

SECURING THE CLOUD WITH VMWARE VSPHERE

Improved Design! Improved Availability!
Improved Security!

STABLE VSPHERE ENVIRONMENT!



This course is going to provide a solid understanding of the various components that make up the vSphere environment. From the virtual CPU to the storage devices attached to your host and everything in and around that network, we will study and understand the interconnectivity and design of all those components. You will walk away with a solid understanding of how the adversary infiltrates the virtual environment and most importantly how you can secure that environment. We will study the virtual components that VMware has developed in the vSphere product line, including the vCpu, vMemory, vNetwork, vStorage, ESX/I host, virtual center, update manager and many other plug-ins, appliances and third-party mitigation tools.

We will also prepare you for the Certified Virtualization Security Expert certification. This is a unique and one-of-a-kind certification intended to prove you have the knowledge necessary to secure a virtual environment, cloud environment that is running on VMware vSphere. When you finish this course you will be able to assess the security posture of your vSphere 4.x architecture, and by extension, the services offered thru and by that architecture, and reducing the identified risks. The course will study the following VMware products: ESX 3.5, ESX 4.x, ESXi 4.x, vCenter 4.x



**CTREC
HILTON**
IT ACADEMY

The Cloud can be a scary place and with 80% of the cloud running on VMware's vSphere products you need to be ready to tackle the difficult aspect of keeping that environment secure. According to a recent survey from IBM, 77% of respondents believe the cloud made protecting privacy more difficult and 50% express worries about data breach or loss. The answer is here, if you are using VMware's vSphere to manage the cloud you will learn what you need to keep that cloud secure, whether it is private or public the detailed hardening recommendations will get you on track to developing the most secure environment possible.

British Airways Business: Life, May 2011

Call CTREC Hilton Today! 1-866-882-8732 or visit www.ctrechilton.com

SECURING THE CLOUD WITH VMWARE VSPHERE



CVSE1021 - A Five Day, Hands-on Bootcamp Covers VMware's VI 3 and vSphere 4 Products!

Don't let your company's network fall victim to fraud or theft!

1. Course Introduction and Methodology

2. Penetration Testing 101

- a. What is a Penetration Test?
- b. What does a Hack Cost You?
- c. Penetration Testing Methodologies
- d. Information Gathering (HOL)
- e. Scanning (HOL)
- f. Enumeration (HOL)
- g. Tools of the Trade (HOL)
- h. Website Review – How to stay up to date!
- i. Hashing, Encryption and Certificates. (HOL)
- j. Different Types of Exploits! (HOL)
- k. Where do we start with vSphere?

3. Primer and Reaffirming our Knowledge

- a. What is Virtualization?
 - a.i. Hypervisor Types
- b. ESX vs ESXi
- c. vSphere 4.1 Product Features
- d. Management Interfaces (HOL)
 - d.i. DRAC/iLO
 - d.ii. Web Interface
 - d.iii. SSH via Putty
 - d.iv. vSphere Client, ESX/i and vCenter
 - d.v. vMA, vCLI, Powershell, PowerGUI
 - d.vi. Communication Ports
- e. General Administrative Features (HOL)
 - e.i. vCenter Views
 - e.ii. Tasks and Alarms
 - e.iii. VM Administration
- f. Advanced Administrative Features (HOL)
 - f.i. DRS
 - f.ii. HA
 - f.iii. Fault Tolerance

4. Security Architecture, vCPU, vMemory

- a. Linux Kernel Architecture
 - a.i. Linux Files System
 - a.ii. ESX/i File Structure
- b. Log Files (HOL)
 - b.i. ESX/i and vCenter
- c. Security Architecture
 - c.i. Virtual Machine Monitor
- d. Security Roles and Permissions (HOL)
- e. VMsafe – Security at its finest
- f. vCPU (HOL)
 - f.i. Buffer Overflow Protection
 - f.ii. vCPU Availability
- g. vMemory
 - g.i. Transparent Page File Sharing
 - g.ii. Balloon Driver
 - g.iii. Swap File
 - g.iv. Compression
 - g.v. Hyperspacing

5. Routing and the vNetwork

- a. Networking Components
 - a.i. vSwitch
 - a.ii. vNIC
 - a.iii. Port Groups
 - a.iv. Uplinks
- b. Physical Switch Configuration (HOL)
- c. NIC Teaming (HOL)
 - c.i. Load Balancing
 - c.ii. Failover
 - c.iii. Security Features
- d. VLAN's (HOL)
- e. vDS
 - e.i. Private VLAN
- f. Network I/O Control
- g. Cisco Nexus 1000v
- h. Network Routing (HOL)

6. vStorage – Architecture and Security Implementations

- a. Virtualized Storage (HOL)
- b. Pluggable Storage Architecture
- c. Storage Control
- d. vSphere API for Array Integration
- e. Fiber Channel
 - e.i. LUN Masking
 - e.ii. SAN Zoning
 - e.iii. Fiber Channel Attacks
 - e.iv. Securing Fiber Channel
- f. iSCSI (HOL)
 - f.i. Software vs Hardware Initiators
 - f.ii. iSCSI Security Features
 - f.ii.1. CHAP
 - f.ii.2. IPSec
 - f.iii. Securing iSCSI

7. Hardening the Virtual Machines

- a. Harden the Server
- b. Unnecessary Functions
- c. Using Templates (HOL)
- d. VM Isolation (HOL)
- e. VM Advanced Settings (HOL)
- f. SetInfo Hazard
- g. VMCI (HOL)
- h. Isolation Tools (HOL)
- i. VMsafe Settings

**“This was some of
the best training I've
ever had.”**

- William L.

Call CTREC Hilton Today! 1-866-882-8732 or visit www.ctrechilton.com

SECURING THE CLOUD WITH VMWARE VSPHERE

8. Hardening the Host

- a. Service Console Security (HOL)
 - a.i. Password Integrity
 - a.ii. sudo
 - a.iii. Wheel Group
- b. File System Integrity
- c. Encrypted Communication
- d. DCUI – Direct Console User Interface (HOL)
- e. CIM – Common Information Model (HOL)
- f. Tech Support Mode (HOL)
- g. Proxy.xml
- h. ESXi Lockdown Mode

9. Hardening Virtual Center

- a. Limiting Administrative Access (HOL)
- b. Limiting Network Connectivity
- c. Server Certificate Replacement (HOL)
- d. Controlling Log Files (HOL)
- e. Custom Rules
- f. Update Manager
- g. VMware Converter
- h. Managing the vCenter Clients (HOL)
- i. vShield (HOL)

10. Virtualizing your DMZ

- a. DMZ Virtualization with the VMware Infrastructure
 - a.i. Virtualized DMZ Networks
- b. Three Typical Virtualized DMZ Configurations
 - b.i. Partially Collapsed DMZ with Separate Physical Trust Zones
 - b.ii. Partially Collapsed DMZ with Virtual Separation of Trust Zones
 - b.iii. Fully Collapsed
- c. Best Practices for Achieving a Secure Virtualized DMZ Deployment (HOL)
 - c.i. Harden and Isolate the Service Console
 - c.ii. Clearly Label Networks for each Zone
 - c.iii. Set Layer 2 Security Options on Virtual Switches
 - c.iv. Separation of Duties
 - c.v. Use ESX Resource Management Capabilities
 - c.vi. Regularly Audit Virtualized DMZ Configuration
- d. Common Attack Vectors (HOL)
 - d.i. SSLv3/TLS Renegotiation
 - d.ii. Web Access Vulnerabilities

11. 3rd Party Mitigation Tools

- a. Altor Networks
- b. Catbird's vCompliance (HOL)
- c. HyTrust
- d. Reflex Systems VMC
- e. CheckPoint Virtual Appliances
- f. Trend Micro (HOL)
- g. TripWire Configuration Management

12. Putting it all Together

- a. Looking back at the key security issues for all topics covered
- b. Design thoughts
- c. Final Hands On Lab – Can you secure your environment?

“These guys are like the Darth Vaders of the network world. I'm glad they are on our side since this was a security course. Our instructor was amazing and by far the best guy we've seen here. This guy is world class.”

- Jim B., CIO

“After taking VMware's® Install and Configure and the DSA class, I thought I knew how to secure our virtual environment. I realized after this class how vulnerable our infrastructure is.”

- Alex W, Sr. Network Administrator



This course prepares the student for the Certified Virtualization Security Expert (CVSE) Exam and Certification.

This industry-recognized certification will show that you are an expert at securing your network.

Call CTREC Hilton Today! 1-866-882-8732 or visit www.ctrechilton.com