Certified Virtualization Security Expert

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.

Runtime: 16:01:17

Course description: This series covers everything you need to know becoming a Certified Virtualization Security Expert. Students will learn about routing and the security design of VMware, Remote DataStore security, Penetration Testing 101, information gathering, scanning and enumeration, penetration testing and the tools of the trade, DMZ virtualization and common attack vectors, hardening your ESX server, hardening your ESXi server, hardening your vCenter server, and 3rd party mitigation tools.

Course outline:

Introduction to Networking
- Introduction
- How Virtual Ethernet Adapters Work
- How Virtual Switches Work
- VMSafe
- Current VMSafe Partners
- Virtual Switch vs. Physical Switch
- Cam Tables
- Spanning Tree Protocol
- Virtual Ports
- Uplink Ports and Port Groups
- Uplinks
- VIrtual Switch Correctness
- VLANs in VMWare Infrastructure
- Failover Configuration
- Virtual Machine Operation
- Summary

Virtual Network Security
- Introduction
- Forged Transmits
- Managing the Virtual Network
- Symmetric vs. Asymmetric Encryption
- Demo: Virtual Switch Security Settings
- Hashes
- Demo: Hashes
- Summary

Remote Access
- Introduction
- Digital Signatures
- Breaking SSL Traffic
- VMTraining's Physical Setup
- Demo: Connecting into DRAC Client
- Demo: DRAC Console
- Demo: PuTTy
- Demo: vSphere Client
- Demo: Virtual Center in vSphere Client
- Demo: ARP Injections
- Demo: ARP Cache Poisoning
- Introduction to Linux
- Summary

Linux
- Introduction
- File System Structure
- Kernel
- Processes
- Processes Continued
- Staring and Stopping Processes
- Interacting with Processes
- Storing Account and Group Information
- Password and Shadow File Formats
- Accounts and Groups
- Linux and UNIX Permissions
- Demo: Introduction to Linux
- Demo: Get IP Address
- Demo: Configuring and Navigating Linux
- Demo: Navigating Linux
- Set UID Programs, Logs, and Editing
- Summary

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

(Continued on page 2)

Certified Virtualization Security Expert

- 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

Exploits and Malware
- Introduction
- Benefits of a Penetration Test
- The Cost of Hacks
- Cost of a Hack: Example
- Current Issues: Malware
- Zombies
- Current Issues: Zombies
- Current Issues: Botnets
- Stolen Information
- Current Issues: Social Engineering and Exploits
- Chained Exploit Example
- Gozalez Indictment
- Summary

Penetration Testing
- Introduction
- The Evolving Threat
- Methodology for Pen Testing/Ethical Hacking
- Penetration Testing Methodologies
- Different Types of Penetration Tests
- Website Review
- Demo: Security Websites
- Demo: More Security Websites
- Management Errors
- VMware Concerns
- Summary

Footprinting
- Introduction
- Methods of Obtaining Information
- Footprinting
- Footprinting Tools
- Maltego GUI
- Demo: Maltego
- Demo: Maltego Transforms
- FireCAT
- Demo: FireCAT
- Summary

Port Scanning
- Introduction
- FireFox Fully Loaded
- Google Hacking
- Advanced Query Operators
- Google Continued
- Shodan
- Demo: Shodan
- Port Scanning
- Popular Port Scanning Tools
- ICMP Disabled
- TCP Connect Port Scan and NMAP
- Half-Open Scan, Firewalled Ports, and UDP Ports
- Demo:
- Demo: Port Scanning wiht NMAP
- Demo: Perform Scan
- Demo: Discovered Ports
- Demo: Reading Output
- Summary

Enumeration
- Introduction
- UDP Port Scan
- Enumeration
- Banner Grabbing
- DNS Enumeration
- Zone Transfers
- Backtrack DNS Enumeration
- Active Directory Enumeration
- LDAPMiner
- Null Session
- Syntax for a Null Session
- Enumeration with Cain and Abel
- NAT Dictionary Attack Tool
- THC-Hydra
- Injecting Abel Service
- Demo: Cain and Abel
- Demo: ARP Poisoning
- Demo: Certificates
- Demo: Modify Port Function
- Summary

Vulnerability Scanners
- Introduction
- BackTrack4
- Vulerability Scanners
- Nessus
- Nessus Report
- Saint
- Saint Sample Report
- OpenVAS
- OpenVAS Infrastructure and Client
- Demo: OpenVAS
- Demo: Connecting to the Server
- Demo: New Connections
- Demo: Perform a Scan
- Demo: Scan Continued
- Demo: Scan Report
- Summary

Password Cracking
- Introduction
- Windows Password Cracking
- SysKey and Cracking Techniques
- Rainbow Tables
- Disabling Auditing
- Clearing the Event Log
- NTFS Alternate Data Stream
- Stream Explorer
- Encrypted Tunnels
- Port Monitoring Software
- Rootkits
- Utilizing Tools
- Defense in Depth
- Meterpreter
- VASTO
- Summary

Pen Testing Tools
- Introduction
- VASTO Modules
- Fuzzers
- Saint
- Core Impact Overview
- Core Impact
- Tool Exploits from NVD
- Wireshark and TCP Stream Reassembling
- ARP Cache Poisoning
- ARP Cache Poisoning in Linux
- Cain and Abel
- Ettercap
- Summary

Virtualized DMZ
- Introduction
- Virtualized DMZ Networks
- Three Typical Virtualized DMZ Configurations
- Partially-Collapsed DMZ with Virtual Separation
- Fully-Collapsed DMZ
- Best Practices
- Network Labeling
- Layer 2 Security Options on Virtual Switches
- Enforce Separation of Duties
- ESX Management Capabilities
- Summary

Common Attack Vectors
- Introduction
- Common Attack Vectors
- How Fake Certificate Injection Works
- Generic TLS Renegotiation Prefix Injection
- Test Vulnerabilities
- Vulnerability Requirements
- Generic Example
- Patched Server with DIsabled Recognition
- Keeping Up to Speed
- SchmooCon 2010: Timeline
- SchmooCon 2010: Identification
- SchmooCon 2010: Server Log In
- SchmooCon 2010: Vulnerability
- SchmooCon 2010: Redirection Proxy
- SchmooCon 2010: Vulnerable Versions
- SchmooCon 2010: Gueststealer
- Summary

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
- Verify File Permissions
- Demo: Graph

Certified Virtualization Security Expert

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

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 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