VMWARE vSphere 4.x – Latest Threats, Hardening and Design

Code: ACBE–GEN-VMHARDENING

Days: 3

Course Description:

This course is going to provide you the details needed to harden your vSphere environment, whether it is the host, vCenter or Virtual Machine. We will also spend time on design of the network and your DMZ. This class finishes up looking at many really great 3rd party mitigation tools, you will walk away with hands on knowledge of how these tools can help you with security within your vSphere environment.

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 or 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.

Outline:

1. Course Introduction and Methodology
2. Design for Security
    a. Key Items to Consider
        i. Can you have a secure virtual environment?
        ii. Holistic View
        iii. Monitoring
            1. Port Level or Application Level?
        iv. Policy Enforcement
        v. Secure Privileged Access
        vi. Secure Multi-tenancy
    b. The Many Layers
        i. Physical Layer
        ii. Virtualized Layer
        iii. Cloud Layer
    c. DMZ Designs
        i. Five Dimensional Decision
            1. Security, Virtualization, Network, Management and Storage
    d. Sample Designs
        i. Can we improve?
3. 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)
4. vSphere Technology and Threats
    a. Hypervisor Threats
    b. vCenter Threats
    c. Physical Layer Threats
    d. Web Based Threats
    e. Network Threats
5. 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
6. Hardening the Host
    a. Service Console Security (HOL)
        i. Password Integrity
        ii. sudo
        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
7. 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)
8. Putting it all Together
    a. Looking back at the key security issues for all topics covered!
    b. Final Hands On Lab – Can you secure your environment?