Phase 2: Augmenting Rules

Add Additional Information to Rules

- References
  - Pointers to further information
- Assessment Categories
  - How can the rule be tested or verified?

Why Add References?

- Facilitate communication between benchmark author and audience
- Clearly indicate applicable platform
- Cite precise configuration controls
- Refer to widely-recognized regulatory frameworks

Common References

- CPE: Common Platform Enumeration
- CCE: Common Configuration Enumeration
- NIST Special Publication 800-53: *Recommended Security Controls for Federal Information Systems*

Common Platform Enumeration (CPE)

- Standard names for platform types
- Unambiguous indication of benchmark target
- Sections can be labeled as appropriate
  - Functionality only available in a specific version
  - For a supporting application

http://cpe.mitre.org/

CPE Examples

- Operating Systems
  - cpe:/o:redhat:enterprise_linux:5.0
- Applications
  - cpe:/a:microsoft:excel:2003:sp2
- Hardware
  - cpe:/h:apple:iphone:1.1.2

Common Configuration Enumeration (CCE)

- Standard enumeration of security-relevant configuration controls
- Technical and platform-specific
- Does not assert a recommendation
- Allows fast, accurate correlation
  - Across repositories
  - By different groups of people
  - Between different tools

http://cce.mitre.org/

CCE Example

ID	CCE-2891-0
DESCRIPTION	The "Disable CTRL+ALT+Delete Requirement for Logon" policy should be set correctly.
PARAMETER	Enabled / Disabled
TECHNICAL MECHANISM	(1) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD (2) defined by Local or Group Policy
REFERENCE	NIST SP 800-68: Table: 5.28 Value: disabled

NIST SP 800-53

Title	Recommended Security Controls for Federal Information Systems
Publisher	National Institute of Standards and Technology (NIST)

- Provides recommended minimum security controls
  - For compliance with FISMA (Federal Information Security Management Act)
- Widely used outside of government
- Freely available
- High level and cross-platform

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

800-53 Example

ID	AC-9
TITLE	PREVIOUS LOGON NOTIFICATION
CONTROL	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.
SUPPLEMENTAL GUIDANCE	None
CONTROL ENHANCEMENTS	None

Other References

- Many other forms of references can add value and context to your documents
  - Enumerations – CVE, CWE, CAPEC, etc.
  - High-level controls – ISO/IEC, NIST 800-26, etc.
  - Guidance – FDCC, other benchmarks
  - Organization-specific directives – E.g. CSO mandates

Exercise 5: Add References with RT

- Add references to the “Maximum Password Age” rule
- Demo version of the RT can be found here:
  - C:\BDCTools\rt\RTClient.jar
- Log in as:
  - Username: ‘bsmith’
  - Password: ‘password’

Rule Categories

Check

- A tool can run a test and decide TRUE or FALSE

Report

- A report is needed for further analysis to determine compliance

Question

- A question must be asked of a user to determine compliance

Category Hierarchy

Check

- Can extract relevant system data
- Can evaluate extracted data

Report

- Can extract relevant system data
- CANNOT evaluate extracted data
  - Requires human judgment (What is “sufficient”, “necessary”?)
  - Lack the technical means to evaluate (complex operation)

Question

- CANNOT extract relevant system data
  - Data does not exist on scanned system (“Is door locked?”)
  - Cannot locate the data
  - Lack the technical means to extract the data (new repository)

MITRE

Benefits to Categorization

- Applying assessment categories to rules during development:
  - Suggests the level of effort required to add compliance checks to a benchmark
  - Provides a rough estimate of how much of a guide can be covered with compliance checks
  - Helps indicate which checking system to use

Exercise 6: RT Categorization

- Categorize the rules for the ‘Microsoft Windows XP’ guide
- Demo version of the RT can be found here
  - C:\BDCTools\rt\RTClient.jar
- Log in as:
  - Username: ‘bsmith’
  - Password: ‘password’

Exercise 6 Continued: RT Categorization

Review each rule and determine the appropriate category.

Check

- Can extract relevant system data
- Can evaluate extracted data

Report

- Can extract relevant system data
- CANNOT evaluate extracted data
  - Requires human judgment (What is "sufficient", "necessary"?)
  - Lack the technical means to evaluate (complex operation)

Question

- CANNOT extract relevant system data
  - Data does not exist on scanned system ("Is door locked?")
  - Cannot locate the data
  - Lack the technical means to extract the data (new repository)

MITRE