

CERT

Virtual Training Environment: A New Model for Security and Compliance Training

James Wrubel
jcw@cert.org

About CERT®

Carnegie Mellon University

- U.S. Government Center of Excellence in Cyber-Security

Software Engineering Institute

- Federally funded Research and Development Center (FFRDC)
- Sponsor is DoD
- **CERT®**
 - Internet's Hub for Cyber Security

CERT's Training Problem

History

- Four-course IA and Forensics training curriculum (14 instruction days)
- Targeted at system administrators and first responders
- Captured to DVD for retention

Issues

- Logistics
 - Bringing students to material
 - Bringing material to students
- Accessibility
 - Replicating Lab environment
 - Installing DVDs
- Time!

CERT's Solution – VTE

Web-based individual training on IA/IT topics

- Worldwide availability
- Deep, integrated instruction
- Leverages curriculum model and material
- Establish expert network to add/improve content

Content Types

- **Documents:** Handbooks, technical notes, white papers
- **Demos:** Narrated recordings of instructors configuring systems and software
- **Lectures:** Video-captured course deliveries including student interactions
- **Labs:** Hands-on environments using virtual machine technology

CERT's Solution – VTE (2)

Library Mode

- Open, public access (except for Labs)
- Quick access to specific topics and content

Training Mode

- Instructor-facilitated courses online using CERT material
- Robust progress tracking and reporting
- Quizzes
- Content neutral

How VTE Helps

No Logistics Necessary

- Travel, lodging, per diem, opportunity cost
- The lab in the basement

Rich, Interactive, Accessible Content

Visible Training Progress

- Quizzes
- Group and Individual Reporting

Context

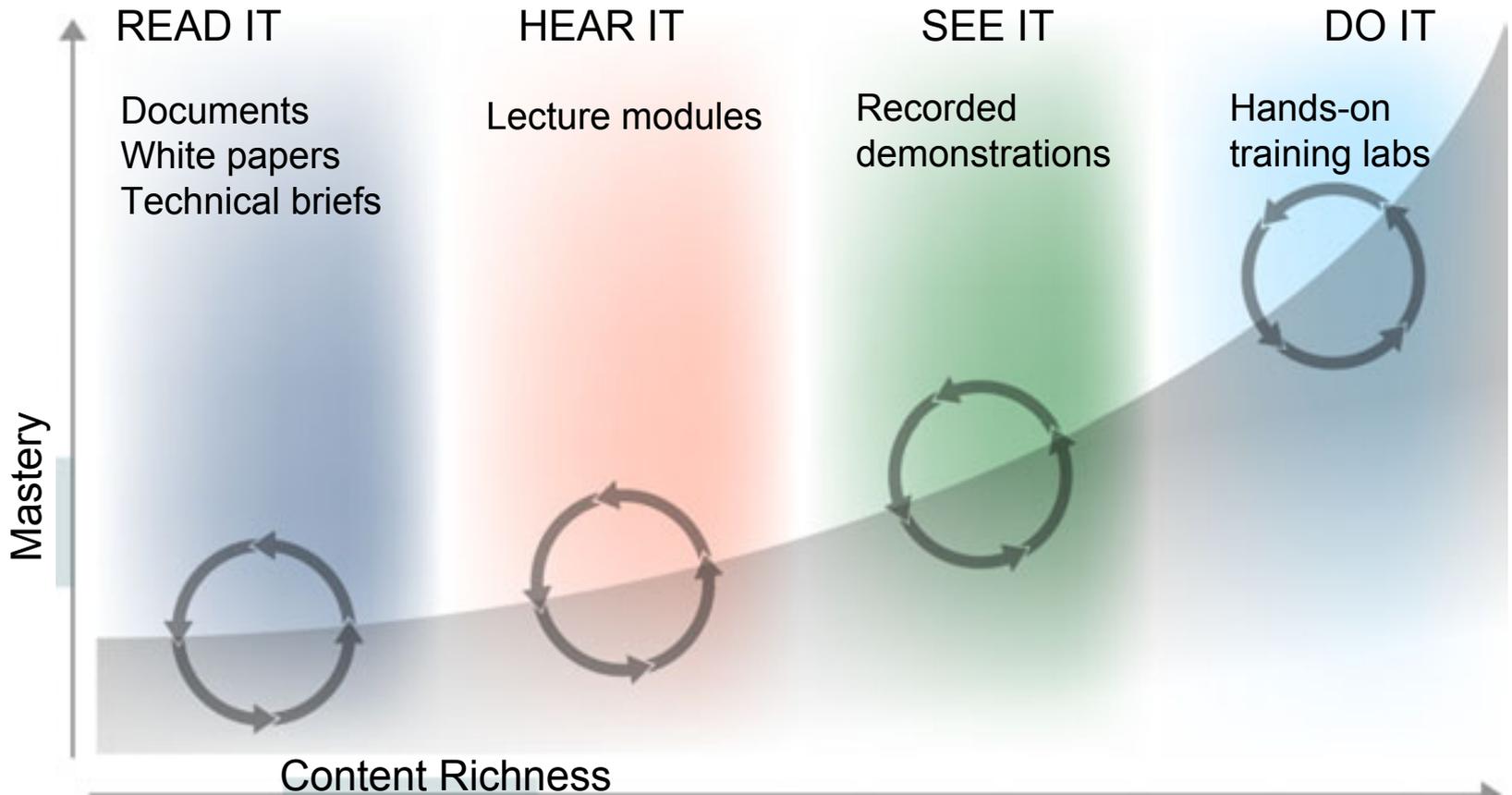
- Scenarios woven through content
- Video from student POV

Time!

- Interrupt-driven workforce
- Impact of turnover

The VTE 'Power Curve'

“[Students retain] 10 percent of what they read, 26 percent of what they hear, 30 percent of what they see, 50 percent of what they see and hear, 70 percent of what they say, and 90 percent of what they say as they do something.” (Stice 1987).



What You Can Do With VTE

- Take instructor-facilitated courses online
 - Individual
 - Workforce
- Report compliance with training mandates
 - DoD 8570
 - FISMA
- Consolidate or Eliminate Training Labs
- Host Your Own Content
 - Any type VTE can present
 - Access-controlled
- Partner with CERT® to develop new material

VTE: Progress Reporting

Report Filters: No filters have been set.

Set Report Filters

Report using date range

From

26 January 2006 12:00 PM

To

26 January 2006 12:00 PM

Show data from people I manage directly.

Show data from people I manage directly and indirectly.

Report on user group(s)

Add/Remove Groups

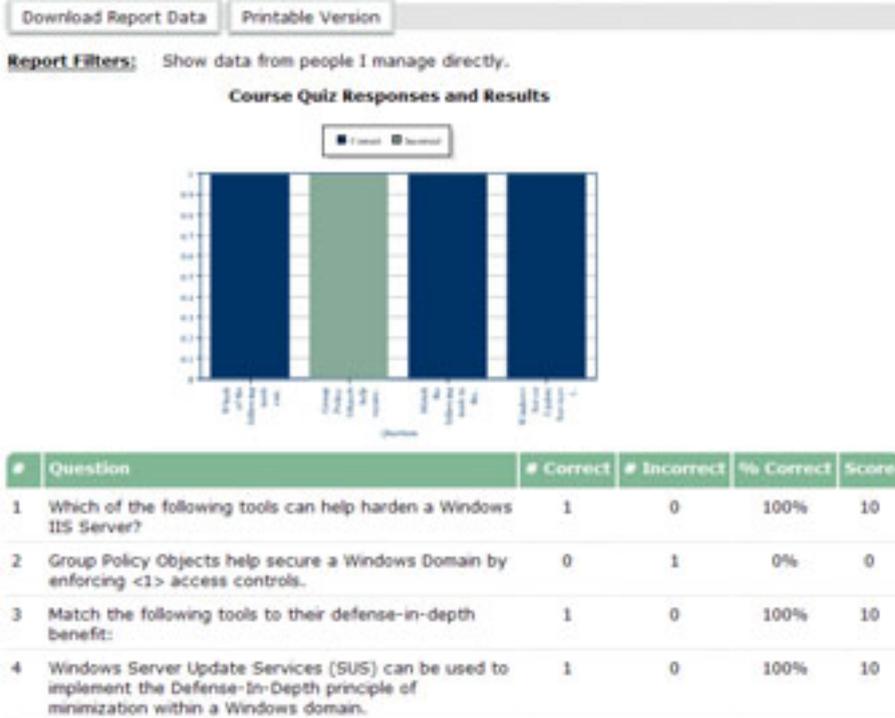
Save

Reset

Cancel

- Filter reports based on:
 - People you manage (direct or indirect)
 - Specific Groups
 - Time ranges

VTE: Progress Reporting - 2



- Individual Question level
- Who answered what, how?
- Multiple formats for report data
 - Online
 - CSV
 - Printable summary

VTE System Requirements

Web Browser: IE 6.0+ or Mozilla Firefox 1.0+

Screen Resolution: 1024x768+

Broadband Internet Connection (>200kbps)

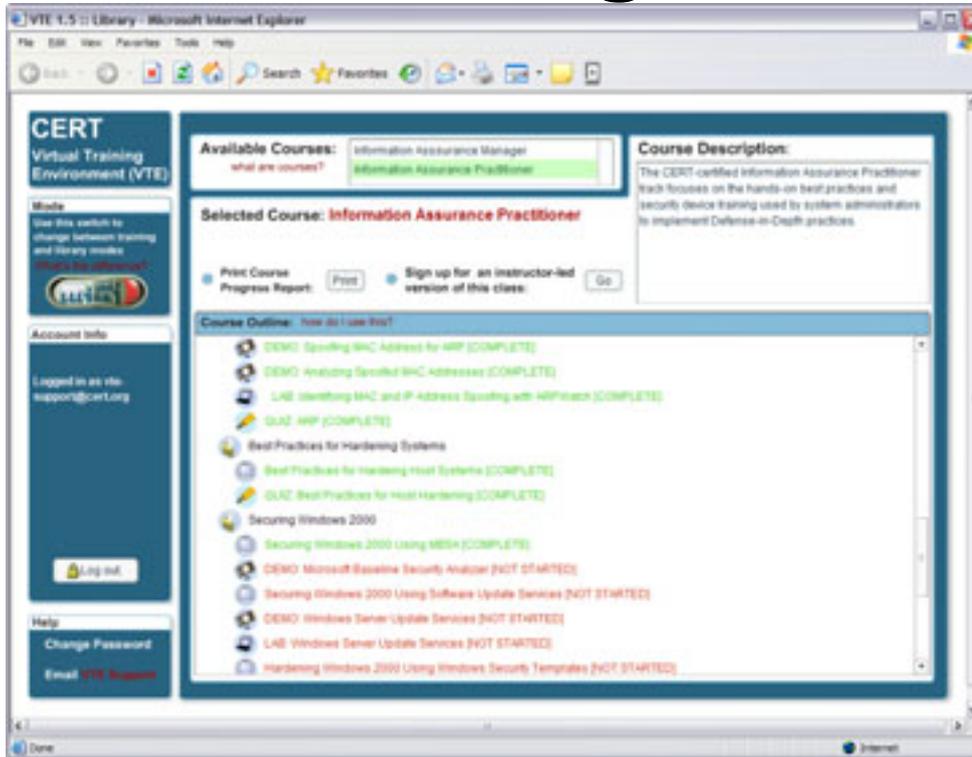
- Sometimes a problem in deployed environments

For Curriculum/Library/Video: Macromedia Flash 6.0 r65+

For Lab environment:

- Internet Explorer must be configured to allow signed ActiveX or Signed Applets to run (or pushed out using GPO)
- For Firefox, Java VM 1.4.2 or 1.5 must be installed

VTE: Training Mode



- Multiple training 'tracks' using outline-style navigation
- Lectures, demos, labs, quizzes
- System handles progress and completion reporting

VTE: Viewing Lecture Topics

The screenshot displays a video lecture player interface. On the left, there is a video thumbnail showing a man in a blue shirt standing in a room. Below the thumbnail are tabs for 'Outline', 'Thumbs', 'Notes', and 'Search'. Under 'Slide Notes', the text reads: 'actually go ahead and correct this if you want. You can go out to Microsoft's site, download the hot fixes or it'll tell you if there's no hot fix available, what you need to do to'. A progress bar at the bottom of the notes section shows '5 minutes 31 seconds Remaining'. The main slide area is titled 'Hardening Windows 2000 Systems' and contains the following text: 'Determine the initial security posture of system' followed by two bullet points: '▪ Microsoft Baseline Security Analyzer (MBSA)' and '▪ Languard Network Security Scanner'. Below the text are two screenshots: the first shows a Windows XP desktop with a command prompt and a file explorer window, and the second shows the Microsoft Baseline Security Analyzer (MBSA) application window. At the bottom of the slide, there is a control bar with a play button, a progress bar, and the text 'Slide 2 of 3 | Playing 05:28 / 1:0:58'. The slide footer includes '© 2005 by Carnegie Mellon University' and the CERT logo.

- Synchronized slide and video with available searchable transcript
- VCR-style controls
- Remembers where you left off

VTE: Assessments

QUIZ: Windows 2000 Hardening

Which of the following tools can help harden a Windows IIS Server?

- A) NTFS Permissions
- B) Active Server Page (ASP) Lockdown Tool
- C) IISHarden.exe
- D) IISLockdown.exe

Submit Clear

QUIZ: Windows 2000 Hardening

Complete the sentence below by filling in the blanks.

Group Policy Objects help secure a Windows Domain by enforcing access controls.

Submit Clear

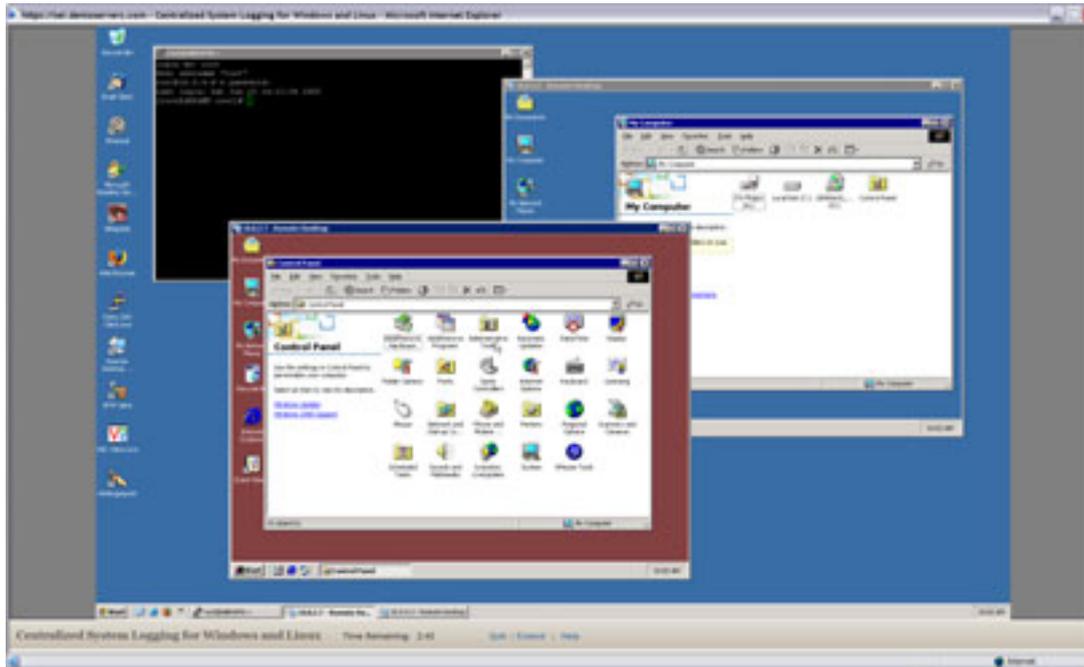
QUIZ: Windows 2000 Hardening

Match the following tools to their defense-in-depth benefit:

Column 1	Column 2
<ul style="list-style-type: none"> <input type="checkbox"/> IRLScan.exe <input type="checkbox"/> Security Configuration Toolkit <input type="checkbox"/> Host-Based Firewall <input type="checkbox"/> IIS <input type="checkbox"/> IISLockdown 	<ul style="list-style-type: none"> A. Used to apply patches to servers across the organization from a central location B. Provides network level access controls according to predefined rules C. Provides policy level access controls according to predefined templates D. Used to block certain types of requests at the IIS level E. Assesses the security posture of one or more Windows hosts

Submit Clear

VTE: Hands-on Labs



- Synchronized slide and video with available searchable transcript
- VCR-style controls
- Remembers where you left off

Questions? Trial Accounts?

<https://vte.cert.org>

