTD, MTTR, false positive rate, SLA compliance
- Security dashboards and executive reporting
- Vulnerability management reporting — aging reports, SLA breach tracking
- Communicating risk to non-technical stakeholders
- Compliance reporting — audit evidence, control testing results
- Incident report writing — technical details, executive summaries, IoCs
- Threat intelligence sharing — ISACs, STIX/TAXII, vendor sharing programs
- Continuous improvement cycles — Plan-Do-Check-Act (PDCA)

Key Security Metrics:

Executive Reporting: Board and executive reports emphasize business risk, compliance posture, and trend data — not technical details. Frame security metrics in business terms: "Data breach risk reduced 40% through patch compliance improvements" rather than "CVE coverage improved."