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

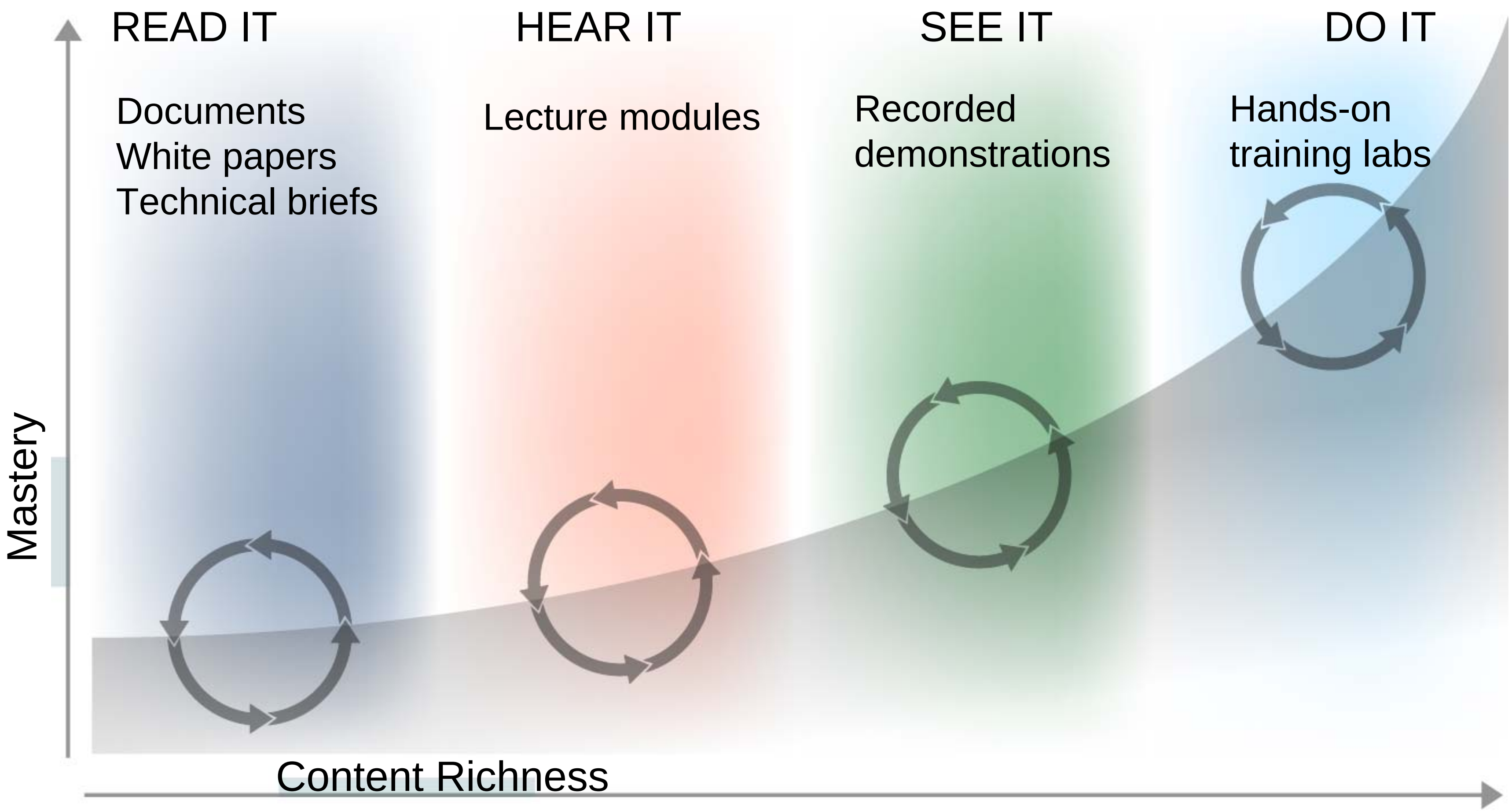
- Scenarios woven through content
- Video from student POV

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

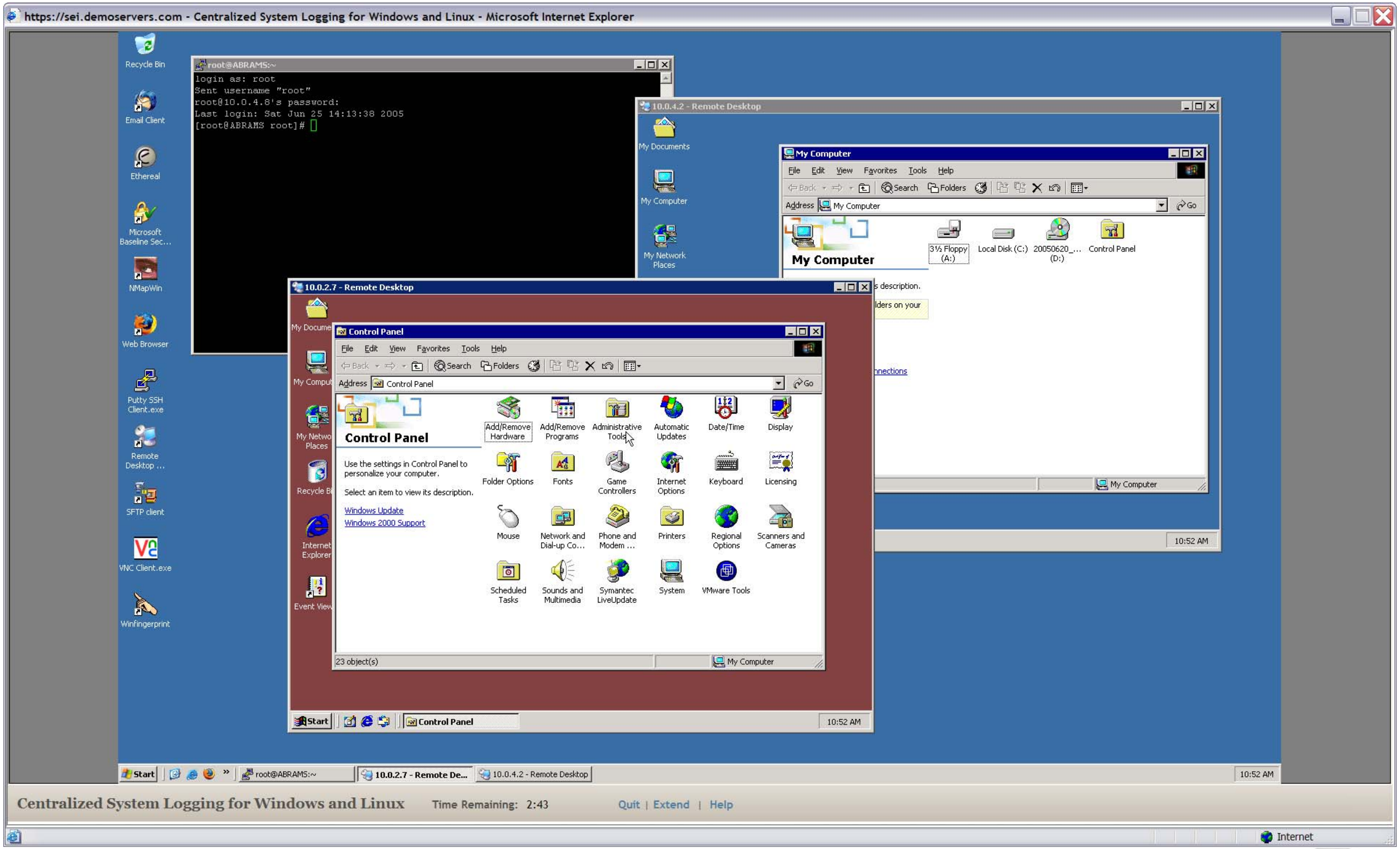
The U.S. Department of Homeland Security uses VTE to:

- 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



https://sei.demoservers.com - Centralized System Logging for Windows and Linux - Microsoft Internet Explorer

root@ABRAMS:~

```
login as: root
Sent username "root"
root@10.0.4.8's password:
Last login: Sat Jun 25 14:13:38 2005
[root@ABRAMS root]#
```

Control Panel

Use the settings in Control Panel to personalize your computer.

Select an item to view its description.

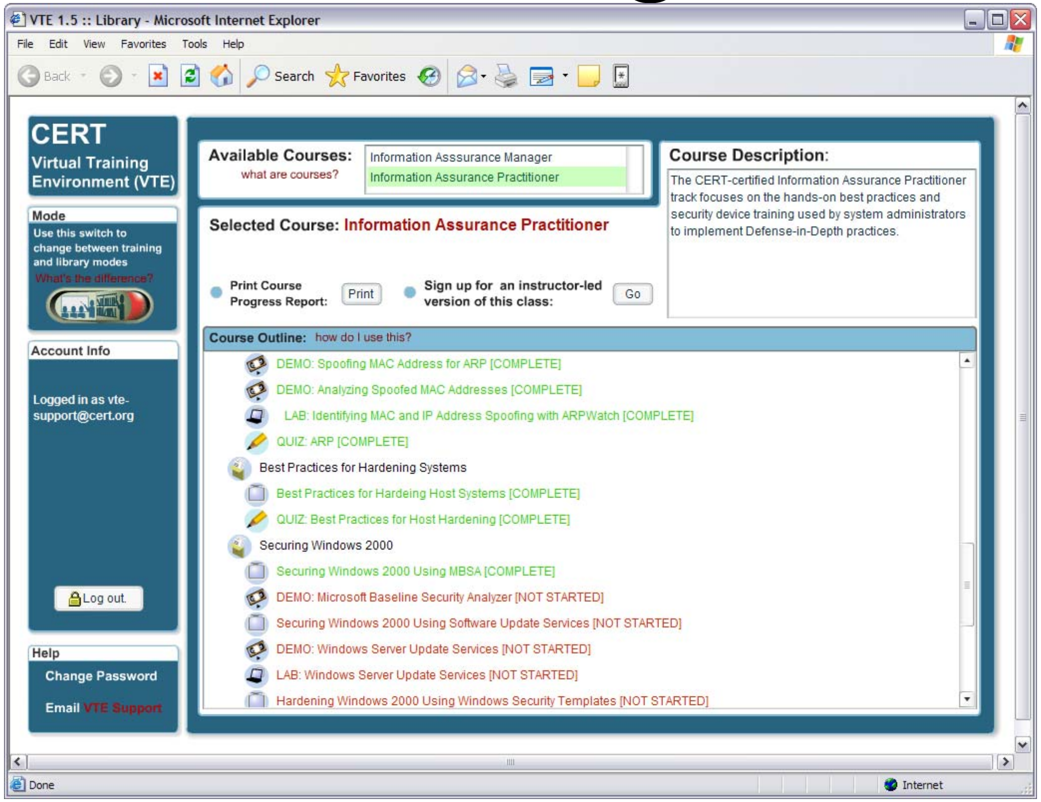
Windows Update

Windows 2000 Support

23 object(s)

Centralized System Logging for Windows and Linux Time Remaining: 2:43 Quit | Extend | Help

VTE: Training Mode


VTE 1.5 :: Library - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Print
Go
Log out
Done
Internet

CERT Virtual Training Environment (VTE)

Mode

Use this switch to change between training and library modes

What's the difference?

Account Info

Logged in as vte-support@cert.org

Help

Change Password

Email VTE Support

Available Courses: what are courses?

Information Assurance Manager

Information Assurance Practitioner

Course Description:

The CERT-certified Information Assurance Practitioner track focuses on the hands-on best practices and security device training used by system administrators to implement Defense-in-Depth practices.

Selected Course: Information Assurance Practitioner

Print Course Progress Report:

Sign up for an instructor-led version of this class:

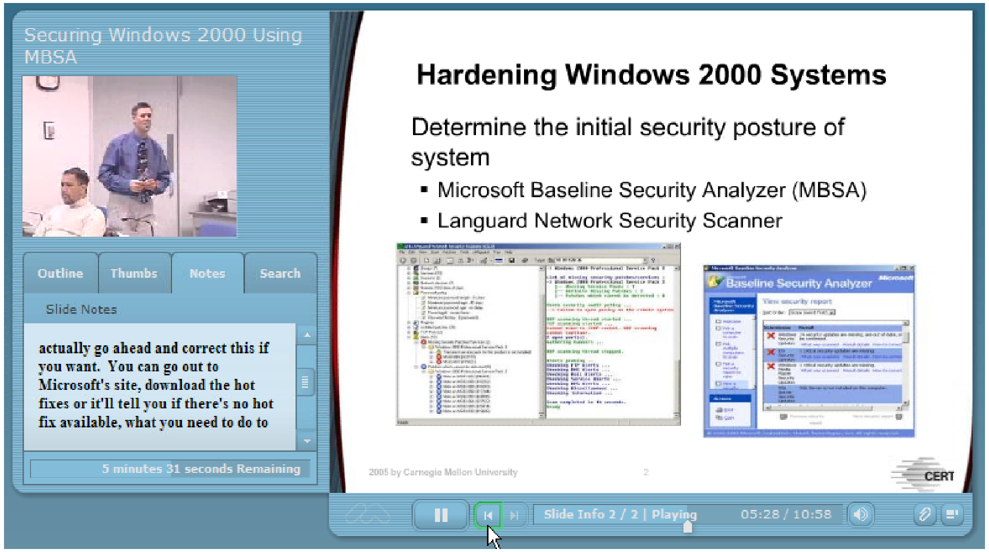
Course Outline: how do I use this?

- DEMO: Spoofing MAC Address for ARP [COMPLETE]
- DEMO: Analyzing Spoofed MAC Addresses [COMPLETE]
- LAB: Identifying MAC and IP Address Spoofing with ARPWatch [COMPLETE]
- QUIZ: ARP [COMPLETE]
- Best Practices for Hardening Systems
  - Best Practices for Hardeing Host Systems [COMPLETE]
  - QUIZ: Best Practices for Host Hardening [COMPLETE]
- Securing Windows 2000
  - Securing Windows 2000 Using MBSA [COMPLETE]
  - DEMO: Microsoft Baseline Security Analyzer [NOT STARTED]
  - Securing Windows 2000 Using Software Update Services [NOT STARTED]
  - DEMO: Windows Server Update Services [NOT STARTED]
  - LAB: Windows Server Update Services [NOT STARTED]
  - Hardening Windows 2000 Using Windows Security Templates [NOT STARTED]

Launch

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

VTE: Viewing Lecture Topics



Securing Windows 2000 Using MBSA
Outline
Thumbs
Notes
Search
Slide Notes
5 minutes 31 seconds Remaining
Slide Info 2 / 2 | Playing
05:28 / 10:58

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

Hardening Windows 2000 Systems

Determine the initial security posture of system

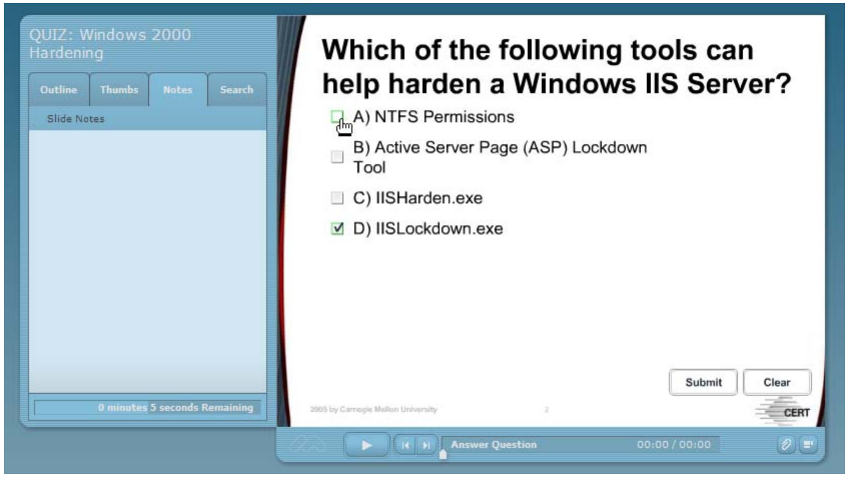
- Microsoft Baseline Security Analyzer (MBSA)
- Languard Network Security Scanner

Baseline Security Analyzer
2005 by Carnegie Mellon University
2
CERT

Launch

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

VTE: Assessments


QUIZ: Windows 2000 Hardening
Outline
Thumbs
Notes
Search
Slide Notes
0 minutes 5 seconds Remaining
Submit
Clear
2005 by Carnegie Mellon University
2
CERT
Answer Question
00:00 / 00:00

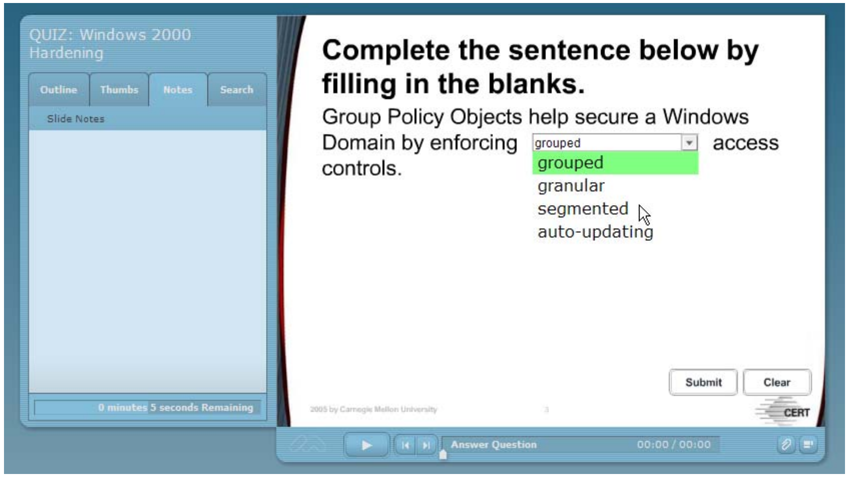
Which of the following tools can help harden a Windows IIS Server?

□ A) NTFS Permissions

□ B) Active Server Page (ASP) Lockdown Tool

□ C) IISHarden.exe

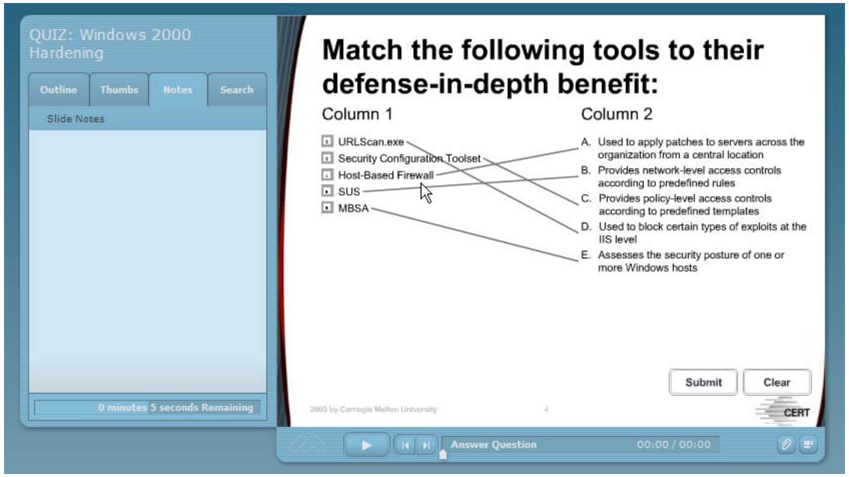
☑ D) IISLockdown.exe


QUIZ: Windows 2000 Hardening
Outline
Thumbs
Notes
Search
Slide Notes
0 minutes 5 seconds Remaining
Submit
Clear
2005 by Carnegie Mellon University
3
CERT
Answer Question
00:00 / 00:00

Complete the sentence below by filling in the blanks.

Group Policy Objects help secure a Windows Domain by enforcing [grouped ▾] access controls.

- grouped
- granular
- segmented
- auto-updating


QUIZ: Windows 2000 Hardening
Outline
Thumbs
Notes
Search
Slide Notes
0 minutes 5 seconds Remaining
Submit
Clear
2005 by Carnegie Mellon University
4
CERT
Answer Question
00:00 / 00:00

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

Column 1

- URLScan.exe
- Security Configuration Toolset
- Host-Based Firewall
- SUS
- MBSA

Column 2

A. Used to apply patches to servers across the organization from a central location

B. Provides network-level access controls according to predefined rules

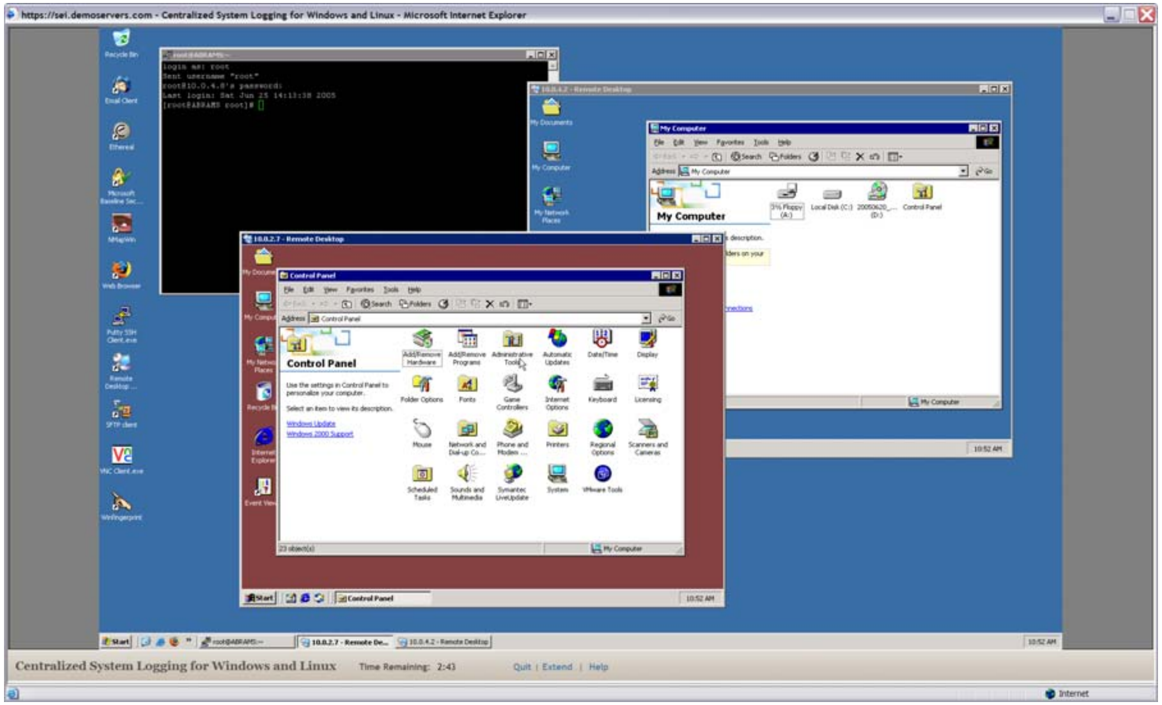
C. Provides policy-level access controls according to predefined templates

D. Used to block certain types of exploits at the IIS level

E. Assesses the security posture of one or more Windows hosts

Launch

VTE: Hands-on Labs



https://sei.demoservers.com - Centralized System Logging for Windows and Linux - Microsoft Internet Explorer

```
login as: root
Sent username "root"
root@10.0.4.8's password:
Last login: Sat Jun 25 14:13:38 2005
[root@ABRAMS root]#
```

Control Panel

Use the settings in Control Panel to personalize your computer.

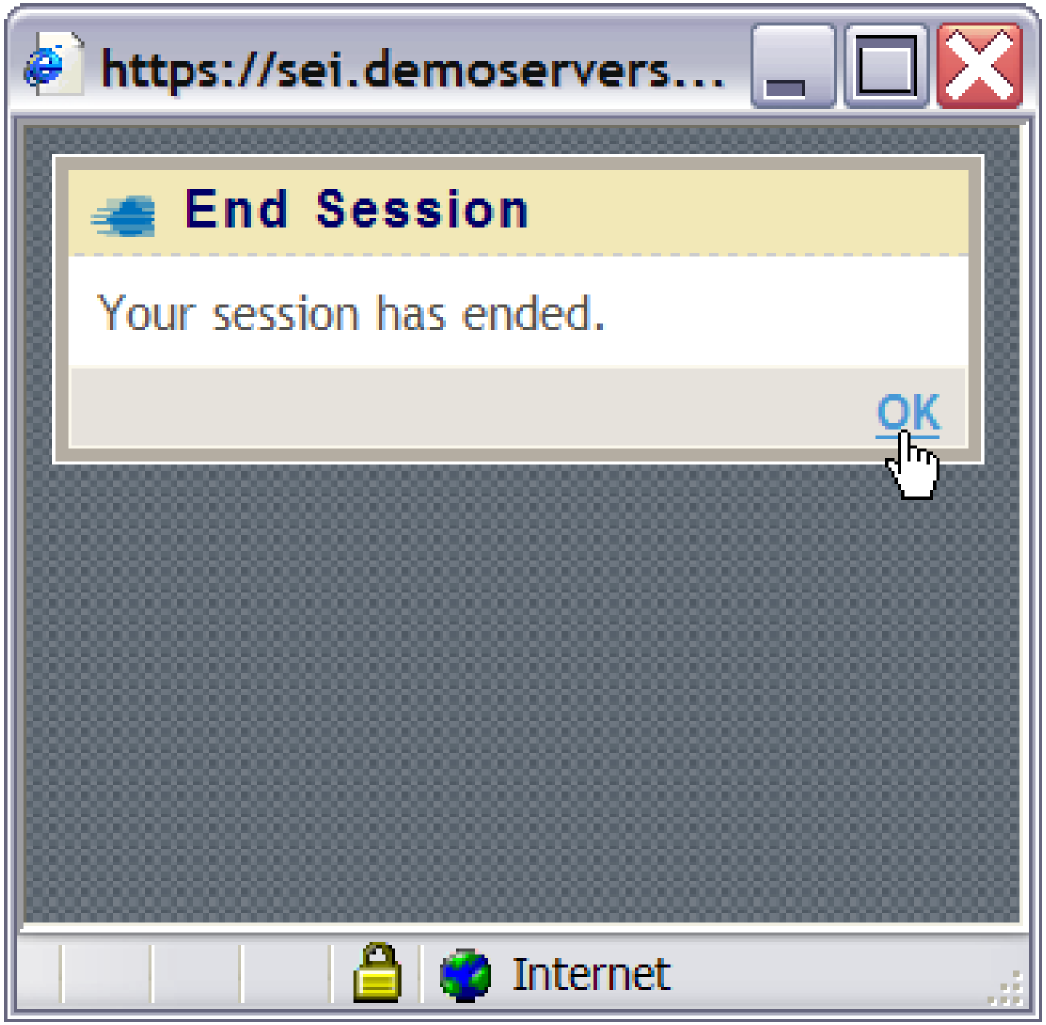
Select an item to view its description.

Centralized System Logging for Windows and Linux Time Remaining: 2:43

[Launch](#)

- Browser-based, embedded desktop
- Uses virtual machine technology
- Deploys on demand

Questions? Trial Accounts?



End Session

Your session has ended.