CMSGu2018-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Virtualization and Hypervisor Security

CERT-MU

National Computer Board
Mauritius

December 2018

Issue No. 2

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide an overview on the security risks to virtualization and hypervisors and how to counteract these risks.

1.2 Audience

The target audience of this guideline includes all system administrators and technical personnel involved in the implementation of virtualised severs.

1.3 Document Structure

This document is organised into the following sections:

Section 1 details the structure of the document.
Section 2 gives a background on virtualization and explains the concept of virtual machines and hypervisors.
Section 3 presents the risks to virtualization and hypervisor security.
Section 4 highlights the countermeasures.
Section 5 concludes the document.
Section 6 provides the references used to draft the document.

2.0 Background

Traditionally, setting up a computing server only required a dedicated host with dedicated resources, such as central processing unit (CPU), memory, network and storage. Modern systems revolve around technology that allows us to create virtual machines to emulate what used to be physical, dedicated resources. This practice is known as virtualization and supports more scalable and dynamic environments.

A critical component of this technology is the hypervisor, the collection of software modules that enables this virtualization and thus enables multiple computing stacks, each made of an operating system (OS) and application programs meant to be run on a single physical host. Such a physical host is called a Virtualized Host and is also referred to as a Hypervisor Host. The individual computing stacks are encapsulated in an artifact called a Virtual Machine (VM).

To make a VM an independent executable entity, it should include resources, such as CPU and memory, allocated to it. The VMs are also called "Guests," and the OS running inside each of them is called "Guest OS." The resources associated with a VM are virtual resources, as opposed to physical resources associated with a physical host.

The hypervisor forms part of the virtualization layer in a virtualized host and plays many of the same roles that a conventional OS does on a non-virtualized host, or server. Similar to a conventional OS provides isolation between the various applications, or processes, running on a server, the hypervisor provides isolation between one or more VMs running on it

3.0 Virtualization and Hypervisor Security Risks

Nowadays, virtualization has become indispensable for organizations that are looking for better resource provisioning, easier IT management, less hardware, and lower costs. Global cloud computing and digital systems today would not exist without virtualization and hypervisors. Virtualization and hypervisors are basic tools for implementing digital systems that respond to varying demands without slow and expensive physical reconfiguration of hardware and rebuilding of software execution stacks and heavy investment in hardware that is only utilized during peak loads. However, virtualization is a complex and constantly evolving field, which comes with certain risks, that are explained below:

1.Resource simulations

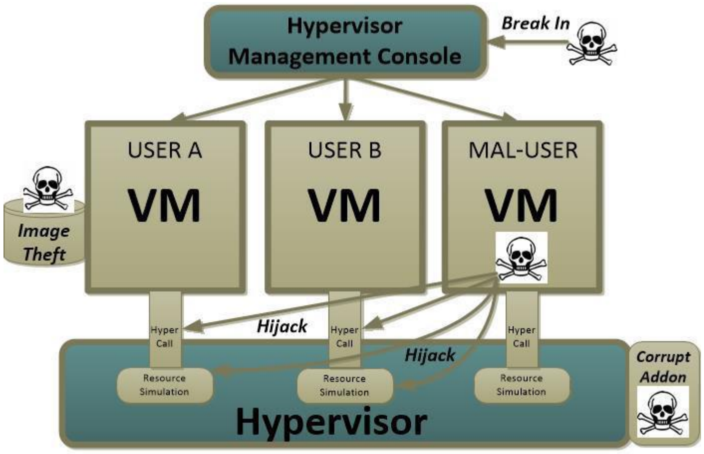
A hypervisor provides software simulations of basic computing resources that isolate VMs from one another. However, the isolation may have soft spots. For example, freed simulated memory for one VM might be the same physical memory the hypervisor allocates to another VM. If the hypervisor does not blank out the reallocated physical memory, the second VM has access to data from the first VM and a data breach ensues. All resource simulations are subject to dangerous implementation errors. Simulated CPU registers, storage buffers and network buffers, all present opportunities for coding mistakes that permit data or control breaches.

2. Hypervisor APIs

The APIs with which hypervisors communicate with VMs and the underlying physical resources are also vulnerable. For example, a call from a VM to the hypervisor that is not properly authenticated could masquerade as a call from a different VM, allowing access to unauthorized data or actions. The same applies to faulty drivers that interface between hypervisor and physical hardware.

3. VM management

VM management controls also present dangers. Depending on the hypervisor architecture, VM activity is regulated by a hypervisor control console or a specially empowered VM. These control facilities start, suspend or stop VMs. Most VMs can be ordered to write an image to a file that can be used to start a replica VM in the exact state when the image was made. If a hacker can gain unauthorized access to the control facility, they can stop, start and steal VMs at their own will, which is the virtual equivalent of an intruder in a data centre flipping switches and pulling off equipment.



VM Management Control Risk

4.Inter-process communication obscurity

A virtualized stack which contains several interacting processes, for example, an archetypal LAMP (Linux, Apache, MySQL, Perl/Python/PHP) stack, inter-process communication and file access is simulated within the hypervisor process. Consequently, these activities may be invisible to monitoring systems that are intended to detect anomalous malicious activity over the usual non-virtual interfaces.

5. Hypervisor add-ons

Most hypervisor systems include some facility for add-ons, optional features not available with the basic system. Rogue add-ons can maliciously open backdoors and other remote access portals, exfiltrate data, or other nefarious actions. Add-on mechanisms that are designed for third-party additions are often useful, but also more open to subversion.

6. VM images

VM users have to be cautious about securing VM images. One danger is unauthorized instantiation of a critical VM from a stolen image. Another subtler danger is that hackers may be able to analyse the image, which will contain a dump of memory contents. Ordinarily, developers assume that critical data like passwords held in memory is safe, but that is not the case when memory is dumped to an image on disk. Therefore, hackers may be able to extract information from VM images that developers think is safe.

4.0 Countermeasures

1. Create separate VM and management networks

Keep your VM network away from your management network to keep your virtualized environment secure. If your VMs are compromised by malware, it will not be able to affect your hypervisor.

2. Set access privileges

Set strict access restrictions on the software to prevent unauthorized users from accessing VM settings and viewing your most sensitive data.

3. Disable unnecessary services

Off-the-shelf operating systems will have many unnecessary services and apps that increase the attack surface of your VMs. If you are unsure about which ones to disable, consult with a virtualization specialist.

4. Pay attention to physical security

Breaking in to a server room is the easiest way to compromise hypervisors, so make sure your physical servers are behind locked doors and watched over by staff at all times.

5. Install latest network security tools

Due to network intrusions affecting hypervisor security, installing cutting-edge firewalls and intrusion prevention systems is highly recommended. These security tools monitor network traffic for abnormal behavior to protect you from the newest exploits.

6. Stay up to date with hypervisor updates

Hypervisors must be patched to defend against the latest threats. On the other hand, the security of your hypervisors can also be untrusted to a highly experiences and certified managed services provider.

5.0 Conclusion

Virtualization has become essential for businesses looking for better resource provisioning, easier IT management, reduced hardware, and minimized costs. However, virtualization is a continuously progressing area, which comes with risks and one such risk concerns hypervisor security. Therefore, business should stay ahead of the line and implement all security controls and adopt best practices with regards to securing their virtualized servers and hypervisors.

6.0 References

- www.nist.gov
- www.infoworld.com
- www.techadvisory.org
- www.techadvisory.org