

# Advanced VMware Security

## Course Overview

This course is far more advanced than any typical security course. Students will learn about the security protocols that administrators utilize to secure their environment and dive head first into the actual workings of the VMware environment. Students will learn about various threats and how to prevent and secure the VMware environment from them. It is recommended that students have an in-depth knowledge of VMware's ESX/ESXI virtualization environment.

## Course Outline

<b><u>Course Introduction</u></b>	4m
Course Introduction	
<b><u>Chapter 01 - Primer and Reaffirming Our Knowledge</u></b>	2h 38m
Primer and Reaffirming Our Knowledge	
ESX Networking Components	
How Virtual Ethernet Adapters Work	
How Virtual Switches Work	
VMsafe Overview	
Current VMsafe Partners	
Virtual Switch vs. Physical Switch	
Spanning Tree Protocol Not Needed	
Virtual Ports	
Uplink Ports	
Port Groups	
Uplinks	
Virtual Switch Correctness	
VLANs in VMWare Infrastructure	
NIC Teaming	
Load Balancing	
Failover Configurations	
Normal Operation	
Connection Fails	
Signaling Process - Beaconing	
Data Rerouted	
Layer 2 Security Features	
Forged Transmits	
Managing the Virtual Network	
Symmetric vs. Asymmetric Encryption	
Demo - Security in vSwitches	
Hashes	
Demo - Hashes	
Digital Signatures	
Breaking SSL Traffic	
Demo - Lab Environment	
Demo - ARP Cache Poison	
File System Structure	

Kernel  
Processes  
Starting and Stopping Processes  
Interacting with Processes  
Accounts and Groups  
Password & Shadow File Formats  
Accounts and Groups (cont.)  
Linux and UNIX Permissions  
Demo - Intro to Linux  
Set UID Programs  
Logs and Auditing  
Chapter 01 Review

## **Chapter 02 - Routing and the Security Design of VMware**

1h 21m

Routing and the Security Design of VMware  
Security of Routing Data  
How Traffic Routes Between VMs on ESX Hosts  
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 Architecture  
VMware Infrastructure Architecture and Security Features  
Virtualization Layer  
CPU Virtualization  
Memory Virtualization  
Cloud Burst  
Virtual Machines  
Service Console  
Virtual Networking Layer  
Virtual Switches  
Virtual Switch VLANs  
Demo - Using VLAN's  
Major Benefits of Using VLANs  
Standard VLAN Tagging  
Virtual Ports  
Virtual Network Adapters  
Virtualized Storage  
VMware VirtualCenter  
Chapter 02 Review

## **Chapter 03 - Remote DataStore Security**

39m

Remote DataStore Security  
ESX / ESXi and Fibre Channel SAN Environment and Addressing  
Mask and Zone SAN Resources Appropriately  
LUN Masking and Zoning  
Fiber Channel  
DH-CHAP  
Switch Link  
What is FC-SP (Fiber Channel - Security Protocol)?  
ESP Over Fiber Channel

Fiber Channel Attacks - The Basics  
Steps in Securing Fiber Channel  
iSCSI vs. Fiber Channel  
ESX / ESXi and iSCSI SAN Environment and Addressing  
Hardware vs. Software Initiators  
iSCSI Security Features  
Secure iSCSI Devices Through Authentication  
Demo - Storage Security Settings  
IPSec  
IPSec Implementation  
Steps in Securing iSCSI  
Chapter 03 Review

### **Chapter 04 - Penetration Testing 101**

1h 16m

Penetration Testing 101  
What is a Penetration Test  
Benefits of a Penetration Test  
What Does a Hack Cost You?  
Cost of a Hack - Example  
Current Issues  
Chained Exploit Example  
Demo - Gonzalez Indictment  
The Evolving Threat  
Methodology for Penetration Testing / Ethical Hacking  
Penetration Testing Methodologies  
Types of Tests  
Website Review  
Demo - Website Review  
Seven Management Errors  
Some VMware Issues  
Not Just About the Tools  
Chapter 04 Review

### **Chapter 05 - Information Gathering, Scanning and Enumeration**

1h 47m

Information Gathering, Scanning and Enumeration  
What is the Hacker Wanting to Know?  
Methods of Obtaining Information  
Footprinting  
Maltego  
Maltego GUI  
Demo - Maltego  
Firecat v1.6.2  
Demo - Firecat  
FireFox Fully Loaded  
Johnny.lhackstuff.com hackersforcharity.org  
Google and Query Operators  
Google  
Shodan - You Have to be Kidding Me!  
Demo - Shodan  
Introduction to Port Scanning

Popular Port Scanning Tools  
ICMP Disabled  
NMAP TCP Connect Scan  
TCP Connect Port Scan  
Nmap  
Half-open Scan  
Firewalled Ports  
NMAP and Your VMware Servers  
Additional NMAP Scans  
NMAP UDP Scans  
Demo - NMAP  
UDP Port Scan  
Enumeration Overview  
Banner Grabbing  
Banner Grabbing with Telnet  
SuperScan 4 Tool: Banner Grabbing  
DNS Enumeration  
Zone Transfers  
Backtrack DNS Enumeration  
Active Directory Enumeration  
LDAPMiner  
Null Sessions  
Syntax for a Null Session  
Viewing Shares  
Enumeration with Cain and Abel  
NAT Dictionary Attack Tool  
THC-Hydra  
Injecting Abel Service  
Demo - Cain  
Chapter 05 Review

## **Chapter 06 - Penetration Testing and the Tools of the Trade**

1h 29m

Penetration Testing and the Tools of the Trade  
Vulnerabilities in Network Services  
BackTrack4  
Vulnerability Scanners  
Nessus  
Nessus Report  
Saint  
SAINT - Sample Report  
OpenVAS  
OpenVAS Infrastructure  
OpenVAS Client  
Demo - OpenVAS  
Windows Password Cracking  
Syskey Encryption  
Cracking Techniques  
Rainbow Tables  
Disabling Auditing  
Clearing the Event log

NTFS Alternate Data Stream  
Stream Explorer  
Encrypted Tunnels  
Port Monitoring Software  
RootKit  
The Metasploit Project  
Defense in Depth  
Meterpreter  
VASTO  
VASTO Modules  
Fuzzers  
SaintExploit at a Glance  
Core Impact Overview  
Core Impact  
Total Exploits from NVD Included in the Penetration Testing Tool  
Wireshark  
TCP Stream Re-assembling  
ARP Cache Poisoning  
ARP Cache Poisoning (Linux)  
Cain and Abel  
Ettercap  
Chapter 06 Review

## **Chapter 07 - DMZ Virtualization and Common Attack Vectors**

52m

DMZ Virtualization and Common Attack Vectors  
DMZ Virtualization with VMware Infrastructure  
Virtualized DMZ Networks  
Three Typical Virtualized DMZ Configurations  
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  
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  
Common Attack Vectors  
How We Understand Fake Certificate Injection to Work  
Generic TLS Renegotiation Prefix Injection Vulnerability  
Testing for a Renegotiation Vulnerability  
Vulnerability Requirements  
Generic Example  
Patched Server with Disabled Renegotiation  
Demo - SSL Renegotiation Test  
Schmoo Con 2010: Virtualization Vulnerabilities Found!  
Schmoo Con 2010: Timeline  
Schmoo Con 2010: Identification

Schmoo Con 2010: Server Log In  
Schmoo Con 2010: Server on the Internet  
Schmoo Con 2010: Vulnerability  
Schmoo Con 2010: Redirection Proxy  
Schmoo Con 2010: Vulnerable Versions  
Schmoo Con 2010: Gueststealer  
Chapter 07 Review

## **Chapter 08 - Hardening Your ESX Server**

3h 2m

Hardening Your ESX Server  
Section 1 - 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  
Example Network Architecture  
Arp Cache Poisoning  
VM Segmentation  
Minimize Use of the vSphere Console  
Virtual Machine Files and Settings  
Disable Copy and Paste Operations  
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  
Demo - Security on your Virtual Machines  
Section 2 - Configuring the ESX/ESXi Host  
Configuring the Service Console in ESX  
Demo - Control VIC Access  
Demo - Service Console Administration  
Configure the Firewall for Maximum Security  
Demo - Firewall Configuration  
Limit the Software and Services Running in the Service Console  
Processes Running in SC  
Use vSphere Client and vCenter to Administer the Hosts Instead of Service Console  
Use a Directory Service for Authentication  
Demo - AD Integration  
Strictly Control Root Privileges  
Control Access to Privileged Capabilities  
Demo - SSH Access and SUDO  
Establish a Password Policy for Local User Accounts  
ESX/Linux User Authentication  
Configuring ESX Authentication  
ESX Authentication Settings  
Reusing Passwords

Configuring Password Complexity  
Do Not Manage the Service Console as a Linux Host  
Maintain Proper Logging  
ESX4 Log File Locations  
Maintain Proper Logging (cont.)  
ESX Log Files  
Establish and Maintain File System Integrity  
Secure the SNMP Configuration  
Protect Against the Root File System Filling Up  
Disable Automatic Mounting of USB Devices  
Isolate the Infrastructure-related Networks  
VLAN1  
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  
Chapter 08 Review

### **Chapter 09 - Hardening Your ESXi Server**

20m

Hardening Your ESXi Server  
Differences: VMware ESX vs. ESXi  
Differences: VMware ESX and ESXi  
Configuring Host-level Management in ESXi  
ESXi -Strictly Control Root Privileges  
Control Access to Privileged Capabilities ESXi  
DCUI  
Control Access to Privileged Capabilities ESXi (cont.)  
Maintain Proper Logging - ESXi  
Establish and Maintain Configuration File Integrity ESXi  
Ensure Secure Access to CIM  
Audit or Disable Technical Support Mode  
Chapter 09 Review

### **Chapter 10 - Hardening Your vCenter Server**

1h 28m

Hardening Your vCenter Server  
VirtualCenter  
Set Up the Windows Host for Virtual Center with Proper Security  
Limit Network Connectivity to Virtual Center  
Use Proper Security Measures When Configuring the Database for Virtual Center  
Enable Full and Secure Use of Certificate-based Encryption  
Default Certificates  
Replacing Server-Certificates  
vCenter Log Files and Rotation  
Collecting vCenter Log Files  
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  
Verify the Integrity of VI Client  
Monitor the Usage of VI Client Instances  
Avoid the Use of Plain-Text Passwords  
vShield Zones Overview  
vShield VM Wall Features  
vShield VM Flow Features  
Demo - vShield Zones  
Chapter 10 Review

**Chapter 11 - 3rd Party Mitigation Tools**

25m

3rd Party Mitigation Tools  
Virtualization: Greater Flexibility, Diminished Control  
Making Sense of the Virtualization Security Players  
1K View of Players  
In-depth Look - Authors Picks HyTrust Appliance  
HyTrust Appliance - Key Capabilities (cont.): Unified Access Control  
HyTrust Appliance - Key Capabilities (cont.): Policy Management  
HyTrust Appliance - Key Capabilities (cont.): Audit-quality Logging  
HyTrust Appliance - Key Capabilities (cont.): Hypervisor Hardening  
In-depth Look - Authors Picks Catbird  
Catbird - Policy-driven Security  
Catbird - Continuous Compliance  
What's Missing?  
Making Sense of It All  
Chapter 11 Review  
Course Closure

**Total Duration: 15hrs 22m**