Certified Virtualization Security Expert, Part 6 of 6: Hardening and Third Party Tools

Meet the expert: Duane has been working in the IT industry for over two decades. He has primarily focused on security related matters such as
Penetration Testing and Forensics. He has appeared as an expert witness in multiple court hearings on IT related matters. Duane has worked for or with most US and some foreign military branches, U.S government agencies, banking and regulatory industries and Fortune 500 companies. Duane contributed to the coordination and execution of IT counter-hacking & security courses for the US Marine Corps, US Army, US Air Force, U.S. Treasury, Sprint, IBM, Washington Mutual and Service Canada.

Tim one of the World’s leading trainers in technology, >networks, virtualization and, applications. He has been a technical trainer and consultant for security and virtualization for the past 25 years. He has 29 industry technical certifications from CISCO, Microsoft and Novell. Tim has been a noted speaker at many industry events such as Infosec World 2010, Innatech and GISSA. He is a contributing author of VMware vSphere and Virtual Infrastructure Security Securing ESX in the Virtual Environment.

Prerequisites: This is part 6 of the series.

Runtime: 01:49:52

Course description: This course finishes out the series by taking a look at the differences between ESX and ESXi. It discusses Root privileges, controlled access, and securing SNMP configuration. This course discusses how to audit or disable tech support mode and provides an overview of third party security players as add-ons such as: Catbird, Altor, HyTrust, Reflex and Tripwire.

Course outline:

Hardening VirtualCenter
- Introduction
- Set up the Windows Host for VirtualCenter
- Limit Network Connectivity to VirtualCenter
- Proper Security Measures
- Certificate-Based Encryption
- vCenter Log Files and Rotation
- Collecting vCenter Log Files
- VirtualCenter Custom Roles
- Document and Minitor Changes to the Configuration
- VirtualCenter Add-on Components
- VMware Update Manager
- VMware Converter
- VMware Guided Consolidation
- General Considerations
- Client Components
- Verify the Integrity of the VI Client
- Monitor the Usage of VI Client Instances
- Avoid the Use of Plain-Text Passwords
- vShield Zones Overview
- vShield VM Wall and Flow Features
- Summary

Hardening VirtualCenter Demo
- Introduction
- Demo: vShield Manager
- Demo: Deploy OVF Template
- Demo: Configure Install Parameters
- Demo: Add vShield Plugin
- Demo: Datacenter Changes
- Summary

Hardening Virtual Center Demo Part 2
- Introduction
- Demo: Verify Protection
- Demo: Zenmap
- Demo: Deny the vSphere Client at the DataCenter
- Demo: Communicating from Inside the Data Center
- Demo: Scanning
- Demo: VM Flow
- Summary

Third Party Mitigation Tools
- Introduction
- The Virtualization Security Players
- 1K View of Altor
- 1K View of Catbird and Hytrust
- 1K View of Reflex
- 1K View of Trend Microsystems
- 1K View of Tripwire
- In-Depth Look at HyTrust
- HyTrust Key Capabilities: Unified Access Control
- HyTrust Key Capaibilties: Policy Management
- HyTrust Key Capabilities: Audit-Quality Logging
- In-Depth Look at Catbird
- Trust Zones
- Catbird: Continuous Compliance
- What's Missing
- Making Sense of It All
- Summary