VMware vSphere Security Cookbook

Over 75 practical recipes to help you successfully secure your vSphere environment

Mike Greer

[PACKT] PUBLISHING enterprise professional expertise distilled

VMware vSphere Security Cookbook

Over 75 practical recipes to help you successfully secure your vSphere environment

Mike Greer

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

VMware vSphere Security Cookbook

First published: November 2014

Production reference: 1181114

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78217-034-1

www.packtpub.com

Credits

Author

Mike Greer

Reviewers

Mike Armstrong

Alexandre Borges

Mario Russo

Aravind Sivaraman

Acquisition Editor

Nikhil Karkal

Content Development Editor

Poonam Jain

Technical Editor

Faisal Siddiqui

Copy Editors

Relin Hedly

Dipti Kapadia

Project Coordinator

Mary Alex

Proofreaders

Simran Bhogal

Stephen Copestake

Maria Gould

Ameesha Green

Paul Hindle

Indexer

Rekha Nair

Graphics

Ronak Dhruv

Production Coordinators

Kyle Albuquerque

Conidon Miranda

Cover Work

Conidon Miranda

About the Author

Mike Greer is an accomplished IT Security Practitioner and Enterprise architect with a proven track record of successful, highly-complex projects over the past 20 years. Infusing security into the core infrastructure is one of his greatest concerns while enabling customers to achieve and preserve a secure business posture. As a consultant or instructor in his professional career, he continues to provide consultancy services on a number of subject matters that include strategy, virtualization, messaging, database, and infrastructure optimization. He is the founder of Evolution Security Solutions, a start-up company focusing on strategy, virtualization, and security. His industry certifications include CCSK, CISM, CISSP, ITIL, VCP, MCSE, and MCITP.

Evolution Security Solutions provides vCIO services in addition to strategy, security, cloud, and virtualization consulting.

I'd like to thank Gloria, Declan, and Colin for their support and understanding during the course of this project.

About the Reviewers

Mike Armstrong is a Sr. Site Reliability Engineer at VMware that supports OneCloud, VMware's private cloud environment. He is also a VMware vExpert and has been working with virtualization technologies since 2005. He has been in the IT industry for 30 years and has worked with various technologies. Mike's certifications include VCAP5-DCA, VCP4 & 5, MCITP, MCSE, and ITILv3.

Alexandre Borges is an Oracle ACE in Solaris and has been teaching courses on Oracle Solaris since 2001. He worked as an employee and a contracted instructor at Sun Microsystems, Inc. until 2010, teaching hundreds of courses on Oracle Solaris (such as Administration, Networking, DTrace, and ZFS), Oracle Solaris Performance Analysis, Oracle Solaris Security, Oracle Cluster Server, Oracle/Sun hardware, Java Enterprise System, MySQL Administration, MySQL Developer, MySQL Cluster, and MySQL tuning. He was awarded the title of Instructor of the Year twice for teaching Sun Microsystems courses.

Since 2009, he has been imparting training at Symantec Corporation (NetBackup, Symantec Cluster Server, Storage Foundation, and Backup Exec) and EC-Council (Certified Ethical Hacking (CEH)). In addition, he has been working as a freelance instructor for Oracle education partners since 2010.

In 2014, he became an instructor for Hitachi Data Systems (HDS) and Brocade. Currently, he also teaches courses on Reverse Engineering, Windows Debugging, Memory Forensic Analysis, Assembly, Digital Forensic Analysis, and Malware Analysis. Alexandre is also an (ISC)2 CISSP instructor and has been writing articles on the Oracle Technical Network (OTN) on a regular basis since 2013. He has also authored *Oracle Solaris 11 Advanced Administration Cookbook* by Packt Publishing.

Dedicated to my wife, Fernanda.

Mario Russo has worked as an IT architect, a senior technical VMware trainer, and in the presales department. He has also been working on VMware technology since 2004. In 2005, he worked for IBM on the first large project Consolidation for Telecom Italia on the Virtual VMware ESX 2.5.1 platform in Italy with the Physical to Virtual (P2V) tool. In 2007, he conducted a drafting course and training for BancoPosta, Italy, and project disaster and recovery (DR Open) for IBM and EMC. In 2008, he worked for the project Speed Up Consolidation BNP and the migration P2V on VI3 infrastructure at BNP Cardif Insurance.

He is a VMware Certified Instructor (VCI Level 2) and has a certificate in VCAP5-DCA. He is the owner of Business to Virtual, which specializes in offering virtualization solutions. He was also the technical reviewer of *Implementing VMware Horizon View 5.2*, *Implementing VMware vCenter Server*, *Troubleshooting vSphere Storage*, and *VMware Horizon View 5.3 Design Patterns and Best Practices.*

I would like to thank my wife, Lina, and my daughter, Gaia. They're my strength.

Aravind Sivaraman is a virtualization consultant with more than 8 years of experience in the IT industry. For the past 5 years, he has been focusing on virtualization solutions, especially VMware products. He holds different certifications from VMware, Microsoft, and Cisco and has been awarded with the VMware vExpert title for 2013 and 2014. He is a VMware Technology Network (VMTN) and Experts Exchange contributor. He maintains his personal blog at `http://aravindsivaraman.com/` and can be followed on Twitter `@ss_aravind`.

He has also technically reviewed *Troubleshooting vSphere Storage* and is the co-author of *VMware ESXi 5.1 Cookbook*, both by Packt Publishing.

I would like to thank and dedicate this book to my wife Madhu, my parents, and my family members, who are always there for me no matter what, for all their unconditional support and for teaching me to never give up.

---

www.PacktPub.com

Support files, eBooks, discount offers, and more

For support files and downloads related to your book, please visit `www.PacktPub.com`.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`https://www2.packtpub.com/books/subscription/packtlib`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can search, access, and read Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Free access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view 9 entirely free books. Simply use your login credentials for immediate access.

Instant updates on new Packt books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter or the *Packt Enterprise* Facebook page.

Table of Contents

Preface

This book features two topics that I have a keen interest in: security and virtualization. The virtualization space can be complex in its own right, and like other technological areas, adding sufficient security can prove to be quite labor intensive and often frustrating. As technology evolves, the idea of building an infrastructure or project in a secure manner from the beginning is still somewhat novel in its approach. While more security controls are available in products, I find that such controls and features continue to be underutilized or not implemented at all.

Consider the following: on receiving a plate of pasta at your local restaurant, you are generally asked, "Would you like cheese with that?" This simple scenario and the relationship between pasta and cheese is an apt metaphor for the way security is applied to the Information Technology (IT) infrastructure in many businesses today.

My core philosophy is to help those in need. By and large, given my profession, ensuring privacy and providing some form of data security seems the logical approach. I hope this cookbook that deals with security tasks specific to the VMware vSphere 5.5 product set will enable you to get a better understanding of the virtualization environment with step-by-step instructions.

This book covers implementing specific security features of the vSphere 5.5 virtualization platform in a step-by-step format. Each topic contains a high-level overview to give context to the cookbook recipes. This book is not intended to provide reference architectures or theories behind specific security topics implemented by vSphere.

What this book covers

Chapter 1, *Threat and Vulnerability Overview*, provides you with an overview of threats and vulnerabilities specific to the virtualization infrastructure. This chapter covers a high-level review of hypervisor, virtual machine, network, storage, and physical threats and vulnerabilities.

Chapter 2, *ESXi Host Security*, introduces you to hardening the ESXi host from both the console and the vSphere client. This chapter covers the host firewall and configuration of services.

Chapter 3, *Configuring Virtual Machine Security*, focuses on security of the guest virtual machine, covering both management of the virtual machine and configuration of the virtual machine. Configuration of guest operating system security and virtual machine isolation controls are covered in this chapter.

Chapter 4, *Configuring User Management*, guides you through the secure user administration of a virtualization environment using vCenter. Topics include configuring Active Directory integration, configuring Single Sign-On, assigning permissions, and administrative roles.

Chapter 5, *Configuring Network Security*, introduces you to security options in the configuration of virtual network switches and port groups.

Chapter 6, *Configuring Storage Security*, introduces you to the configuration of storage security from a vSphere perspective. The majority of this chapter covers iSCSI authentication between source and target systems. On completion of this chapter, you will be able to configure iSCSI authentication on a vSphere 5.5 host.

Chapter 7, *Configuring vShield Manager*, introduces you to the installation and configuration of vShield Manager, from downloading and installing the virtual appliance to configuration of user and group access—including SSL certificate configuration.

Chapter 8, *Configuring vShield App*, introduces you to vShield App configuration and setup on the ESXi host. The common application firewall settings are also covered.

Chapter 9, *Configuring vShield Edge*, introduces you to the setup and configuration of vShield Edge. In addition, adding and managing appliances and interfaces is covered, along with VPN, firewall, and gateway configurations.

Chapter 10, *Configuring vShield Endpoint*, introduces you to vShield Endpoint protection, installation, and configuration, and the importance of endpoint protection in securing the virtual infrastructure.

Chapter 11, *Configuring vShield Data Security*, introduces you to the configuration of vShield Data Security options and policies. Customizing data polices and reports are also covered.

Chapter 12, *Configuring vSphere Certificates*, guides you through the tasks involved in assigning issued X.509 certificates to vSphere component services. The SSL tool is used to assign certificates to vCenter, Update Manager, Web Client, Log Manager, Inventory Manager, and Single Sign-On services.

Chapter 13, *Configuring vShield VXLAN Virtual Wires*, introduces the prerequisites for implementing VXLAN virtual wires, configuring virtual wires and configuring firewall rules for virtual wires.

What you need for this book

You should have knowledge of basic VMware virtualization concepts such as datacenters, clusters, hosts, datastores, networks, and virtual machines.

A background of governance and security is helpful when evaluating how the security procedures covered in this book can provide additional controls in a virtualized environment.

You need to install VMware vSphere Client 5.5 or VMware vSphere Web Client. The web client is heavily referenced in the text and is the preferred VMware management tool going forward.

Who this book is for

This book is intended for the virtualization professional who is experienced with VMware vSphere setup and configuration, but who hasn't had the opportunity to investigate securing the environment properly.

This book covers all the major security options for vSphere 5.5 deployment in a modular fashion where only the recipe pertaining to the task is required. In other words, the book is not meant to be read from cover to cover, but rather used as a toolkit for specific tasks and scenarios in the virtualization infrastructure environment.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "The Windows Firewall can also be enabled and disabled by using the `netsh.exe` command via the command line."

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes, for example, appear in the text like this: "Click on **OK** to initiate the snapshot."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or disliked. Reader feedback is important for us because it will help us develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title in the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1
Threat and Vulnerability Overview

In this chapter, we will cover the following topics:

- Risk overview
- Hypervisor threats
- Hypervisor vulnerabilities
- Guest virtual machine threats
- Guest virtual machine vulnerabilities
- Network threats
- Network vulnerabilities
- Storage threats
- Storage vulnerabilities
- Physical threats
- Physical vulnerabilities
- Security Concepts

Introduction

Risk management, while outside the scope of this book, is a key foundation in the creation of a secure system. Proper risk assessment will not only identify what is being protected, the cost, and the criticality of those assets, but also identify the likelihood of the system or systems being breached. With the state of governance, compliance, and the growing requirement to notify customers of the security breach, it's more important than ever to create an auditable system based on well-defined security policies.

Not long ago, type I hypervisor systems, such as VMware ESX and Microsoft Hyper-V, were considered inferior for the task of running highly secure environments. The virtualization market has made substantial progress in the security space in a short span of time.

This chapter provides a brief overview and review of the risk and the associated components of risk pertaining to the virtualization environment. The ultimate goal is to determine the **acceptable risk**, which is the level of risk that a company is willing to take in order to conduct business.

Risk overview

The risk equation is composed of three components: threat, vulnerability, and cost.

Risk = Threat x Vulnerability x Cost

In brief, **Cost** is the damage measured in currency, as experienced in the loss of hardware or software. The cost also includes consulting hours or quantifiable staff time spent in remediating the damages caused. While cost is a key factor in the risk formula, it falls outside the scope of this book. Please refer to sites such as `http://www.isaca.org` for further information on risk and risk management.

The **Threat** component of the risk equation is measured in frequency or rate. For example, the threat of a user deleting a file will be greatly reduced if a user only has read permission on the file. By the same token, an organization with 10,000 computers has a much higher potential threat of a virus infection than an organization with 1,000 computers.

While there are threats associated specifically with the virtualization environment, a great deal of risk is caused by the misconfiguration of systems and policies. With the added complexity of virtualization comes additional layers that need to be addressed in order to make the environment secure. Without end-to-end security communication in the **Storage Area Network** (**SAN**), the storage switch, hypervisor host, and virtual machine are at risk. Likewise, communication between virtual networking components and physical networking components presents many opportunities for misconfiguration, thereby leading to the opportunity for a security breach.

The **Vulnerability** component, at a broad level, is measured as a percentage, which is similar to the case of a threat. The term vulnerability is most closely tied to a known deficiency or bug that presents a clear vector for compromise, and as such, caries a likelihood of 100 percent if the system is not patched to protect against said exploit.

Considering the risk equation, vulnerability is the component that has the most control. Vulnerabilities in the hypervisor platform will typically be patched by the vendor, in this case, VMware. By utilizing tools such as Update Manager, system administrators are able to keep the host systems patched in a timely and regular manner.

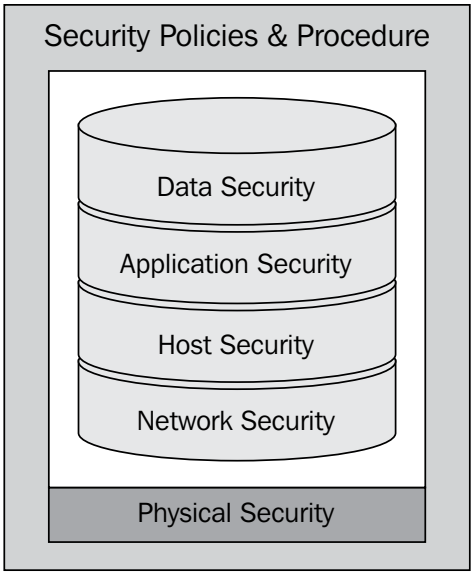
During the software patching cycle, it's important to do proper testing before applying a patch to a production system. This is even more critical for virtualized systems since a single virtualized host can hold a large number of virtual machines and thus will be affected adversely by a patch crippling a host.

Normal network vulnerabilities are still present in a virtualized environment. The mix between virtual networking and physical networking can present a different set of vulnerabilities based on the environment. It is important for the networking team and the server virtualization team to work together in order to ensure that both the physical and virtual networks are correctly configured and secure.

Understanding defense-in-depth

In addition to risk is the concept of defense-in-depth. The defense-in-depth model uses a layered approach, which not only increases the attacker's risk of detection but also reduces an attacker's chance of success. Defending the organization in depth means the application of a combination of people, processes, and technology to protect against threats at each layer. A good defense-in-depth architecture will build each layer of the security under the assumption that the other layer has been breached. If one layer is missing something, another layer might stop it and thereby stop the attacker.

In brief, the model consists of a series of interconnected components. The fundamental layer of policy and procedure affects every other layer. This layer includes both security policies and security procedures, as shown in the following figure:



The next layer is the **Physical Security** layer. This layer encompasses the remaining layers and includes secure facilities, mantraps, surveillance, and biometric identification devices.

The traditional host layer is now broken up into the virtual host and the virtual machine. The virtual host, also known as the hypervisor, includes signed drives, a secured kernel layer, and minimal management attack surfaces. The virtual machine layer includes the guest operating system, host hardening, patch management, and strong authentication. The guest operating system might also include a host-based firewall, intrusion detection system, and disk encryption system.

The data layer of the defense-in-depth model includes **Access Control Lists** (**ACLs**) and encryption.

The application layer includes hardening practices such as mechanisms to prevent SQL injection, as an example.

The network layer consists of an internal network and perimeter layers. These layers are traditionally separated by a security device such as a firewall. In a virtualized environment, both an internal network and a perimeter network can and often do reside within the same set of virtual host machines. In a complex networking scheme, it's even more critical to ensure that trusted network traffic and untrusted network traffic are properly separated in the virtual environment.

In a traditional physical environment, overall security is often more difficult to achieve, simply because there are more components and the risk of misconfiguration is higher. For example, securing a mission-critical application is more efficient when the majority of components are virtual and can be configured together by a team or an individual. In a physical environment, the same tasks could span numerous individuals around the globe. The virtual environment provides the administrator with an encapsulated landscape, which provides a better structure for tracking critical components.

The remainder of this chapter will highlight the threats and vulnerabilities to core services utilized in a virtualization environment, including storage, networks, hypervisors, virtual machines, and physical security.

Hypervisor threats

Hypervisor threats from attackers are growing in popularity. In fact, the vulnerability that allows a virtual machine to escape to the hypervisor has been documented in a certain number of 64-bit operating systems that have been virtualized. In addition, a limited number of Intel CPUs are vulnerable to a local privilege-escalation attack. The attack essentially allows the virtual machine access to a ring of the kernel on the hypervisor host. While this did affect several hypervisor platforms, it did not affect the VMware ESX platform.

VMware continues to innovate in the area of isolating components of the virtual landscape with various products, including **Network Virtualization Platform** (**NSX**). NSX is designed with the **Software Designed Data Center** (**SDDC**) approach in mind. Achieving true isolation in a multitenant cloud model is the goal. Increased isolation and controls will help to minimize hypervisor threats.

The following is an example of a guest VM affecting the host at the workstation level, not at the server level. The vulnerability listed in the National Vulnerability Database (`http://nvd.nist.gov`) is as follows:

National Cyber Awareness System

Vulnerability summary for CVE-2007-4496

Original release date: 09/21/2007

Last revised: 03/08/2011

Source: US-CERT/NIST

Overview

Unspecified vulnerability in EMC VMware workstation before 5.5.5 build 56455 and 6.x before 6.0.1 Build 55017, player before 1.0.5 Build 56455 and Player 2 before 2.0.1 Build 55017, ACE before 1.0.3 Build 54075 and ACE 2 before 2.0.1 Build 55017, and server before 1.0.4 Build 56528 allows authenticated users with administrative privileges on a guest operating system to corrupt memory and possibly, execute arbitrary code on the host operating system via unspecified vectors.

Impact

CVSS severity (Version 2.0)

CVSS v2 base score: 6.5 (medium) (AV:A/AC:H/Au:S/C:C/I:C/A:C) (legend)

Impact subscore: 10.0

Exploitability subscore: 2.5

CVSS Version 2 metrics:

Access vector: Local network exploitable

Access complexity: High

Authentication: Required to exploit

Impact type: This provides administrator access; allows complete confidentiality, integrity, and availability violation; allows unauthorized disclosure of information; and allows disruption of service

In this case, the user with administrative privileges in the guest operating system was able to execute the code against the host. Keep in mind that this was not just any host; this was a VMware workstation, which is a different type of hypervisor.

Hypervisor vulnerabilities

Hypervisor vulnerabilities affect the ability to provide and manage core elements, including CPI, I/O, disk, and memory, to virtual machines hosted on the hypervisor. As with any other software system, vulnerabilities are identified and vendors work toward patching them as quickly as possible before an exploit is found.

Several key vulnerabilities exist at this time, specific to VMware ESXi, including buffer overflow and directory traversal vulnerabilities. The following information is taken from the National Vulnerability Database (`http://nvd.nist.gov`):

National Cyber Awareness System

Vulnerability summary for CVE-2013-3658

Original release date: 09/10/2013

Last revised: 09/12/2013

Source: US-CERT/NIST

Overview

Directory traversal vulnerability in VMware ESXi 4.0 through 5.0 as well as ESX 4.0 and 4.1 allows remote attackers to delete arbitrary host OS files via unspecified vectors.

Impact

CVSS severity (Version 2.0):

CVSS v2 base score: 9.4 (high) (AV:N/AC:L/Au:N/C:N/I:C/A:C) (legend)

Impact subscore: 9.2

Exploitability subscore: 10.0

CVSS Version 2 metrics:

Access vector: Network exploitable

Access complexity: Low

Authentication: Not required to exploit

Impact type: This allows unauthorized modification and the disruption of service

Note that the access vector for both of these vulnerabilities is termed network exploitable, meaning that the vulnerability is remotely exploitable with only network access. The attacker does not need local access to exploit this type of vulnerability. The vulnerability listed in the National Vulnerability Database (`http://nvd.nist.gov`) is as follows:

National Cyber Awareness System

Vulnerability summary for CVE-2013-3657

Original release date: 09/10/2013

Last revised: 09/13/2013

Source: US-CERT/NIST

Overview

Buffer overflow in VMware ESXi 4.0 through 5.0 as well as ESX 4.0 and 4.1 allows remote attackers to execute the arbitrary code or cause a denial of service via unspecified vectors.

Impact

CVSS severity (Version 2.0):

CVSS v2 base score: 7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)

Impact subscore: 6.4

Exploitability subscore: 10.0

CVSS Version 2 metrics:

Access vector: Network exploitable

Access complexity: Low

Authentication: Not required to exploit

Impact type: This allows unauthorized disclosure of information, unauthorized modification, and the disruption of service

When attackers find a vulnerability such as this and see that no authentication is required to exploit and the access vector is network exploitable, they move this up the list as a potential low-risk, high-value target.

It should be noted that at the time of writing this book, these vulnerabilities were active; however, VMware releases patches on a regular basis and some or all of the example vulnerabilities might have already been remediated.