Certified Virtualization Security Expert, Part 5 of 6: Hardening the Server

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 5 of the series

Runtime: 04:18:57

Course description: This course is about the hardening techniques of the ESX server. It will cover best practices, isolation, and how templates can be used effectively. It will also cover VM segmentation, limiting data flow, the setinfo hazard, directory services control access and maintaining logs.

Course outline:

Hardening VMs
- Introduction
- Virtual Machines
- Disable Unnecessary or Superfluous Functions
- Templates
- Prevent VMs from Taking Over Resources
- Isolate VM Networks
- Example Network Architecture
- ARP Cache Poisoning
- Virtual Machine Segmentation
- Disable Copy and Paste Operations
- Limit Data Flow
- Limit Data Flow Continued
- SetInfo Hazard
- SetInfo Hazard Continued
- Non-Persistent Disks
- Persistent Disks
- Ensure Unauthorized Devices are Not Connected
- Avoid DoS caused by Virtual Disk Modification
- Summary

Verify File Permissions
- Introduction
- Verfiy File Permissions
- Demo: Graph
- Demo: Virtual System Center
- Demo: Assign Permissions
- Demo: Permissions Continued
- Demo: User Permissions
- Demo: XP-Attacker
- Configuring ESX and ESXi
- Summary

Configure Service Console and Firewall
- Introduction
- Configuring the Service Console in ESX
- Demo: Set up ESX Access
- Demo: Checking Access
- Demo: Users and Groups
- Demo: esxadmins
- Configure the Firewall for Maxium Security
- Demo: Firewall Services
- Demo: Reading Firewall Information
- Demo: Turn off Unnecessary Ports
- Limiting Running Services
- Summary

Service Console
- Introduction
- Limit What's Running in the Service Console
- Processes Running in SC
- The vSphere Client
- Use a Directory Service for Authentication
- Demo: Active Directory Integration
- Demo: Enable the Domain
- Demo: Authentication
- Demo: No Password Account
- Root
- Summary

Control Access
- Introduction
- Strictly Control Root Privileges
- Control Access to Privileged Capabilities
- Demo: Hardening ESX
- Demo: sshd-config
- Demo: Special User Permissions
- Demo: User vs. Group Permissions
- Demo: Successful Login
- Summary

Control Access Part 2
- Introduction
- Demo: Banner
- Demo: Other Commands
- Demo: Implementing sudo
- Demo: Changes for sudo
- Demo: sudoers File

(Continued on page 2)

Certified Virtualization Security Expert, Part 5 of 6: Hardening the Server

- Demo: Sudo Changes
- Demo: Run Commands as Another User
- Demo: Running Commands Continued
- Password Aging and Complexity
- Summary

Configure ESX
- Introduction
- ESX/Linux User Authentication
- Configuring ESX Authentication
- ESX Authentication Settings
- Reusing Passwords
- Configuring Password Complexity
- Managing ESX
- Maintain Proper Logging
- Best Practices for Logging
- ESX Log Files
- Establish and Maintain File System Integrity
- SNMP
- Protect Against the Root File System Filling Up
- Disable Automatic Mounting of USB Devices
- Isolation
- VLAN1
- Encryption Issues
- Do Not Use Promiscuous Mode on Network Interfaces
- Protect Against MAC Address Spoofing
- Protect Against Network Attacks
- Summary

Hardening an ESXi Server
- Introduction
- Differences: VMware ESX and ESXi
- Configure Host-Level Management
- Strictly Control Root Privileges
- Control Access to Privileged Capabilities
- Control Access to Privileged Capabilities Cont.
- Privilege Levels
- DCUI
- DCUI Continued
- Maintain Proper Logging
- Establish and Maintain ConfigFile Integrity
- Secure the SNMP Connection
- Ensure Secure Access to CIM
- Audit or Disable Technical Support Mode
- Summary