

Managing the Assessment Project

- The “yellow brick road”
 - Scope
 - Methodology
 - Report/deliverable
- Detours along the way
 - Expectations
 - “Rules of Engagement”
 - Points of contact
 - Logistics

Class 6

1

Security Assessment Process Overview

- Scope – How much to review, in what detail
- Standards against which to perform the assessment
- Methodology - methods and tools to perform assessment
- Fact finding – Collect information about security configuration
- Analysis – Determine security vulnerabilities, potential consequences, and likely countermeasures
- Delivery – Provide report to management, with recommendations for action

Class 6

2

Managing the Assessment Project

- Scope
 - Why is the assessment being held (and what is necessary to satisfy this need)?
 - Which parts of the organization will be evaluated?
 - What servers should be evaluated?
 - Which subnets?
 - Which desktop systems?
 - Which facilities?
 - Who will be interviewed?
 - How in-depth will the technical review be?
 - What will the deliverable look like? How detailed will it be?

Class 6

3

Managing the Assessment Project

- Standards
 - Risk-based
 - Applicable published standards:
 - NIST
 - PCI
 - HIPAA
 - NSA/IAM or NSA/IEM
 - Other
 - “Best practices”
 - Specific client-specified standards

Class 6

4

Managing the Assessment Project

- Methodology
 - Tools used
 - Who will be interviewed
 - What documentation will be reviewed
 - How facts will be compared to standards
 - Compliance vs. non-compliance
 - Ranking of risk (hi/med/low)

Class 6

5

Managing the Assessment Project

- Fact Finding
 - Process of obtaining information about the security status of systems and processes with scope
 - Uses specified tools and methodology
 - May be documented as a report sections consisting solely of fact finding results, without any added judgement or analysis

Class 6

6

Managing the Assessment Project

- Analysis
 - Using the raw information obtained via fact finding, determine if the security configuration satisfies the standard
 - If part of scope, assess level of risk in any deficiency found
 - Involves the professional judgement of the security assessor

Class 6

7

Managing the Assessment Project

- Report/deliverable
 - Format
 - Size
 - Sections
 - Audience

Class 6

8

Managing the Assessment Project - General

- “Rules of Engagement”
 - General rules for conducting the assessment, to ensure impact on normal operations is minimized
 - Essential where an outside party is directly accessing systems, using tools to obtain security configuration information
 - Especially essential for a penetration test

Class 6

9

Managing the Assessment Project - General

- Points of contact
 - Management
 - Report regular process
 - Resolve internal political issues
 - Report critical, urgent issues
 - Technical
 - Resolve any problems caused by scanning or other activity
 - Prevent panic about network under attack

Class 6

10

Managing the Assessment Project - General

- Logistics
 - Work location
 - Where will interviews be held?
 - Network connections for email
 - Administrative support (phones, printers, copy machines, etc.)
 - Parking, building access

Class 6

11

The Assessment Proposal

- The work proposed to be conducted
- A typical proposal describes the:
 - Objectives
 - Scope
 - Methodology
 - Timeframe
 - Report format
 - Risks and required client commitment

Class 6

12

Managing the Assessment Project

- Make sure you have written approval of ALL management whose approval is required.
 - The authority to spend money on the assessment is not the same as the authority to perform an assessment.
 - A key manager that refuses to cooperate with an assessment can sink the entire project. Better to know this before starting!

Class 6

13

Managing the Assessment Project

- Project plan
- Kick-off meeting
- Periodic status meetings
- Wrap up meeting (“out brief”)
- Optional
 - Interview management to assess criticality of systems
 - Research to determine likely threats

Class 6

14

The Final Report

- Length
 - What does the client expect?
 - What is appropriate for the scope?
- Audience for report (and how to deal with multiple audiences)
 - Executive summary
 - Main report body
 - Appendices for detailed technical review

Class 6

15

The Final Report

- Executive summary
- Main report body:
 - Background
 - Scope
 - Methodology
 - Findings
 - Recommendations
- Appendices for detailed technical review

Class 6

16

The Final Report

- How to indicate relative importance of findings? One way is with respect to normal management processes:
 - *Essential*, the risk is high enough that normal processes should be short-circuited
 - *Important*, normal management processes should govern countermeasure implementation
 - *Observe*, no specific action required, other than to ensure vulnerability does not become a problem
- Specific data stores, systems, and business processes affected by a vulnerability should be noted

Class 6

17

Assessment Standards

- If performed for a specific standards evaluation (HIPAA, PCI, NIST, etc.) then standards are specified.
- If not then vulnerabilities can be of 3 types:
 - Inherent vulnerabilities
 - Organizational policy violations
 - Best-practice violations

Class 6

18

Assessment Coverage

- IT Management
- End user practices
- Physical security
- Technical Security
 - Servers
 - Network
 - Desktop systems

Class 6

19

Assessing IT Management

- Account Management
 - Who adds, changes, disables end user accounts?
 - What about system administrators, programmers, etc.
- Change Control
 - Are all production changes approved and documented?
- Security Management
 - Policies
 - Procedures
 - Standards

Class 6

20

Assessing IT Management

- Which systems are most critical to the business?
 - If nobody is sure, then this itself is a finding
- Is there a good inventory of systems?
- Is there a network topology map (and associated documentation)?
- If you don't know you have it, you can't secure it!

Class 6

21

Assessing End User Practices

- Do end users understand management directives?
 - Review end user training materials, published policies, etc.
 - Interview end users.
 - Observe working practices
 - Walkthrough during lunch. Note unattended workstations

Class 6

22

Assessing Physical Security

- Does physical security support information security objectives?
 - Front lobby
 - Main server room
 - Wiring closets
 - Conference rooms (open Ethernet jacks, etc.)
 - End user areas
 - Trash bins
 - Who controls facility security? Are these systems secure?

Class 6

23

Technical Assessment Tools

- Intent is to review host configuration for known security flaws and/or compliance with security standards and policies
- Requires informed client cooperation to install and use these on client systems or networks
 - Open discussion of risks and agreement how to minimize these
- A clean de-installation is very important once information has been collected

Class 6

24

Technical Assessment Tools

Examples:

- CISecurity audit tools, host assessment tools
- Nessus/Nmap, network-based tools
- Microsoft Baseline Security Analyzer, host assessment tool for Microsoft systems
- CA-Examine, Vanguard tools for legacy mainframe analysis

Class 6

25

Technical Assessment Areas

- Authentication (password policies)
- Access Control
- Audits (event logging)
- Security patches up-to-date
- Only required and documented services and applications present
- Physical control over boot access and system console

Class 6

26

Technical Assessment Areas - Authentication

- Authentication (password policies)
 - Default passwords changed?
 - Password length
 - Password composition
 - Regular password change

Class 6

27

Technical Assessment Areas – Access Control

- Access Control
 - Supported by file system?
 - Levels/categories of user?
 - Which file system objects protected? How?
 - Access controls over non-file objects:
 - Printers
 - Network access
 - OS commands
 - Application functions

Class 6

28

Technical Assessment Areas – Auditing

- Auditing (event logging)
 - Enabled?
 - What is logged?
 - Success / failures?

Class 6

29

Technical Assessment Areas – Patch Management

- Security patches up-to-date
 - Which patches are required?
 - Which have been performed?

Class 6

30

Technical Assessment Areas – Minimize services

- Only required and documented services and applications present
 - What is running?
 - Network provided services?
 - Other services?
 - Should it be running?

Class 6

31

Technical Assessment Areas – Physical Access Control

- Physical control over boot access and system console
 - Who can access server?
 - What boot media can be used?
 - Any evidence of boot from media?

Class 6

32