tenable

Solution Brief

Tenable and VMware

Mitigating System Vulnerabilities and Security Misconfigurations Within Your VMware Virtual Environment

Key Challenges

With advanced cyberthreats clearly on the rise, and with roughly two-thirds of x86 server workloads virtualized, IT organizations simply can't afford to ignore the security posture of their VMware virtual systems. And they also can't afford to let unauthorized and/or insecure virtual machines (VMs) go unchecked in between periodic full-network vulnerability scans.

Since most vulnerability scanners aren't equipped to properly interrogate virtual platforms or detect new VMs in real time through passive vulnerability scanning, many VMware customers are unknowingly at risk. Without a full-featured vulnerability management solution specifically designed to monitor virtual environments and detect newly deployed VMs in real time, VMware customers face numerous challenges:

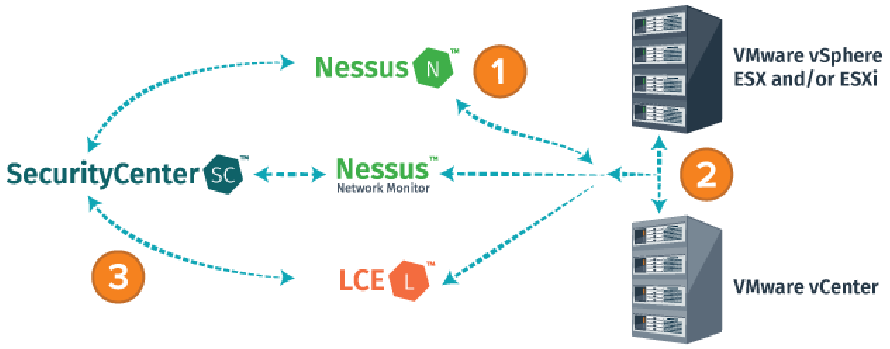
- Inability to detect VMware-specific vulnerabilities and security misconfigurations
- Inability to audit VMware patches
- Inability to demonstrate regulatory compliance of virtual systems
- Inability to mitigate "VM sprawl"

Solution Overview

Tenable™ is a proud VMware Technology Alliance Partner. Its award-winning Tenable Nessus® and Tenable SecurityCenter® vulnerability management offerings are leveraged by thousands of VMware customers to identify over 140 VMware-specific system vulnerabilities and security misconfigurations.

Tenable's 100% asset discovery capability—driven by its Tenable Nessus Network Monitor and Log Correlation Engine® (LCE®) technologies—ensures that you're never left in the dark as VMs are deployed. New VMs are passively discovered in between active vulnerability scans and are instantly assessed for security risks. And when active vulnerability scans are performed, Tenable's VMware SOAP (simple object access protocol) API enables seamless authentication to VMware vSphere and vCenter systems, increasing the depth and accuracy of your credentialed scans while auditing the efficacy of your VMware patch deployments.

How It Works



Step 1: Tenable Nessus scanner connects to VMware host and authenticates VMware admin credentials via Tenable's VMware SOAP API as a prerequisite to performing a credentialed scan.

vmware®

Components:

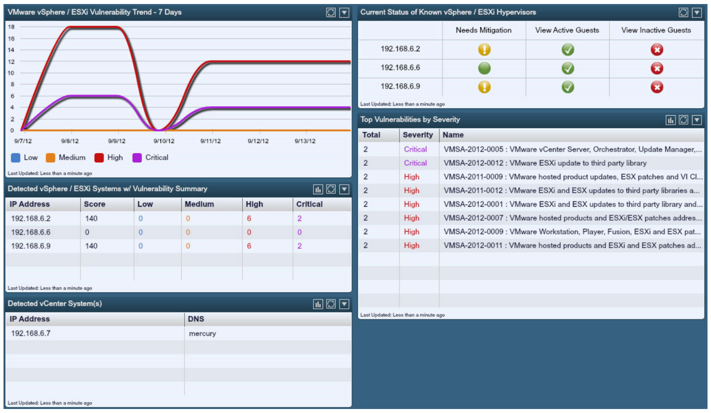
- Tenable SecurityCenter
- Tenable Nessus
- Tenable VMware SOAP API
- Tenable Nessus Network Monitor
- Tenable Log Correlation Engine
- VMware vSphere ESX and/or ESXi
- VMware vCenter

Benefits:

- Detect VMware-specific vulnerabilities and security misconfigurations
- Audit the efficacy of deployed VMware system patches
- Demonstrate compliance with industry and/or government regulations
- Help contain VM sprawl by passively detecting new VM
- Leverage VMware platform for deploying vulnerability management software components

Step 2: Tenable Nessus scanner, equipped with 140+ VMware-specific plugins/checks, identifies potential VMware vulnerabilities and security misconfigurations and audits deployed VMware patches.

Step 3: Tenable Nessus Network Monitor and LCE identify new VMs in real time and assess them for potential security risks. Dynamic asset lists are created in SecurityCenter to trigger active credentialed Nessus scans of new VMs for deeper analysis.


VMware vSphere / ESXi Vulnerability Trend - 7 Days
18
16
14
12
10
8
6
4
2
0
9/7/12
9/8/12
9/9/12
9/10/12
9/11/12
9/12/12
9/13/12
Low
Medium
High
Critical
Last Updated: Less than a minute ago

Detected vSphere / ESXi Systems w/ Vulnerability Summary

IP Address	Score	Low	Medium	High	Critical
192.168.6.2	140	0	0	6	2
192.168.6.6	0	0	0	0	0
192.168.6.9	140	0	0	6	2

Last Updated: Less than a minute ago

Detected vCenter System(s)

IP Address	DNS
192.168.6.7	mercury

Last Updated: Less than a minute ago

Current Status of Known vSphere / ESXi Hypervisors

	Needs Mitigation	View Active Guests	View Inactive Guests
192.168.6.2	!	✓	✗
192.168.6.6	●	✓	✗
192.168.6.9	!	✓	✗

Last Updated: Less than a minute ago

Top Vulnerabilities by Severity

Total	Severity	Name
2	Critical	VMSA-2012-0005 : VMware vCenter Server, Orchestrator, Update Manager,...
2	Critical	VMSA-2012-0012 : VMware ESXi update to third party library
2	High	VMSA-2011-0009 : VMware hosted product updates, ESX patches and VI Cl...
2	High	VMSA-2011-0012 : VMware ESXi and ESX updates to third party libraries a...
2	High	VMSA-2012-0001 : VMware ESXi and ESX updates to third party library and...
2	High	VMSA-2012-0007 : VMware hosted products and ESXi/ESX patches addres...
2	High	VMSA-2012-0009 : VMware Workstation, Player, Fusion, ESXi and ESX pat...
2	High	VMSA-2012-0011 : VMware hosted products and ESXi and ESX patches ad...

Last Updated: Less than a minute ago

The Tenable SecurityCenter interactive dashboard helps you monitor and prioritize potential system vulnerabilities and security misconfigurations of your VMware vSphere and vCenter hosts.

Integration Benefits

When selecting a vulnerability management system to protect both your physical and virtual computing environments, be sure to select one that is specifically designed to operate with your VMware environment. Such a solution should come equipped with a subset of plugins/checks to uncover VMware-specific system vulnerabilities and security misconfigurations to help you harden your virtual systems and maintain regulatory compliance. This helps U.S. federal agencies comply with the DISA VMware Security Technical Implementation Guide (STIG) and all organizations align with VMware's recommended hardening guidelines—an important step in maintaining PCI compliance.

Your active vulnerability scanners should also come equipped with a SOAP-based API to facilitate authentication to VMware hosts when performing credentialed scans of your vSphere and vCenter systems. This not only maximizes vulnerability detection accuracy, but also enables IT organizations to audit the efficacy of their installed VMware patches.

By selecting a vulnerability management solution capable of 100% asset discovery—through passive vulnerability scanning and log correlation—you'll have a new weapon in the fight against VM sprawl. And if your vulnerability management solution is completely software based, you can even leverage your VMware infrastructure to deploy your vulnerability management solution components.

The benefits of a combined Tenable and VMware solution are compelling:

- Rely on VMware-specific plugins/checks to uncover vSphere and vCenter system vulnerabilities and security misconfigurations
- Audit the efficacy of patches deployed to your VMware hosts
- Harden your VMware assets to comply with PCI, DISA STIG and other industry and government regulations
- Fight VM sprawl by identifying new VMs in real time and assessing them for security flaws
- Leverage your VMware platform to deploy components of your vulnerability management solution

About VMware

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the Cloud Era. Customers rely on VMware to help them transform the way they build, deliver and consume Information Technology resources in a manner that is evolutionary and based on their specific needs. With 2012 revenues of $4.61 billion, VMware has more than 500,000 customers and 55,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at vmware.com.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact