Securing The Cloud with VMWARE vSphere ONLINE TRAINING

Code: ACBE–GEN-VMSECURE_ONLINE

Days: 5

Course Description:

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

Outline:

1. Course Introduction and Methodology

2. Penetration Testing 101
   - What is a Penetration Test?
   - What does a Hack Cost You?
   - Penetration Testing Methodologies
   - Information Gathering (HOL)
   - Scanning (HOL)
   - Enumeration (HOL)
   - Tools of the Trade (HOL)
   - Website Review – How to stay up to date!
   - Hashing, Encryption and Certi_cates.
   - (HOL)
   - Di_erent Types of Exploits! (HOL)
   - Where do we start with vSphere?

3. Primer and Rea_rming our Knowledge
   - What is Virtualization?
     Hypervisor Types
   - ESX vs ESXi
   - vSphere 4.1 Product Features

- Management Interfaces (HOL)
    - DRAC/iLO
    - Web Interface
    - SSH via Putty
    - vSphere Client, ESX/i and vCenter
    - vMA, vCLI, Powershell, PowerGUI
    - Communication Ports
- General Administrative Features (HOL)
    - vCenter Views
    - Tasks and Alarms
    - VM Administration
- Advanced Administrative Features (HOL)
    - DRS
    - HA
    - Fault Tolerance

4. Security Architecture, vCPU, vMemory
    - Linux Kernel Architecture
        - Linux Files System
        - ESX/i File Structure
    - Log Files (HOL)
        - ESX/i and vCenter
    - Security Architecture
        - Virtual Machine Monitor
    - Security Roles and Permissions (HOL)
    - VMsafe – Security at its _nest
    - vCPU (HOL)
        - Bu_er Over_ow Protection
        - vCPU Availability
    - vMemory
        - Transparent Page File Sharing
        - Balloon Driver
        - Swap File
        - Compression
        - Hyperspacing

5. Routing and the vNetwork
    - Networking Components
        - vSwitch
        - vNIC
        - Port Groups
        - Uplinks
    - Physical Switch Con_guration (HOL)
    - NIC Teaming (HOL)
        - Load Balancing
        - Failover
        - Security Features
    - VLAN’s (HOL)
    - vDS
        - Private VLAN
    - Network I/O Control
    - Cisco Nexus 1000v
    - Network Routing (HOL)

6. vStorage – Architecture and Security
   - Implementations
   - Virtualized Storage (HOL)
   - Pluggable Storage Architecture
   - Storage Control
   - vSphere API for Array Integration
   - Fiber Channel
     - LUN Masking
     - SAN Zoning
     - Fiber Channel Attacks
     - Securing Fiber Channel
   - iSCSI (HOL)
     - Software vs Hardware Initiators
     - iSCSI Security Features
     - 1. CHAP
     - IPSec
     - Securing iSCSI

7. Hardening the Virtual Machines
   - Harden the Server
   - Unnecessary Functions
   - Using Templates (HOL)
   - VM Isolation (HOL)
   - VM Advanced Settings (HOL)
   - SetInfo Hazard
   - VMCI (HOL)
   - Isolation Tools (HOL)
   - VMsafe Settings

8. Hardening the Host
   - Service Console Security (HOL)
     - Password Integrity
     - sudo
     - Wheel Group
   - File System Integrity
   - Encrypted Communication
   - DCUI – Direct Console User Interface
   - (HOL)
   - CIM – Common Information Model
   - (HOL)
   - Tech Support Mode (HOL)
   - Proxy.xml
   - ESXi Lockdown Mode

9. Hardening Virtual Center
   - Limiting Administrative Access (HOL)
   - Limiting Network Connectivity
   - Server Certi_cate Replacement (HOL)
   - Controlling Log Files (HOL)
   - Custom Rules
   - Update Manager
   - VMware Converter
   - Managing the vCenter Clients (HOL)

- vShield (HOL)

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

11. Party Mitigation Tools
    - Altor Networks
    - Catbird's vCompliance (HOL)
    - HyTrust
    - Re_ex Systems VMC
    - CheckPoint Virtual Appliances
    - Trend Micro (HOL)
    - TripWire Con_guration Management

12. Putting it all Together
    - Looking back at the key security issues for all topics covered
    - Design thoughts
    - Final Hands On Lab – Can you secure
    - your environment?

Follow a Westcon Training Online *:*
Joining a Westcon online training is easy – from either a Mac, PC, iPad®, iPhone® or Android device.
Once subscribed to the training, attendees simply click the meeting link Westcon Academy provides by email.
While joining, attendees choose whether to conference in via phone or their computers' microphone and speakers.

For the practical lab exercises, we work together by sharing keyboard and mouse control between instructor and student.
For the presentation, the Westcon instructors Interact on the screen using the pen, highlighter, arrow and spotlight tools.