Vulnerability Management Activities

Chapter 3

Episode 3.01

Vulnerability Identification

Objective 1.3 Given a scenario, perform vulnerability management activities.

- Vulnerability identification
  - Asset criticality
  - Active vs. passive scanning
  - Mapping/enumeration

Regulatory Environments

- ISO/IEC 27001
  - Standard for managing information systems
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Corporate policy
- Data classification

Vulnerability Identification

- Asset inventory
  - All endpoints?
  - Servers only?
  - Inventory all assets to determine vulnerability identification considerations
- Asset criticality
  - Necessary to determine mediation priorities

Vulnerability Identification

- Active vs. passive scanning

Passive	Active
Listen to network traffic	Send specially-crafted packets to determine what's going on
Quieter, doesn't affect network traffic	Noisier, affects network traffic
Safer	Can be detrimental and cause systems to slow down or crash

Mapping/ Enumeration

- Common techniques
  - ICMP echo request
  - TCP SYN to port 443
  - TCP ACK to port 80
  - ICMP timestamp request
- Nmap is a great tool to use here

Vulnerability Identification

- Vulnerability scanning
  - Web application

Episode 3.02

Scanning Parameters and Criteria

Objective 1.3 Given a scenario, perform vulnerability management activities.

• Scanning parameters and criteria

- Risks associated with scanning activities
- Vulnerability feed
- Scope
- Credentialed vs. non-credentialed
- Server-based vs. agent-based
- Internal vs. external
- Special considerations
  - Technical constraints
  - Workflow
- Sensitivity levels
- Regulatory requirements
- Segmentation

Scanning Parameters and Criteria

- Risks associated with scanning activities
  - May impact availability
- Regulatory requirements
  - Work within regulatory environments
- Technical constraints
- Workflow
  - Work with your available resources (personnel and technical)

Scanning Parameters and Criteria

- Sensitivity levels
  - Clearance and classified data
  - Sensitive data (PHI, PII, payment cards, etc.)
  - Are you authorized to view data?
- Segmentation
  - VLANs in logical architecture
  - Understand network architecture for appropriate scans
- Vulnerability feed
  - Up-to-date known vulnerability information
- Scope
  - How many devices/ endpoints?

Scanning Parameters and Criteria

- Credentialed vs. non-credentialed scan

Credentialed	Non-Credentialed
Insider (authorized)	Outsider (not authorized)
Shows vulnerabilities of an attacker after elevating privileges	Shows what an attacker can see before elevating privileges

Scanning Parameters and Criteria

- Server-based vs. agent-based scan

Server-Based	Agent-Based
Easier to set up (central server sends out traffic to scan targets)	Install software and run scans on each endpoint
Increases traffic on network	Much less traffic on network
Not as much access to internal information	

Scanning Parameters and Criteria

- Internal vs. external scan
  - Does scan execute from within corporate network?
  - Or execute from outside the network via external node?
  - Results vary
  - Report results based on internal/external scan

Episode 3.03

Scanning Special Considerations

Objective 1.3 Given a scenario, perform vulnerability management activities.

• Scanning parameters and criteria

- Special considerations
  - Types of data
- Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings

Special Scanning Considerations

- Types of data
  - Scan for everything or just certain types of data?
  - Understand the organization and regulations driving the scans
- Tools
  - Updates and plug-ins help automate scans
  - Nessus
    - Nessus Attack Scripting Language (NASL)
      - Automate aspects of scanning process
      - Consistency in scans
      - Recreate scans

Special Scanning Considerations

- Security Control Automation Protocol (SCAP)
  - Created by NIST
  - Defines modules that dictate compliance requirements/settings
- Intrusion detection system (IDS)/intrusion prevention system (IPS)
  - Firewall may reject scans
- Generating reports
  - Templates/format
  - Automated vs. manual distribution
    - Possible executive presentation to client

Episode 3.04

Validation

Objective 1.3 Given a scenario, perform vulnerability management activities.

- Validation
  - True positive
  - False positive
  - True negative
  - False negative

Validation

- Determining whether data is true or not
- Four response types:
  - True, false, negative, positive
- Four categories:
  - True positive
  - False positive
  - True negative
  - False negative

Episode 3.05

Remediation and Mitigation

Objective 1.3 Given a scenario, perform vulnerability management activities.
• Remediation/mitigation
- Configuration baseline
- Patching
- Hardening
- Compensating controls
- Risk acceptance
- Verification of mitigation

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.
• Documented compensating controls

Remediation/Mitigation

- Configuration baseline
  - Collection of all property settings of a device, OS, application, etc.
  - Compare to current settings and determine changes
  - Often implemented in audit process
  - Find baselines from standards organizations
- Identify vulnerabilities
  - Due to configuration or old software
  - Recommend patching software
    - Especially security patches

Remediation/ Mitigation

- Prioritizing
  - Most crucial vulnerabilities first
    - Highest probability of occurring
    - Highest impact
- Hardening
  - Process of remediating
  - Make a device less susceptible to attack

Remediation/ Mitigation

- Compensating controls
  - Helps mitigate vulnerability without directly addressing the cause
  - Example: firewall with closed ports
  - Ideally implement layers of compensating controls
- Risk acceptance
  - Document
  - Have long-term solution to mitigate eventually
- Verification of mitigation

Episode 3.06

Inhibitors to Remediation

Objective 1.3 Given a scenario, perform vulnerability management activities.

• Inhibitors to remediation

- Memorandum of understanding (MOU)
- Service-level agreement (SLA)
- Organizational governance
- Business process interruption
- Degrading functionality
- Legacy systems
- Proprietary systems

Inhibitors to Remediation

- Memorandum of understanding (MOU)
  - Authorizes/limits scanning activities
- Service-level agreement (SLA)
  - Dictates what each party does
  - May limit remediation actions
  - May limit scanning capabilities
- Organizational governance
  - Potential limits on remediation due to collateral impact

Inhibitors to Remediation

- Business process interruption
- Degrading functionality
- Legacy systems
- Proprietary systems