DAVE SHACKLEFORD

VIRTUALIZATION SECURITY

[PROTECTING VIRTUALIZED ENVIRONMENTS]

SYBEX® SERIOUS SKILLS.

Chapter 2

Securing Hypervisors

This chapter is about locking down virtualization platforms, specifically Type I hypervisors. Hardening the hypervisor should really be viewed as a standard practice, much as it should be for enterprise servers of any importance. There are an incredible number of configuration options for the major platforms (ESXi, Hyper-V, and XenServer). In this chapter, I'll cover the most fundamental, getting you to a sound security state that conforms to industry best practices. Where appropriate, I'll refer to outside sources for more in-depth information that's somewhat outside the scope of this book. Overall, these settings will help you secure your hypervisors to a reasonable level for most organizations.

In this chapter, you will learn about the following topics:

- Principles of hypervisor configuration and security
- Configuring VMware ESXi, Microsoft Hyper-V, and Citrix XenServer

Hypervisor Configuration and Security

A virtualization hypervisor platform, as described in Chapter 1, "Fundamentals of Virtualization Security," is software that emulates physical hardware to numerous guest operating systems and applications, allowing them to run concurrently on one physical machine. Every hypervisor platform has its own architectural nuances, but most hypervisors (also called virtual machine monitors, or VMMs) have a design somewhat similar to that shown in Figure 2.1.

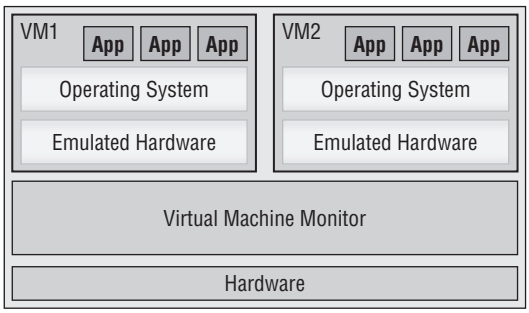

FIGURE 2.1 Hypervisor architecture

As you can see in the diagram, the VMM is a low-level component that functions in many ways as the OS of the virtual hosting platform. To ensure that the entire virtual environment is protected from attacks, bugs, or operational mishaps, it's paramount to keep it as up-to-date as possible and to configure some fundamental controls.

There are a number of distinct aspects of securing a hypervisor system of any sort, and the most common hypervisor platforms — VMware ESXi, Microsoft Hyper-V, and Citrix XenServer — all have multiple configuration controls that should be implemented and maintained by system administrators.

There are two fundamental principles to keep in mind when evaluating VMM security:

- The VMM is in many cases almost an operating system unto itself and has many characteristics similar to an OS.
- The VMM is interconnected with all hardware on the physical platform and acts as a conduit to any and all resources, such as storage, network, CPU, and memory, when virtual machines (VMs) ask for them.

Additionally, the VMM itself must be managed by administrators using a client or central console, a topic that we'll cover in more depth later in the book in Chapter 5, "Virtualization Management and Client Security".

The primary areas of concern for any VMM security configuration efforts are as follows:

Patching In most cases, especially with Type I hypervisors, the VMM is decoupled from other OS components, and therefore the VMM must be patched separately. Patching the hypervisor should be considered a core operational practice in IT and should align with current high-priority patching cycles. Additional detail on patching processes and best practices will be covered in Chapter 8, "Change and Configuration Management."

Establishing secure communications Many hypervisors use Secure Sockets Layer (SSL) or the newer Transport Layer Security (TLS) along with digital certificates to establish a means of securely communicating with remote clients and management platforms. In many cases, the digital certificates that are installed initially are not secure and should be configured or replaced prior to production operation. Another common control available for securing communication with the hypervisor or VMs is IPSec encryption.

Changing default settings Many hypervisor configuration settings are not secure by default, and some hypervisors ship with default content that can be removed. For example, the older VMware ESX hypervisor had a number of Linux Web service components, binaries, and even user accounts that weren't necessary. Changing settings and removing generic default content makes up a large percentage of VMM hardening activities.

Enabling operational security Common tools and protocols like Simple Network Management Protocol (SNMP) and Network Time Protocol (NTP) are used to provide consistency and accuracy in log files, monitoring, and numerous other operational activities. Configuring these services and protocols to function properly within the IT environment is an important step to ensuring long-term continuity for the virtual systems and applications.

Securing and monitoring critical configuration files Every hypervisor platform has a number of files that are critical for configuration and control of the VMM system and services. These files should be carefully protected with permissions and monitoring controls.

Securing users and groups Hypervisor platforms have a set of local users and groups that can be used to access the system and control services. In most cases, the default sets of users and groups are not as secure as they could be, with too much access and users that don't need to be active at all. Restricting these and controlling what they can access is another key step in protecting the system overall.

Locking down access to the hypervisor platform Most hypervisor platforms have a native console interface that can be accessed both locally and remotely. This needs to be carefully controlled to ensure that unauthorized access doesn't occur. Another major element of hypervisor access control is configuring the local firewall, if one exists.

ISBN: 978-1-1182-8812-2