PROGRAMMA CompTIA CySA+ (CS0-003)

40 ore

Parts I: Security Operations

1.1 Explain the importance of system and network architecture concepts in security operations

- Log ingestion
  - Time synchronization
  - Logging levels
- Operating system (OS) concepts
  - Windows Registry
  - System hardening
  - File structure o Configuration file locations
  - System processes
  - Hardware architecture
- Infrastructure concepts
  - Serverless
  - Virtualization
  - Containerization
- Network architecture
  - On-premises
  - Cloud
  - Hybrid
  - Network segmentation
  - Zero trust
  - Secure access secure edge (SASE)
  - Software-defined networking (SDN)
- Identity and access management
  - Multifactor authentication (MFA)
  - Single sign-on (SSO)
  - Federation
  - Privileged access management (PAM)
  - Passwordless
  - Cloud access security broker (CASB)

- Encryption
  - Public key infrastructure (PKI)
  - Secure sockets layer (SSL) inspection
- Sensitive data protection
  - Data loss prevention (DLP)
  - Personally identifiable information (PII)
  - Cardholder data (CHD)

1.2 Given a scenario, analyze indicators of potentially malicious activity

- Network-related
  - Bandwidth consumption
  - Beaconing
  - Irregular peer-to-peer communication
  - Rogue devices on the network
  - Scans/sweeps
  - Unusual traffic spikes
  - Activity on unexpected ports
- Host-related - Processor consumption
  - Memory consumption
  - Drive capacity consumption
  - Unauthorized software
  - Malicious processes
  - Unauthorized changes
  - Unauthorized privileges
  - Data exfiltration
  - Abnormal OS process behavior
  - File system changes or anomalies
  - Registry changes or anomalies
  - Unauthorized scheduled tasks
- Application-related
  - Anomalous activity
  - Introduction of new accounts
  - Unexpected output
  - Unexpected outbound communication
  - Service interruption
  - Application logs
- Other
  - Social engineering attacks
  - Obfuscated links

1.3 Given a scenario, analyze indicators of potentially malicious activity

- Tools
  - Packet capture o Wireshark o tcpdump
  - Log analysis/correlation
    - Security information and event management (SIEM)
    - Security orchestration, automation, and response (SOAR)
  - Endpoint security o Endpoint detection and response (EDR)
  - Domain name service (DNS) and Internet Protocol (IP) reputation
    - WHOIS
    - AbuseIPDB
  - File analysis
    - Strings
    - VirusTotal
  - Sandboxing
    - Joe Sandbox
    - Cuckoo Sandbox
- Common techniques
  - Pattern recognition
    - Command and control
  - Interpreting suspicious commands
  - Email analysis
    - Header
    - Impersonation
    - DomainKeys Identified Mail (DKIM)
    - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
    - Sender Policy Framework (SPF)
    - Embedded links
  - File analysis
    - Hashing
  - User behavior analysis
    - Abnormal account activity
    - Impossible travel
- Programming languages/scripting
  - JavaScript Object Notation (JSON)
  - Extensible Markup Language (XML)
  - Python
  - PowerShell

- Shell script
- Regular expressions

1.4 Compare and contrast threat-intelligence and threat-hunting concepts

- Threat actors
  - Advanced persistent threat (APT)
  - Hacktivists
  - Organized crime
  - Nation-state
  - Script kiddie
  - Insider threat
    - Intentional
    - Unintentional
    - Supply chain
- Tactics, techniques, and procedures (TTP)
- Confidence levels
  - Timeliness
  - Relevancy
  - Accuracy
- Collection methods and sources
  - Open source
    - Social media
    - Blogs/forums
    - Government bulletins
    - Computer emergency response team (CERT)
    - Cybersecurity incident response team (CSIRT)
    - Deep/dark web
  - Closed source
    - Paid feeds
    - Information sharing organizations
    - Internal sources
- Threat intelligence sharing
  - Incident response
  - Vulnerability management
  - Risk management
  - Security engineering
  - Detection and monitoring
- Threat hunting
  - Indicators of compromise (IoC)

        - Collection
        - Analysis
        - Application
    - Focus areas
        - Configurations/ misconfigurations
        - Isolated networks
        - Business-critical assets and processes
    - Active defense
    - Honeypot

1.5 Explain the importance of efficiency and process improvement in security operations

- Standardize processes
    - Identification of tasks suitable for automation
        - Repeatable/do not require human interaction
    - Team coordination to manage and facilitate automation
- Streamline operations
    - Automation and orchestration
        - Security orchestration, automation, and response (SOAR) –
    - Orchestrating threat intelligence data
        - Data enrichment
        - Threat feed combination
    - Minimize human engagement
- Technology and tool integration
    - Application programming interface (API)
    - Webhooks
    - Plugins
- Single pane of glass

Parts II: Vulnerability Management

2.1 Given a scenario, implement vulnerability scanning methods and concepts

- Asset discovery
  - Map scans
  - Device fingerprinting
- Special considerations
  - Scheduling
  - Operations
  - Performance
  - Sensitivity levels
  - Segmentation
  - Regulatory requirements
- Internal vs. external scanning
- Agent vs. agentless
- Credentialed vs. non-credentialed
- Passive vs. active
- Static vs. dynamic
  - Reverse engineering
  - Fuzzing
- Critical infrastructure
  - Operational technology (OT)
  - Industrial control systems (ICS)
  - Supervisory control and data acquisition (SCADA)
- Security baseline scanning
- Industry frameworks
  - Payment Card Industry Data Security Standard (PCI DSS)

- Center for Internet Security (CIS) benchmarks
- Open Web Application Security Project (OWASP)
- International Organization for Standardization (ISO) 27000 series

2.2 Given a scenario, analyze output from vulnerability assessment tools

- Tools
  - Network scanning and mapping
    - Angry IP Scanner
    - Maltego
  - Web application scanners
    - Burp Suite
    - Zed Attack Proxy (ZAP)
    - Arachni
    - Nikto
  - Vulnerability scanners
    - Nessus
    - OpenVAS
  - Debuggers
    - Immunity debugger
    - GNU debugger (GDB)
  - Multipurpose
    - Nmap
    - Metasploit framework (MSF)
    - Recon-ng
  - Cloud infrastructure assessment tools
    - Scout Suite

- Prowler
- Pacu

2.3 Given a scenario, analyze data to prioritize vulnerabilities

- Common Vulnerability Scoring System (CVSS) interpretation
  - Attack vectors
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
  - Impact
    - Confidentiality
    - Integrity
    - Availability
- Validation - True/false positives - True/false negatives
- Context awareness - Internal - External - Isolated
- Exploitability/weaponization
- Asset value
- Zero-day

2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities

- Cross-site scripting
  - Reflected
  - Persistent
- Overflow vulnerabilities
  - Buffer
  - Integer -

    - Heap
    - Stack
- Data poisoning
- Broken access control
- Cryptographic failures
- Injection flaws
- Cross-site request forgery
- Directory traversal
- Insecure design
- Security misconfiguration
- End-of-life or outdated components
- Identification and authentication failures
- Server-side request forgery
- Remote code execution
- Privilege escalation
- Local file inclusion (LFI)/remote file inclusion (RFI)

2.5 Explain concepts related to vulnerability response, handling, and management

- Compensating control
- Control types
    - Managerial
    - Operational
    - Technical
    - Preventative
    - Detective
    - Responsive
    - Corrective
- Patching and configuration management
    - Testing
    - Implementation
    - Rollback
    - Validation
    - Maintenance windows
- Exceptions
- Risk management principles
    - Accept
    - Transfer
    - Avoid
    - Mitigate
- Policies, governance, and service-level objectives (SLOs)
- Prioritization and escalation
- Attack surface management
    - Edge discovery

- Passive discovery
- Security controls testing
- Penetration testing and adversary emulation
- Bug bounty
- Attack surface reduction

- Secure coding best practices
  - Input validation
  - Output encoding
  - Session management
  - Authentication
  - Data protection
  - Parameterized queries
- Secure software development life cycle (SDLC)
- Threat modeling

Parts III: Incident Response and Management

3.1 Explain concepts related to attack methodology frameworks

- Cyber kill chains
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK
- Open Source Security Testing Methodology Manual (OSS TMM)
- OWASP Testing Guide

3.2 Given a scenario, perform incident response activities

- Detection and analysis
    - IoC
    - Evidence acquisitions
        - Chain of custody
        - Validating data integrity
        - Preservation
        - Legal hold
- Data and log analysis
- Containment, eradication, and recovery
    - Scope
    - Impact
    - Isolation
    - Remediation
    - Re-imaging
    - Compensating controls
    -

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle

- Preparation
    - Incident response plan

- Tools
- Playbooks
- Tabletop
- Training
- Business continuity (BC)/ disaster recovery (DR)

- Post-incident activity
  - Forensic analysis
  - Root cause analysis
  - Lessons learned

Parts IV: Reporting and Communication

4.1 Explain the importance of vulnerability management reporting and communication

- Vulnerability management reporting
  - Vulnerabilities
  - Affected hosts
  - Risk score
  - Mitigation
  - Recurrence
  - Prioritization
- Compliance reports
- • Action plans
  - Configuration management
  - Patching
  - Compensating controls
  - Awareness, education, and training
  - Changing business requirements
- Inhibitors to remediation
  - Memorandum of understanding (MOU)
  - Service-level agreement (SLA)
  - Organizational governance
  - Business process interruption
  - Degrading functionality
  - Legacy systems
  - Proprietary systems
- Metrics and key performance indicators (KPIs)

- Trends
- Top 10
- Critical vulnerabilities and zero-days - SLOs

- Stakeholder identification and communication

4.2 Explain the importance of incident response reporting and communication

- Stakeholder identification and communication
- Incident declaration and escalation
- Incident response reporting
  - Executive summary
  - Who, what, when, where, and why
  - Recommendations
  - Timeline
  - Impact
  - Scope
  - Evidence
- Communications
  - Legal
  - Public relations
    - Customer communication
    - Media
  - Regulatory reporting
  - Law enforcement
- Root cause analysis
- Lessons learned
- Metrics and KPIs
  - Mean time to detect
  - Mean time to respond
  - Mean time to remediate
  - Alert volume