# Domain 6: Security Assessment & Testing

MIS-5903

https://community.mis.temple.edu/mis5903sec711summer2022/

1

## Need for Assessment & Testing

- Controls can be applied inconsistently.
- Controls can be misconfigured.
- Controls can be tampered with.
- Controls can become less effective over time.
  - Anti-malware only protects ~38% of attacks
  - Denial of Service; now Distributed Denial of Service
- New threats in the environment.



2

# Tests, Assessments, Audits

- Security Tests – verify that a control is functioning properly
- Security Assessments – comprehensive reviews of security of a system, application, or other environment. A series of tests.
  - Review of threat environment
  - Current and future risks
  - Value of target environment
- Security Audits – must be performed by independent auditors
  - For demonstrating effectiveness of controls to a third party
  - Staff who design, implement, and monitor controls have inherent conflict of interest



3

# Security Tests

- Scheduled periodically
  - Availability of resources
  - Criticality of systems and applications
  - Sensitivity of information
  - Likelihood of technical failure of control mechanism
  - Likelihood of misconfiguration
  - Risk of attack
  - Rate of change of control configuration
  - Other changes in technical environment
  - Difficulty and time required to perform a control test
  - Impact of test on normal business operations



4

# Security Assessments

- Comprehensive review
- Risk assessment identifies vulnerabilities that may allow compromise
  - Current and future risks
  - Nontechnical language
- Recommendations for improving security
- May be internal, or outsourced (based on expertise)
- NIST SP 800-53A is an example



5

# Security Audits

- Example – US Government Accountability Office (GAO) at request of Congress
- Internal audits – reporting line is independent of the functions evaluated
- External audits – performed by outside auditing firm
- Third Party Audits – conducted by, or on behalf of, another organization
  - Regulatory / Contract
  - Initiator selects audit firm and scope



6

# Auditing Standards - AICPA

- American Institute of Certified Public Accounts (AICPA)
  - Statement on Standards for Attestation Engagements (SSAE 18)
    - Type 1 – moment in time; does not involve actual testing of the controls
    - Type 2 – minimum six-month time period; measures effectiveness of controls based on testing.
  - System and Organization Controls
    - SOC1 – SOC for Service Organizations –
    - SOC2 – SOC for Service Organizations – includes Trust Services Criteria
      - HITRUST
      - CSA Star Attestation
    - SOC3 – Trust Services Criteria for General Use Report – freely distributed



7

# Other Auditing Standards

- Control Objectives for Information and related Technologies (COBIT)
  - Common requirements that organizations should have in place
- International Organization for Standardization (ISO)
  - 27001 – Information Security Management System
  - 27002 – Information Security Controls



8

# Information System Audits

- Information System is a "a specific set of people, computers, processes, and information."
- Audits are a "systematic assessment of the security controls on a specific set of people, computers, processes, and information."
- Vulnerability assessments and penetration tests are helpful, but not sufficient to truly assess our security posture.



9

# Information System Security Audit Process

- Determine the goals
- Involve the right business unit leaders
- Determine the scope (not everything is in scope)
- Choose the audit team (internal or external)
- Plan the audit
- Conduct the audit
- Document the results
- Communicate the results



10

## Scope Considerations

- Which subnets and/or systems to test?
- Reviewing artifacts such as passwords, files, log entries?
- Reviewing user behavior/response (e.g. social engineering)?
- Which information to assess?
- What are privacy implications of the audit?
- How will we evaluate processes, and to which extent?



11

## Internal Audits

**Advantages**

- Familiar with inner workings of organization
- Less time to results
- Team always available
- Can re-test
- Cost

**Disadvantages**

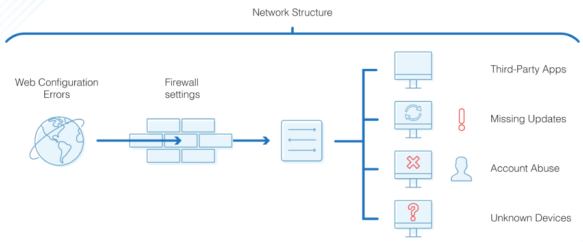
- May have limited exposure to approaches to securing or exploiting information systems
- Potential for conflicts
- Reluctance to report findings (cultural issue)
- Agendas to the audit



12

# Vulnerability Scanning & Testing

- Written agreement required before starting
- Goals:
  - Evaluate the true security posture
  - Identify as many vulnerabilities
    - Evaluation and prioritization
  - Potential elements that might be abused
- Testing ramifications identified






13

# Types of testing

- Personnel – social engineering
- Physical – checking facility and perimeter protection mechanisms
- System and network testing – Automated tools common
  - Network discovery scans
  - Network vulnerability scans
  - Web application vulnerability scans
  - Database vulnerability scans



14

# Comparison of Terms

| Non-Inclusive | Suggested Replacements |
|---|---|
| • Black-box | • Closed-Box |
| • White-box | • Open-box |
| • Blackhat (hacker) | • Hacker |
| • Whitehat (hacker) | • Ethical Hacker |
| • Blacklist | • Block list |
| • Whitelist | • Allow list |
| • Greylist | • Suspicious list |



15

# Comparison of Terms (2)

| Non-Inclusive | Suggested Replacements |
|---|---|
| • Master / Slave | • Primary/Secondary |
| • Disable | • Deactivate |
| • Enable | • Activate |
| • Dummy Value | • Placeholder value |
| • Dummy Variable | • Placeholder variable |
| • Webmaster | • Website administrator |
| • Ticket Master | • Ticket leader |



16

# Comparison of Terms (3)

| Non-Inclusive | Suggested Replacements |
|---|---|
| • Red Team | • Ethical Hacking Team |
| • White Paper | • Expert Paper |
| • War Room | • Situation Room |
| • White space | • Empty Space |
| • Native feature | • Built-In Feature |
| • Scrum master | • Scrum Coach or Team Facilitator |



17

# Prior Knowledge

- Black Box – no "a priori" knowledge of internal design
  - Due to lack of knowledge, may attack systems out of scope
  - Behavioral or Functionality Testing
- White Box – prior complete knowledge
  - Allows to target specific internal controls or features
  - Saves time during testing, reduces likelihood of attacking systems out of scope
- Gray Box – some, but not all information on internal workings is provided
  - Allows a degree of realism



18

## Vulnerability Scanning Capabilities:

- Identify active hosts
- Identify active and vulnerable services (ports) on active hosts
- Identify applications and banner grabbing
- Identify operating systems in use
- Identify vulnerabilities in these operating systems and applications
- Identify misconfigured settings
- Test for compliance with security policies
- Establish the foundation for penetration testing



19

## Describing Vulnerabilities

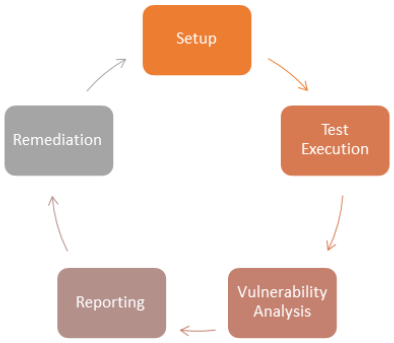
- Common Vulnerabilities and Exposures (CVE) – naming system
- Common Vulnerability Scoring System (CVSS) – scoring
- Common Configuration Enumeration (CCE) – naming for configuration issues
- Common Platform Enumeration (CPE) – naming for operating systems, applications, devices
- Extensible Configuration Checklist Description Format (XCCDF) – language for specifying security checklists
- Open Vulnerability and Assessment Language (OVAL) – language for describing security testing procedures.



20

# Vulnerability Management Workflow

- Detection
- Validation (not a false positive)
- Remediation

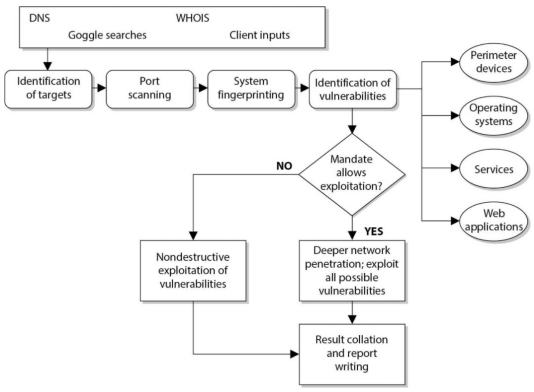





21

# Penetration Test Process

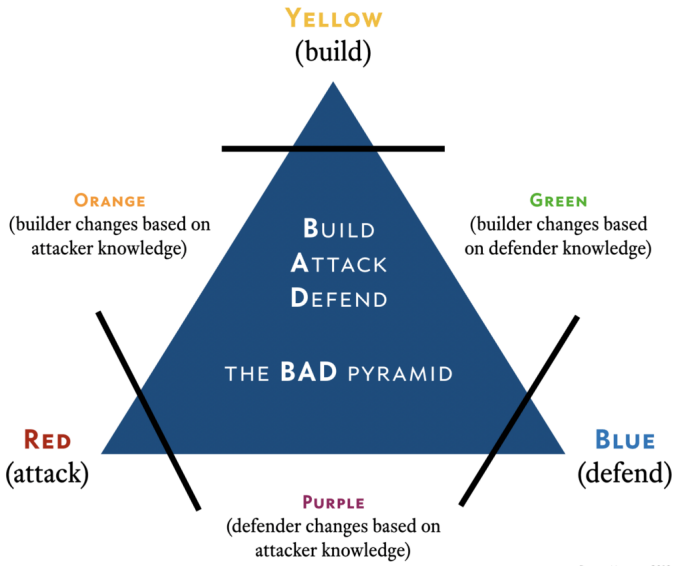
- Planning – scope of test and rules of engagement
- Information Gathering and Discovery
  - port scans, resource identification
  - Wardialing – modems, PBX
- Vulnerability scanning
- Exploitation
- Reporting to Management






22

# Teaming




- Source https://danielmiessler.co





# Network Discovery Scans

- Common Techniques
  - TCP SYN – sends single packet to each port with SYN, request to open connection. SYN & ACK response indicates port is open. (half-open scanning)
  - TCP Connect
  - TCP ACK – Sends packet with ACK; used to determine rules enforced by firewall(s)
  - XMAS Scanning – sends packet with FIN, PSH, and URG. “lit up”

# NMAP Responses

- Open – port is open and accepting connections
- Closed – allowed through firewall, accessible on remote system, but no applications on port
- Filtered – unable to determine due to firewall interfering with connection



25

# Network Vulnerability Scanning

- Uses a database of known vulnerabilities
  - Unauthenticated vs. authenticated
- Performs tests against known vulnerabilities
- False Positive – “matches”, but not a valid result
- False Negative – no “match” to to missed detection *most dangerous*
- Examples:
  - Tenable / Nessus / SecurityCenter
  - Rapid7 NeXpose
  - Qualys QualysGuard
  - OpenVAS



26

## Security Awareness

- Phishing (via digital communication), spear-phishing, whaling
- Pretexting (in person or over the phone)
- Online Safety – awareness of privacy settings.
  - Once posted, cannot be easily retracted
- Drive-By Download – visit a malicious website
- Culture



27

## Common Vulnerability Types

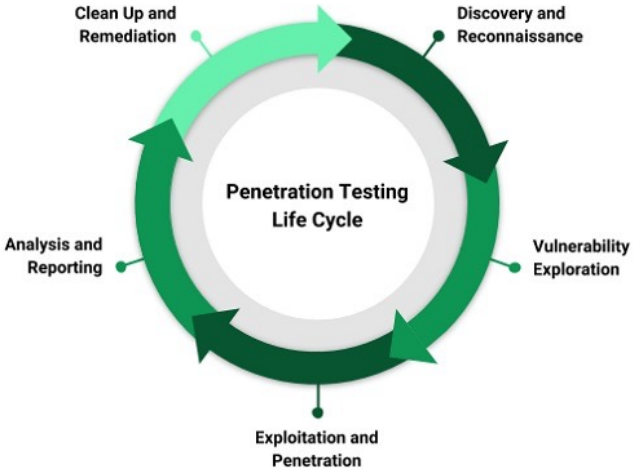
- Kernel Flaw – operating system innermost component not patched
- Buffer overflows – developer training, code scanners, enhanced programming libraries, “typed” languages that disallow buffer overflows.
- Symbolic Links – ensure that the full path to files cannot be circumvented.
- File descriptor attacks – (see buffer overflows)
- Race Conditions – ensure temporary files cannot be read or written
- File and Directory Permissions – supplement with file integrity checkers



28

# Penetration Test Life Cycle

- Zero knowledge (black) – no knowledge, must start from ground zero
- Partial knowledge(gray) – some, but not all information
- Full knowledge(white) – intimate knowledge of target





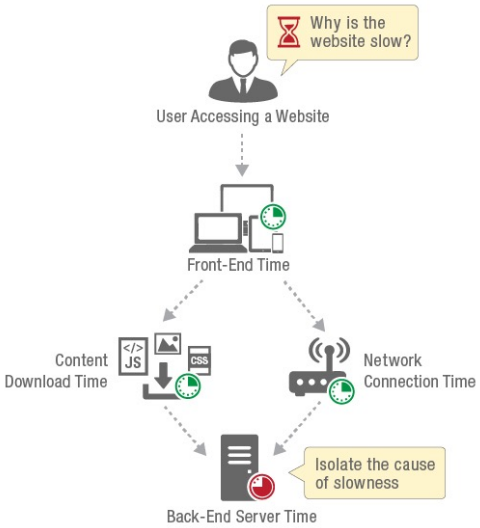



# Penetration Testing Methodologies

- OWASP https://www.owasp.org/index.php/Penetration_testing_methodologies
- Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/research/
- NIST 800-115 https://csrc.nist.gov/publications/detail/sp/800-115/final
- FedRAMP Penetration Test Guidance https://www.fedramp.gov/penetration-testing-for-all-fedramp-moderate-and-high-systems/
- PCI-DSS Information Supplement

# Monitoring

- Real Use Monitoring
  - From user's perspective
  - Lacks predictability or regularity
- Synthetic Transactions
  - Scripted, consistent
- Breach Attack Simulations






31

# Preventing Log Tampering

- Remote Logging
- Simplex Communication (data diode)
- Replication
- Write-Once Media
- Cryptographic Hash Chaining



32

# Auditing Administrative Controls

- Account Management
  - Privileged accounts
  - Authentication (password, two-factor)
  - Limited use of privileged accounts (RunAS, SuDo)
- Adding Accounts
  - Acceptable Use Policy (AUP)
- Modifying Accounts
  - Privilege Accumulation
- Suspending Accounts





# Types of Data – Special Concerns

- User Data Files – multiple backup copies
  - Compliant with policies, regulations, laws
- Databases
  - Test the database is operational, not just the file recovered
- Mailbox
  - Facilitate e-discovery

# Technical Reporting

- Threats
- Vulnerabilities (exploitable)
- Probability / Likelihood
- Impact of Exploitation
- Recommended actions



35

# Executive Summaries

- Return on Investment (ROI)
- Cost Approach – cost of acquiring or replacing an asset
- Income approach – expected contribution of the asset to revenue stream
- Market approach – determine how much other firms pay for a similar asset



36

# Technical Audit Report

- Compelling for *intended* audience
- Conclusions drawn directly from empirical facts
- Includes:
  - Executive Summary – summary of key take-aways
  - Background – why audit was performed
  - Methodology – identify processes, tools, people, locations, scope
  - Findings
    - Technical – Type of system
    - Executive – Based on Business Impact
  - Recommendations
  - Appendices – include raw data



37

# Management Review

- Plan
- Do
- Check
- Act

- PDCA – Deming
  - Shewhart Cycle
  - Later, PDS
- Kaizen – continual improvement




38

# Security Metrics

- Relevant – align with goals
- Quantifiable – objectively measured in a consistent (easy) manner
- Actionable – informs actions, leads to better outcomes
- Robust – trackable over time, allow trend detection
- Simple – Will the audience know what was measured and why it matters
- Comparative – evaluated against something else
  - Ratios, percentages, changes over time



39

# Key Performance / Key Risk Indicators (KPI/KRI)

- Terms:
  - Factor - value that can change over time (e.g. alerts generated)
  - Measurement – value of factor at a point in time.
  - Baseline – arbitrary value as a point of reference. (threshold)
  - Metric – value generated compared against other values or baseline
  - Indicator – interpretation of one or more metrics that describes effectiveness of an element of the ISMS
- KPI – Performance of the ISMS
- KRI – progress in regards to goals / risk appetite
  - SLE / ARO / ALE



40

# Testing Data Backups

- Develop scenarios
- Develop a plan that tests all mission-critical data backups
- Leverage Automation (reduces effort, ensures tests occur periodically)
- Minimize business impact
- Ensure coverage (not necessarily in same test)
- Document the results
- Fix or Improve any issues



41

# Testing Recovery Plans

- Checklist Test (aka Desk Check test)
  - Plans are distributed for review
- Structured Walk-Through Test
  - Groups Meet to review. Verifies plan is complete.
- Tabletop Exercises – based on scenario. Verifies everyone knows role(s).
- Simulation Test – drill a specific scenario
- Parallel Test
  - Some systems are copied to alternate site
  - Results are compared with primary site
- Full Interruption test
  - Primary site shut down



42

## Other Training

- Emergency Response
- Fire Safety
- First Aid, CPR
- Technical training for support systems



43

## Next Steps…

- Continue Discussion on Class Website
- Questions?



44