Benchmark Development Course

Purpose

Designed to teach participants how to create Security Guidance that is

Standards-based

Structured

Automatable

through five phases of development

Share MITRE's experience, knowledge, and tools to help vendors and security content developers produce good guidance more efficiently.

Approach

- Describe best practices in developing security guidance
- Demonstrate how the new benchmarking technology applies to security guidance
- Provide tools to facilitate guidance development
- Showcase completed benchmarks

Audience Participation Encouraged

MITRE

Demonstrations

Platform

- Windows XP

Examples

- Password Strength, Complexity

MITRE

Take Away

Participants should…

…understand the key factors that go into producing good security guidance

…have a general awareness of the tools that are available to assist them in developing a new configuration guide

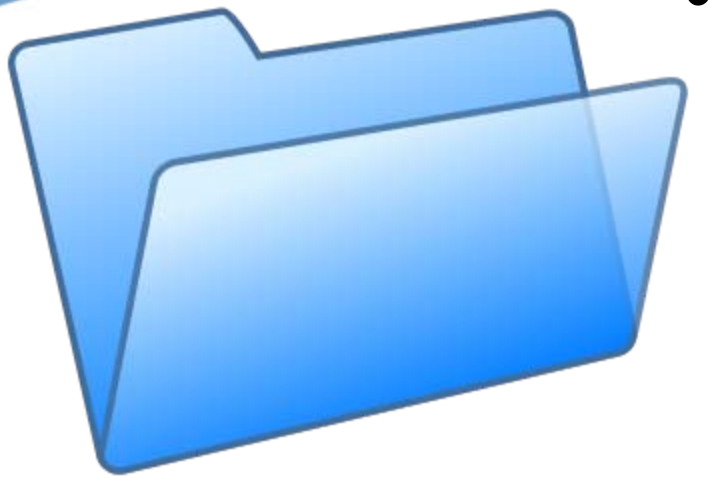
…have a general knowledge of the standards that are utilized for expressing security guidance

…understand why it is crucial to facilitate security guidance through standardization

CD

- BDC_CD
  - BDC Slides
  - BDC Tools
    - Benchmark Editor
    - ovaldi
    - Reference Docs
    - rt
    - samples
    - wit
  - Benchmark Guide
  - Informational Flyers
    - CVE, OVAL, CCE, CPE, Benchmark Editor, and more
  - XCAT

System Course Material



- BDC Tools
  - Benchmark Editor
  - ovaldi
  - Reference Docs
  - rt
  - samples
  - wit
- XCAT

Feedback

benchmarkcourse@mitre.org

Questions • Comments • Suggestions

For the most up to date information join the Benchmark Discussion Forum found at: http://benchmarkdevelopment.mitre.org/

What is a Benchmark?

A document that specifies settings and option selections that minimize the security risks associated with computer hardware or software.

Two Types of Benchmarks

Benchmark

- Security guidance written using the XCCDF language
- Does not include compliance checks
- *Could be* read, translated, and presented by checking tools, but *does not* contain information needed to evaluate compliance

Automated Benchmark

- Security guidance written using the XCCDF language and one or more checking languages
- This document *is* intended to contain the information needed to evaluate compliance

MITRE

Why create benchmarks?

- Create/customize guidance for your customers/enterprise that can be used by many tools
- Ensure explicit understanding of compliance requirements
- Build off of an ever-growing library of existing content – you don't need to start from scratch

Why are benchmarks important?

- Structured, accessible, automatable guidance is easier to understand and implement
- *Consistent* and *standardized* approach to developing and documenting data provides enormous value to administrators

How is a Benchmark Used?

Reporting

- maintain state
- provides audit trail

Determine Compliance

- manual checking
- automated checking

Benefits of Automated Benchmarks

- Repeatable
  - Guidance is accompanied by machine-readable tests for compliance
- Faster
  - Compliance assessment is no longer a difficult manual process
- Correlation
  - Results are augmented with standard identifiers for issues

The Security Content Automation Protocol (SCAP)

- SCAP is a set of six standards endorsed by the National Institute of Standards and Technology (NIST)
- SCAP allows exchange of end-system security content and automated compliance testing
- Four of the standards directly support automated benchmarks

SCAP Component Standards

What IT systems do I have in my enterprise?	• CPE
What are the configurable elements on my system?	• CCE
How do I define a policy of secure configurations?	• XCCDF
How can I be sure my systems conform to policy?	• OVAL
What vulnerabilities do I need to worry about?	• CVE
What vulnerabilities do I need to worry about RIGHT NOW?	• CVSS

SCAP Component Standards

What IT systems do I have in my enterprise?	• CPE (Platforms)
What are the configurable elements on my system?	• CCE (Configurations)
How do I define a policy of secure configurations?	• XCCDF (Configuration Checklists)
How can I be sure my systems conform to policy?	• OVAL (Assessment Language)
What vulnerabilities do I need to worry about?	• CVE (Vulnerabilities)
What vulnerabilities do I need to worry about RIGHT NOW?	• CVSS (Scoring System)

Automated Benchmarks with SCAP

What IT systems do I have in my enterprise?	• CPE (Platforms)
What are the configurable elements on my system?	• CCE (Configurations)
How do I define a policy of secure configurations?	• XCCDF (Configuration Checklists)
How can I be sure my systems conform to policy?	• OVAL (Assessment Language)
What vulnerabilities do I need to worry about?	• CVE (Vulnerabilities)
What vulnerabilities do I need to worry about RIGHT NOW?	• CVSS (Scoring System)

Why SCAP?

- Achieve benefits of automated benchmarks via widely recognized standards
- SCAP Validation Program certifies commercial tools as complying with the standards
  - Currently 28 validated tools available
  - Benchmark compliance can be assessed using any SCAP-validated scanner
- In the future, configuring systems to be compliant may be automatable

Benchmark Core Components

- Automation
  - Streamlining user evaluations
- Benchmark Development Tools
  - Create, produce, customize content
  - Locate information
  - Track compliance
- SCAP
  - Standardized format
  - Mappings to common identifiers

Security Guidance Evolution

- Prior to FY01: Traditional Style
  - Security guidance documents were verbose and descriptive, containing architectural, contextual, and tutorial type information
    - Easily 100+ pages
- In FY01: Migrated towards Concise Style
  - Security guidance community influenced by NSA, Center for Internet Security (CIS) and DISA.
    - Concise style of documentation, focusing on application controls

Evolution of Experience

	Application	Produced	Tools
FY05 & FY06	Microsoft Exchange Server Systems Management Server	Word document using Word tables	None
	FY06 Creation of Recommendation Tracker tool		
FY07	Oracle Application Server TIBCO Messaging Server Tivoli Configuration Manager	Automated Benchmark Benchmark Automated Benchmark	Recommendation Tracker
FY08	SharePoint Server 2007 Tivoli Identity Manager	Benchmark Benchmark	Recommendation Tracker

Phases of Benchmark Development