Certified Virtualization Security Expert (Advanced VMware Security)

Modality: On Demand

Duration: 18 Hours

About the course:

This course covers all that you have to know to turn into a Certified Virtualization Security Expert. Understudies will find out about routing and the security plan of Remote DataStore security, VMware, information gathering, Penetration Testing 101, penetration testing and the devices of the trade, scanning and enumeration, solidifying your ESX server, DMZ virtualization and basic assault vectors, hardening your ESXi server, hardening your vCenter server, and outsider mitigation tools.

Course Objective:

- Reaffirming and primer Our Knowledge
- Routing and the Design of Security of VMware
- Security of Remote DataStore
- Penetration Testing 101
- Information Scanning, Gathering, and Enumeration
- Penetration Testing and the Apparatuses of the Trade
- Common attack vectors and DMZ virtualization
- Hardening your ESXi server
- Hardening your ESX server
- Hardening your vCenter server
- 3rd Party Mitigation Tools

Prerequisites:

Basic Computer Experience

An interest in security

Course Outline:

- Course Introduction
- Chapter 01 - Primer and Reaffirming Our Knowledge
- Chapter 02 - Routing and the Security Design of VMware
- Chapter 03 - Remote DataStore Security
- Chapter 04 - Penetration Testing 101
- Chapter 05 - Information Gathering, Scanning and Enumeration
- Chapter 06 - Penetration Testing and the Tools of the Trade
- Chapter 07 - DMZ Virtualization and Common Attack Vectors
- Chapter 08 - Hardening Your ESX Server
- Chapter 09 - Hardening Your ESXi Server
- Chapter 10 - Hardening Your vCenter Server

- Chapter 11 - 3rd Party Mitigation Tools
- Course Summary