



Course VMT-AVS4BCMP-ILT

Advanced VMware® Security

Five days, Instructor-Led

INTRODUCTION

A critical and often overlooked aspect of migrating to a virtualized environment is security and setting up security properly. Like physical machines, virtualization technologies are not secure “out of the box” and VMware is no exception. The Advanced Virtualization Security course focuses on “where the vulnerabilities lie” and how to reduce the attack surfaces in the virtualized environment. It goes beyond the typical security protocols administrators use to secure their environments and delves much deeper into the actual working (and short comings) of the VMware environment. Students will take a 360 degree look at the potential threats, how to defend and defeat them, and establish a solid foundation to build secure virtual data centers from the ground up.

- Learn the actual internal workings of VMware, and compare them to physical and virtual devices.
- Discover how to securely set up port groups and VLANs.
- Understand the aspect of securing failover configurations
- Distinguish between Denial of Service Failovers that wide open failovers and closed failovers.
- Dive deep into the different layers of security and explore features to include how traffic routes between VM’s and different hosts, common denominators of Physical and Virtual Environments, and how to make the virtual environment the most secure.
- Walk away knowing how to secure a VMware environment in a DMZ and how to protect yourself from the common vulnerabilities of VMware attack surfaces from the eyes of an attacker.
- Receive in depth information on how to harden you ESX environment, and comprehensively understand all aspects of how to do that.
- Demonstrate their proficiency in class working on a state-of-the-art data center and performing hands-on labs to reinforce the learning objectives.
- Course developed and taught by a Licensed Penetration Tester who has a long history of vulnerability audits with US National Security Teams and audits of many foreign governments.
- Designed and taught from the perspective of how an attacker would get into your Virtual Environment from an attacker who has done JUST THAT!

AUDIENCE PROFILE

System Administrators and Security Administrators using virtualization software.

PREREQUISITES

Virtual Infrastructure 3.5 Ultimate Bootcamp or equivalent. In lieu of hands-on classroom training, an in-depth knowledge of VMware’s ESX virtualization environment is required.

COURSE OUTLINE

MODULE 1: PRIMER AND REAFFIRMING OUR KNOWLEDGE

Chapter Overview

- ESX Networking Components

Five days, Instructor-Led

- Virtual Ethernet Adapters and How They Work.
- Virtual Switches and How They Work
- Virtual Switches vis-a-vis Physical Switch
- Why The Spanning Tree Protocol is Superfluous
- What are Virtual Ports and Why Should we be Concerned?
- VMWare so-called "Uplink Ports" and their interaction with the Physical equivalent
- Concept of Port Groups - They are out of this (physical) world!
- Uplinks
- Virtual Switch Correctness
- VLANs in VMware Infrastructure
- NIC Teaming
- Load Balancing
- Failover Configurations
- Layer 2 Security Features
- Managing the Virtual Network with "VirtualCenter"
- File System Structure
- Kernel
- Processes
- When do the processes start?
- Starting and Stopping Processes
- Interacting with Processes
- Account and Groups
- Password and Shadow File Formats
- Linux and Unix Permissions
- Set UID Programs
- Trust Relationships
- Logs and Auditing

MODULE 2 - PENETRATION TESTING 101

Chapter Overview

- What is a Penetration Test?
- Benefits of a Penetration test
- What is the Cost of a Hack?
- Example
- Current Issues
- Malware/Virus
- Active Zombies
- Hash Collisions
- SQL Injection
- Identity Theft
- Social Engineering, EXploits and Chained Exploits
- Chained Exploit Example
- The Evolving Threat

Five days, Instructor-Led

- Pen Testing Methodology
- Types of Tests
- Website Review
- Common Management Errors
- It's not Just about the Tools!

MODULE 3 - ROUTING AND THE SECURITY DESIGN OF VMWARE

Chapter Overview

- Security of Routing Data
- How traffic is routed Between Virtual Machines on ESX host
- Different vSwitches, same port group and VLAN
- Same vSwitch, different port group and VLAN
- Same vSwitch, same port group and VLAN
- Security Design of the VMware Infrastructure 3 Architecture
- VMware Infrastructure Architecture and Security Features
- Virtualization Layer
- CPU Virtualization
- Buffer overflow
- Memory Virtualization
- Virtual Machines
- Service Console
- Virtual Networking Layer
- Virtual Switches
- Virtual Switch LANs
- Virtual Ports
- Virtual Network Adapters
- Virtual Switch Isolation
- Virtual Switch Correctness
- Virtualized Storage
- SAN Security
- VMware Virtual Center

MODULE 4 – INFORMATION GATHERING, SCANNING AND ENUMERATION

Chapter Overview

- What information does the hacker gather?
- Methods of Obtaining Information
- Footprinting Defined
- Maltego
- Firefox Add
- Google Hacking
- Introduction to Port Scanning
- Port Scanning Tools

Five days, Instructor-Led

- NMAP
- TCP Connect Port Scan
- Half-Open Scan
- Firewalled Ports
- Service Version Detection
- Additional NMAP Scans
- UDP Scans
- Enumeration Overview
- Web Server Banner Grabbing
- Telnet
- SuperScan4
- SMTP Server Banner
- DNS Enumeration
- Zone Transfers
- Backtrack Tools
- Active Directory Enumeration
- LDAP miner
- Null Sessions
- Enumeration with Cain and Abel
- NAT Dictionary Attack Tool
- THC-Hydra
- Cool Stuff with Cain

CHAPTER 5 – DMZ VIRTUALIZATION

Chapter Overview

- Virtualized DMZ Networks
- Typical Virtualized DMZ
- Three Typical Virtualized DMZ Configurations
- Partially Collapsed DMZ with Separate Physical Trust
- Zones
- Partially Collapsed DMZ with Virtual Separation of Trust
- Zones
- Fully Collapsed DMZ
- Best Practices for Achieving a Secure Virtualized DMZ Deployment
- Harden and Isolate the Service Console
- Clearly Label Networks for each Zone within the DMZ
- Set Layer 2 Security Options on Virtual Switches
- Enforce Separation of Duties
- Use ESX Resource Management Capabilities
- Regularly Audit Virtualized DMZ Configuration

CHAPTER 6 – REMOTE DATASTORE SECURITY

Chapter Overview

- Mask and Zone SAN Resources
- LUN Masking
- SAN Zoning
- Port Zoning
- Hard and Soft Zoning
- WWN Zoning
- Classes of Attacks against SANs
- Fiber Channel
- Fiber Channel – Security Protocol
- ESP over Fiber Channel
- DH-CHAP
- Switch Link
- Attacking Fiber Channel
- Securing iSCSI, iFCP and FCIP over IP networks

CHAPTER 7 – PENETRATION TESTING AND THE TOOLS OF THE TRADE

Chapter Overview

- Vulnerabilities in Network Services
- Vulnerability Assessment Scanners
 - Nessus
 - Saint
- Windows Password Cracking
 - Syskey Encryption
 - Cracking Techniques
 - Cryptanalysis
- Disabling Auditing
 - Clearing the Event Log
- Alternate Data Streams
 - Stream Explorer
 - Encrypted Tunnels
 - Port Monitoring Software
 - Rootkits
 - Metasploit
 - Fuzzers
 - SaintExploit
 - Core Impact
 - Penetration Testing Tool Comparison
 - Wireshark
- ARP Cache Poisoning
- Cain and Abel

Five days, Instructor-Led

- Ettercap
- Breaking SSL Traffic
- Hash Algorithm
 - MD5 Hash Collisions

CHAPTER 8 – HARDENING YOUR ESX SERVER

Chapter Overview

- Hardening Your ESX Server
- ESX Best Practices
 - Virtual Machines
 - Secure Virtual Machines as You Would Secure Physical Machines
 - Disable Unnecessary or Superfluous Functions
 - Take Advantage of Templates
 - Prevent Virtual Machines from Taking Over Resources
 - Isolate Virtual Machine Networks
 - Arp Cache Poisoning
 - VM Segmentation
 - Minimize Use of the VI Console
 - Virtual Machine Files and Settings
 - Disable Copy and Paste Operations Between the Guest Operating System and Remote Console
 - Limit Data Flow from the Virtual Machine to the Datastore
 - SetInfo Hazard
 - Do Not Use Nonpersistent Disks
 - Ensure Unauthorized Devices are Not Connected
 - Prevent Unauthorized Removal or Connection of Devices
 - Avoid Denial of Service Caused by Virtual Disk Modification Operations
 - Specify the Guest Operating System Correctly
 - Verify Proper File Permissions for Virtual Machine Files
 - Configuring the Service Console in ESX 3.5
 - Configure the Firewall for Maximum Security
 - Limit the Software and Services Running in the Service Console
 - Use VI Client and VirtualCenter to Administer the Hosts Instead of Service Console
 - Use a Directory Service for Authentication
 - Strictly Control Root Privileges
 - Control Access to Privileged Capabilities
 - Establish a Password Policy for Local User Accounts
 - Do Not Manage the Service Console as if it were a Linux Host
 - Maintain Proper Logging
 - Establish and Maintain File System Integrity
 - Secure the SNMP Configuration
 - Protect against the Root File System Filling Up
 - Disable Automatic Mounting of USB Devices
- Best Practices ESXi

Five days, Instructor-Led

- Configuring Host-level Management in ESXi 3.5
- Strictly Control Root Privileges
- Control Access to Privileged Capabilities
- Maintain Proper Logging
- Establish and Maintain Configuration File Integrity
- Secure the SNMP Configuration
- Ensure Secure Access to CIM
- Audit or Disable Technical Support Mode
- Configuring the ESX/ESXi Host
- Isolate the Infrastructure-related Networks
- Configure Encryption for Communication between Clients and ESX/ESXi
 - Label Virtual Networks Clearly
 - Do Not Create a Default Port Group
 - Do Not Use Promiscuous Mode on Network Interfaces
 - Protect against MAC Address Spoofing
 - Secure the ESX/ESXi Host Console
 - Mask and Zone SAN Resources Appropriately
 - Secure iSCSI Devices through Authentication
 - VirtualCenter
 - Set Up the Windows Host for VirtualCenter with Proper Security
 - Limit Administrative Access
 - Limit Network Connectivity to VirtualCenter
 - Use Proper Security Measures when Configuring the Database for VirtualCenter
 - Enable Full and Secure Use of Certificate-based Encryption
- VirtualCenter Server Certificates Replacement
 - Pre-Installation
 - During Installation
 - Post-Installation
 - Use VirtualCenter Custom Roles
 - Document and Monitor Changes to the Configuration
 - VirtualCenter Add-on Components
 - VMware Update Manager
 - VMware Converter Enterprise
 - VMware Guided Consolidation
 - General Considerations
- Client Components
 - Restrict the use of Linux-based Clients
 - Verify the Integrity of VI Client
 - Monitor the Usage of VI Client Instances
 - Avoid the Use of Plain-Text Passwords
- Appendix:
 - The Basics of SAN Security, Part I
 - Increasing Security Concerns
 - Security Domains

Five days, Instructor-Led

- Administrator-to-Security Management Domain
- Host-to-Switch Domain
- Security Management-to-Fabric Domain
- Switch-to-Switch Domain
- Data Integrity and Security
 - So What Is Zoning?
 - Zoning Types
 - Configuring Zoning Components
 - LUN Masking
 - Persistent Binding
 - Security Technologies
 - Host-to-Fabric
 - Summary and Conclusions
- Security Management Part 2
- Fibre Channel Security Management
- Authentication and Authorization
- Configuration Management
- SAN Access
- SAN Security Benefits
- Host-Based and Switch Based Mapping
- Controller-based Mapping
- WWN Privileged Access
- Redundancy
- Management
- Summary and Conclusions
- Appendix 1 – Malware
- Distributing Malware
- Malware Capabilities
- Netcat
 - Netcat Switches
- Executable Wrappers
- Avoiding Detection
- BPMTK
- Appendix 2 – SQL Injection
- What is SQL Injection?
- Why SQL Injection?
- Attacking Database Servers
 - SQL Ping2
 - osql.exe