Addressing the Security Challenges of Virtualization

“Vulnerabilities Exposed” Webcast Series Part 2

Paul Asadoorian, Jack Daniel, & Russell Butturini
“Vulnerabilities Exposed” Series

• Part 2 of a 4-part series
• Part 1: “Reducing Your Patch Cycle to Less Than 5 Days” is available
• Archives & slides: www.tenable.com/vulns-exposed

Strategies & solutions for today’s common security challenges
Today’s Webcast Roadmap

• Virtualization evolution – How we got here

• Virtualization challenges – The problems we face

• Solutions – Procedural & tactical
Virtualization Evolution
In the Beginning, There Was One

IBM System/370:
- supported virtual memory & virtual disks
- Ran multiple OSes at once
- Took up LOTS of space!

Source: ibm.com
Then There Were Many

LOTS of servers!

Ran one OS at a time

Cables, heat, noise, & power consumption

Source: futurepredictions.com
And Now…

Back to one big server!

Runs multiple OSes at once!

Virtual memory & virtual disks!

Difference: Takes up way less space, consumes less power, less wiring, & generates slightly less heat

Source: dell.com
Virtualization Problems

Having your own cloud is not all it’s cracked up to be...
Problem: “VM Sprawl”

- Easy to create & clone servers
- Disk space & memory costs falling
- Allows you to scratch itch for new servers

End result: Greatly increased attack surface!
Problem: “Whack-a-Mole”

- VMs easy to create then suspend
- What happens when someone else brings it online 3 months later?
- Is it up-to-date on patches and hardened?
- Creates several moving targets…

End result: Your attack surface is ever-changing!
Virtualization Abstracts the Physical Layer

• Successful virtualization layer attacks put attacker in your datacenter
• Guest OSes can be attacked to jump into host virtualization
  ▪ Even if your guest OS is fully patched & hardened

End result: Successful attacks against virtualization layer will obtain access to all hosted servers
Solution: Nessus

Nessus is your Ninja Umbrella!

Photo Credit: www.thinkgeek.com
Nessus Discovers VMware

You don’t know what you don’t know (until you run a Nessus scan)

Vulnerability Summary

- VMware ESX/GSX Server detection
- VMware Virtual Machine Detection

No credentials required
VMware Discovery: Workstations

Discovers VMware clients, such as VMware workstation & VMware Fusion
VMware Local Patch Checking

Supports VMware Fusion, Workstation, vSphere, & vCenter

Vulnerability Summary

- **high** VMSA-2012-0009 : ESXi and ESX patches address critical
  - Gain a shell remotely
  - 5
- **info** VMware ESX/GSX Server detection
  - Service detection
  - 5
- **info** VMware vSphere Detect
  - Service detection
  - 5
- **info** VMware vCenter Detect
  - Service detection
  - 1
Secure Access to VMware API

Policy Preferences

Preference Type: VMware SOAP API Settings

- VMware user name: root
- VMware password: 
- Ignore SSL Certificate: 

Update Cancel
VMware Configuration Auditing

• Compare your configuration
  o VMware's security guide
  o Tenable’s best practice guide

• Tune policies & compare against your production standards

• In-depth info examples:
  o VMware Tools installation status
  o OS info
  o Run state (active or suspended)
<table>
<thead>
<tr>
<th>Status</th>
<th>Component</th>
<th>Description</th>
<th>Product</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>failed</td>
<td>ESXi</td>
<td>config-ntp</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>failed</td>
<td>ESXi</td>
<td>enable-remote-syslog</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>failed</td>
<td>VM</td>
<td>disconnect-devices-usb</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>failed</td>
<td>VM</td>
<td>limit-console-connections-one</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>failed</td>
<td>vCenter</td>
<td>enable-nfc-ssl</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>warning</td>
<td>ESXi</td>
<td>set-password-complexity</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>passed</td>
<td>ESXi</td>
<td>disable-ssh</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>passed</td>
<td>ESXi</td>
<td>enable-ad-auth</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>passed</td>
<td>VM</td>
<td>disable-console-paste</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
<tr>
<td>passed</td>
<td>VM</td>
<td>use-vm-templates</td>
<td>VMware vCenter/vSphere</td>
<td>2</td>
</tr>
</tbody>
</table>
VMware Virtual Machine Info

### Description

The list of current VMs and their base OS should be reviewed.

### Audit File

Tenable_vCenter_vSphere_Best_Practices.audit

### Reference Information

**ID:** os-listing

### Affected Host List (2)

<table>
<thead>
<tr>
<th>Host</th>
<th>Severity</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.26.22.47</td>
<td>info</td>
<td></td>
</tr>
<tr>
<td>Test VM 5, poweredOff (toolsNotInstalled) - Microsoft Windows Server 2008 R2 (64-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test VM 10, poweredOn (toolsNotInstalled) - Other (32-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test VM 11, poweredOff (toolsNotInstalled) - Microsoft Windows Server 2008 R2 (64-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test VM Audit (172.26.23.123) - CentOS 4/5/6 (32-bit)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Amazon AMI Patch Checking

I get to say, “Secure your cloud!”

Make sure your Amazon AMI images are patched

Plugins: Amazon Linux Local Security Checks

- Amazon Linux AMI: puppet Arbitrary Code Execution (ALAS-2013-213)
- Amazon Linux AMI: php54 Buffer Overflow Vulnerability (ALAS-2013-212)
- Amazon Linux AMI: php Buffer Overflow Vulnerability (ALAS-2013-211)
- Amazon Linux AMI: curl Information Disclosure Vulnerability (ALAS-2013-210)
- Amazon Linux AMI: fail2ban Denial of Service (ALAS-2013-209)
Solutions: Passive Vulnerability Scanner

**Plugin Details**

**Plugin ID:** 4287  
**Family:** Generic  
**Plugin Name:** VMWare Server Detection

**Description**
The remote host is running VMWare server, an application that allows users to run multiple operating systems virtually. Further, this instance of VMWare is a server application that allows remote administrator access to the VMWare console. The display...

**Solution**
Only allow administrative VMWare connections from trusted hosts.

**Risk Factor:** Info

**Source File:** 4287.prm

**Plugin Details**

**Plugin ID:** 6548  
**Family:** Web Clients  
**Plugin Name:** VMWare VI Client Version Detection

**Description**
The remote host is running the VMWare VI client. The VI client is used to manage virtual machines across a network.

**Solution**
N/A

**Risk Factor:** Info

**Plugin Publication Date:** Aug 23, 2012

**Source File:** 6548.prm
Tenable Resources

Blog:
http://blog.tenable.com

Podcast:
http://www.tenable.com/podcast

Videos:
http://www.youtube.com/tenablesecurity

Discussion Forum:
https://discussions.nessus.org

Buy Nessus, Perimeter Service, PVS, Training & Bundles:
https://store.tenable.com

Become a Tenable Partner:
http://www.tenable.com/partners
Nessus, PVS, & SecurityCenter Info

For more info on Nessus:
http://www.tenable.com/products/nessus

For more info & to evaluate PVS:
http://www.tenable.com/products/passive-vulnerability-scanner

For more info or to evaluate SecurityCenter Continuous View:
http://www.tenable.com/products/securitycenter-continuous-view
Questions?
Thank You!

Contact us:

Paul Asadoorian – paul@nessus.org
Jack Daniel – jdaniel@tenable.com

“Vulnerabilities Exposed” webcast #3:

October 22 at 2 pm EDT
Handling Mobile Threats Before They Cause Loss & Disruption