

# Hacking Uncovered: VMware®

## 5 Day, Hands-On Bootcamp Why You Need This!

*"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*

## Prepare to Defend Yourself!

### Virtualization technologies are not secure "out of the box"

A critical and often overlooked aspect of migrating to a virtualized environment is setting up security properly. Virtualization technologies are not secure "out of the box" and VMware® is no exception. The Hacking Uncovered: VMware® course focuses on where the vulnerabilities lie and how to reduce the attack surfaces in a virtualized environment.

This course goes beyond the typical security protocols administrators use to secure their current environments and dives much deeper into the actual workings and shortcomings of the VMware® 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*

**This course was designed and developed from the perspective of how a hacker will get into your VMware® Environment** by a Licensed Penetration Tester and hacking Guru with a long history of vulnerability audits with: US Dept. of Homeland Security, US Government Agencies (NSA, DOD, DOT, TSA, SEC, CIA, and many others), nuclear power plants, law enforcement agencies, fortune 500 companies, universities, and many foreign governments.



- If you are using any remote storage (iSCSI, NFS, Fibre Channel), this class will show how an attacker can redirect, then copy or even change information before it arrives at the destination!
- Detect potential threats, how to defend and defeat them, and how to establish a solid foundation to build secure virtual data centers from the ground up.
- Any regular user inside your network can take full control of your ESX hosts if they know the right exploits.
- By taking control of your virtual environment a hacker could disable ALL your VMs at one time.
- Prevent theft of confidential records, proprietary files, or sensitive information and ensure compliance with HIPPA, SOX, or STIG standards and regulations.

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

*William L.*

**Contact Us Today  
For More Information!**

# Hacking Uncovered:

# VMware®

On-Site and  
Online Classes Available.  
Call for More Details!

Covers VMware's® VI 3 and  
vSphere 4 Products!

## CVSE1021 - A Five Day, Hands-on Bootcamp

### Chapter 1 – Primer and Reaffirming our Knowledge

- ESX Networking Components
- Virtual Ethernet Adapters and How They Work
- Virtual Switches and How They Work
- VLANs in VMWare Infrastructure
- NIC Teaming, Failover Configurations
- Layer 2 Security Features & File System Structure
- Managing the Virtual Network with "VirtualCenter"
- Kernel, Processes, Account and Groups
- Linux and UNIX Permissions
- Trust Relationships, Logs and Auditing

### Chapter 2 – Penetration Testing 101

- What is a Penetration Test and the benefits?
- What is the Cost of a Hack?
- Current Issues and the Evolving Threat
- Pen Testing Methodology, Types of Tests, Website Review
- Common Management Errors

### Chapter 3 – Routing and the Security Design of VMware

- Security of Routing Data
- How traffic is routed between Virtual Machines on ESX hosts
- Security Design of the VMware Infrastructure 3 Architecture
- VMware Infrastructure Architecture and Security Features

### Chapter 4 – Information Gathering, Scanning and Enumeration

- What information does the hacker gather?
- Methods of Obtaining Information
- Footprinting Defined, Google Hacking
- Introduction to Port Scanning & Tools
- Enumeration Overview

### Chapter 5 – DMZ Virtualization

- Virtualized DMZ Networks
- Three Typical Virtualized DMZ Configurations
- Best Practices for Achieving a Secure Virtualized DMZ Deployment

### Chapter 6 – Remote DataStore Security

- Mask and Zone SAN Resources
- Fiber Channel, Attacking Fiber Channel
- Securing iSCSI, iFCP and FCIP over IP networks

### Chapter 7 – Penetration Testing and the Tools of the Trade

- Vulnerabilities in Network Services & Assessment Scanners
- Windows Password Cracking, Disabling Auditing
- Alternate Data Streams, Encrypted Tunnels
- Port Monitoring Software, Rootkits, Metasploit, Fuzzers
- SaintExploit, Core Impact, Wireshark
- Penetration Testing Tool Comparison
- ARP Cache Poisoning, Hash Algorithm

### Chapter 8 – Hardening your ESX Server

- Hardening Your ESX Server, ESX, ESXi Best Practices
- Configuring the ESX/ESXi Host
- VirtualCenter, Client Components
- The Basics of SAN Security, Part I, Increasing Security Concerns
- Security Domains, Switch-to-Switch Domain
- Data Integrity and Security
- Security Management Part 2
- Fibre Channel Security Management
- Authentication and Authorization
- Configuration Management
- SAN Access, SAN Security Benefits
- Controller-based Mapping, WWN Privileged Access
- Redundancy, Management
- Distributing Malware, Malware Capabilities
- Netcat
- Executable Wrappers
- Avoiding Detection
- BPMTK
- What is SQL Injection?
- Why SQL Injection?
- Attacking Database Servers

**Contact Us Today  
for More Information!**



Show that you are an expert at  
securing your network by getting  
your Certified Virtualization  
Security Expert Certification.

**Don't let your company's  
network be a victim of  
fraud or theft!**