CERT

Virtual Training Environment
Information Assurance and Forensics Training
Anywhere, Anytime

James Wrubel
VTE Platform Lead, CERT
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, perdiem, 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 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
  - For Firefox, Java VM 1.4.2 or 1.5 must be installed
Who’s Using VTE: DoD

The Army Reserve Information Operations Command uses VTE to:

- Quickly spin up new soldiers
- Train in deployed environments (including Iraq)
- Certify soldiers on VTE material
- Build a Cisco Network Device security specialization

The Marine Forces Pacific is using VTE to:

- Pilot 8570 compliance training requirements
- Train in deployed environments
- Build a Cisco Network Device security specialization
Who’s Using VTE: Federal Agencies

The U.S. Department of Homeland Security uses VTE to:

- Develop and deploy custom training material for gap areas such as Computer Forensics
- Support intra-agency training
- Improve Cyber Incident Response capabilities

The U.S. Secret Service will use VTE to:

- Support anywhere, anytime access to computer forensics material (including podcasting)
- Maintain a robust on-demand training capability for forensic tools such as EnCase® Enterprise Edition, AccessData Forensic Toolkit®, and OnlineDFS
VTE: Demonstrations
VTE: Training Mode

- Multiple training ‘tracks’ using outline-style navigation
- Lectures, demos, labs, quizzes
- System handles progress and completion reporting
VTE: Viewing Lecture Topics

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

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

Complete the sentence below by filling in the blanks.
Group Policy Objects help secure a Windows Domain by enforcing access controls.

Launch
VTE: Hands-on Labs

Launch

- Browser-based, embedded desktop
- Uses virtual machine technology
- Deploys on demand
Questions? Trial Accounts?

End Session

Your session has ended.

OK