Certified Virtualization Security Expert, Part 2 of 6: Routing and Security

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 2 of the series

Runtime: 01:56:39

Course description: This course takes a look at how traffic routs and from the perspective of the hacker and how to manipulate or inspect and change it. It then moves into VM's and ESX hosts on both the same switches or port groups. Then SAN security with both fiber channel and iSCSI, and zoning. It will finish up with Security features of iSCSI, authentication and the steps in securing it.

Course outline:

The Virtualization Layer
- Introduction
- How Traffic Routes between VMs on ESX Hosts
- Different vSwitches, Same Port Group and VLAN
- Same vSwitch, Different Port Group and VLAN
- VMWare Security Design
- VMWare Infrastructure Architecture and Security
- The Virtualization Layer
- Virutalization Layer Continued
- More Virtualization Layer
- CPU Virtualization
- Normal Operation
- Buffer Overflow
- Summary

Page Sharing and Isolation
- Introduction
- CPU Virtualization
- Memory Virtualization
- Transparent Page Sharing
- VMware's Transparent Page Sharing
- Cloud Burst
- VM Isolation
- Protecting VMs
- Summary

Virtual Switches and Ports
- Introduction
- Service Console
- Risk Mitigation in the Service Console
- Virtual Networking Layer and Virtual Switches
- Virtual Switch VLANs and
- Demo: Tagging VLANs
- Benefits of VLANs
- Tagging VLANs
- Virtual Ports
- Virtualized Storage
- VMware VirtualCenter
- VirtualCenter Certificate
- VMWare VirtualCenter Continued
- Summary

Remote Data Store Security
- Introduction
- Zoning and Lun Masking
- Zoming and Lun Masking Continued
- Port Zoning
- Hard, Soft, and WWN Zoning
- Fibre Channel
- DH-CHAP
- ESP over Fibre Channel
- Fibre Channel Attacks: The Basics
- Steps in Securing Fibre Channel
- iSCSI vs. Fibre Channel
- ESX/ESXi and iSCSI SAN Environment and Addressing
- Hardware vs. Software Initiators
- Demo: Security Settings
- IPSec
- Securing iSCSI Devices
- Summary