Tenable Webcast Summary
Managing Vulnerabilities in Virtualized and Cloud-based Deployments

Introduction

Server virtualization and private cloud services offer compelling benefits, including hardware consolidation, rapid provisioning and reduced infrastructure complexity. But virtualization technology also introduces security and compliance challenges that are not easily addressed with traditional vulnerability management tools and techniques.

As part of an ongoing series of webcasts into security management topics, Tenable Network Security presented a webinar in June 2013 dedicated to the topic of managing vulnerabilities in virtualized and private cloud environments. Ron Gula, founder and CTO of Tenable Network Security, and Jack Daniel, a technical product manager at Tenable, shared their thoughts. This paper summarizes key points from the webcast.

Key Take-Aways

- Virtualization expands both the number of systems at risk and the overall size of the attack surface.
- No single tool will solve your problem – securing a virtualized environment is a multi-step process.
- Continuous monitoring is a cornerstone of the security process for virtualized environments.

Challenges of Managing Security for Virtual Environments

A server virtualization environment presents all of the configuration and deployment challenges of traditional, physical infrastructure with added complexities:

VM sprawl

Because it's so easy and fast to spin up new servers or clone existing ones, organizations often create a large number of virtual machines, increasing the number of servers to monitor and manage. Any problems that you have in the physical environment will be magnified in the virtual environment. Without tight controls, it's difficult to ensure that all new VMs adhere to appropriate security and configuration controls.

Dynamic environment

Tracking and updating what you have can be a challenge as people create, suspend and move virtual machines. If you don't update your golden image from which virtual machines are deployed, you can end up needing to find and patch many virtual machines.

Many layers, many players
Virtualization adds another team and another skill set to the overall an complex security environment with physical and network layers. Individuals usually lack insight into the areas beyond their own expertise, yet understanding context is critical for assessing risk. With 'silos' of expertise, it can be difficult to get an accurate understanding of the actual risk profile of a virtualized system.

A new attack surface
The virtualization layer is itself another attack surface – one that attackers are starting to target. Management interfaces are often the weak link. An attacker that compromises a web-based management interface can compromise *all* hosts on that server.

Virtual systems can also be particularly vulnerable to Distributed Denial of Service (DOS) attacks that dirsupt service by consuming resources. A DOS attack that ramps up CPU or memory consumption on a virtual machine can actually steal resources from other VMs on the same physical infrastructure, having a broader effect than just the targeted system.

Securing Virtualization is a Process

Tools alone cannot solve the problem. VMware tools, for example, address only VMware issues, while Windows patch management tools focus on their discrete problems. Understanding and addressing the reality of threats in context requires an ongoing, multi-step process.

Step 1: Define policies and procedures
The first step is to develop the policies and procedures that make sense in your organization. The level of acceptable risk and location of particularly sensitive systems will vary for each business.

Step 2 – Develop a plan to stay compliant with change control
Create a plan for remaining compliant with policies. In most cases, this plan should include change control. Although some people see change control systems as a roadblock, when implemented properly, change control enables more frequent change with confidence. If you want to sustain an agile development culture with continuous updates and changes, you need the ability to find and rewind changes that cause problems. And if you're moving from bare iron to virtualization, change control is critical, as changes at one layer can affect systems up the stack.

Step 3: Implement your plan to harden and control systems
Define policies to harden servers appropriately for their function and business risk. For virtual infrastructure, these policies may include simple things like aligning password complexity settings with corporate policies and configuring images according to best practices.

Step 4: Scan your environment
Scan your physical and virtual environment for vulnerabilities and for compliance with policies and hardened configuration policies. *Discovery scans* find running systems, including virtual servers and clients. *Configuration scans* ensure that systems are configured according to internal policies, and *patch audit scans* check that both the virtualization software itself and the hosted servers are running at appropriate patch levels.

Step 5: Distribute the right data to the right people
Distribute the results of the scans to the people who can fix the problems identified. If you make people dig through extraneous layers of information to find their data, they may miss important details.

Step 6: Fix the problems
Track that the reported problems are fixed.

Step 7: Repeat on a regular basis
Changes happen quickly and continuously, particularly in virtualized environments. Continuous network monitoring is an emerging best practice among government and commercial organizations. And any organization can benefit by adding many smaller, targeted scans focusing on critical systems in between larger quarterly or annual scans. This strategy reduces the number of surprises and problems generated by larger quarterly or annual scans.

Using Tenable to Implement your Security Plan

Tenable SecurityCenter™ Continuous View combines active scanning (with Tenable Nessus™), passive detection and log analysis to deliver continuous insight into the security status of your dynamic IT architecture, including virtual and cloud systems.

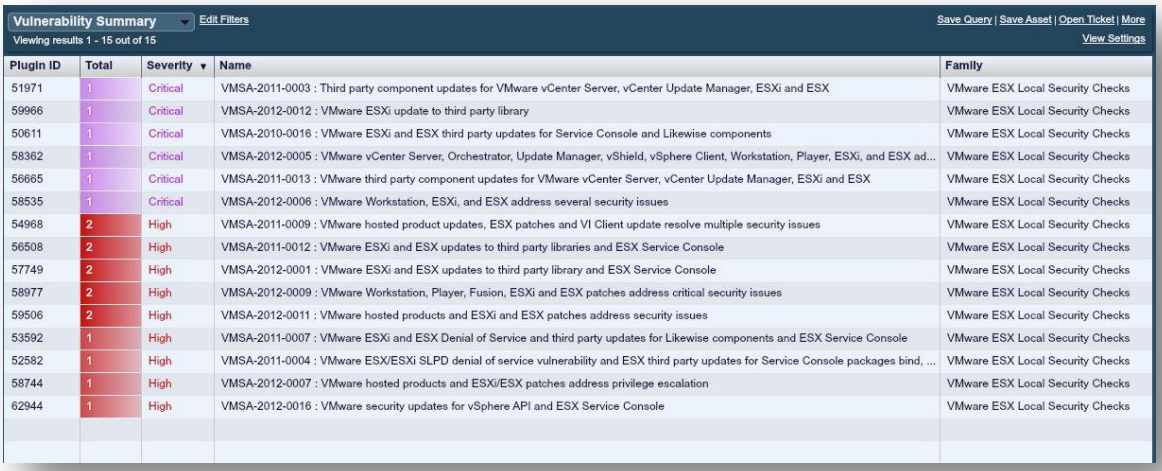
Using Tenable SecurityCenter will help you address steps 4-7 above, with comprehensive scanning, role-based reporting and dashboards, and continuous discovery and monitoring of your virtual environment.

Step 4: Scanning
Using SecurityCenter gives you deep visibility into your virtual environment. Tenable Nessus and SecurityCenter use the VMware API to securely access detailed information about ESX, ESXi or vSphere environments.

Discovery scans can detect and report on:

- VMware servers: including ESXi and vSphere
- VMware clients (VMware workstation and VMware Fusion)
- Other virtualization platforms: KVM, Xen, VirtualBox

Patch audits check patch levels for VMware server and client software, including VMware Fusion, Workstation, ESX/ESXi, vSphere, and vCenter.



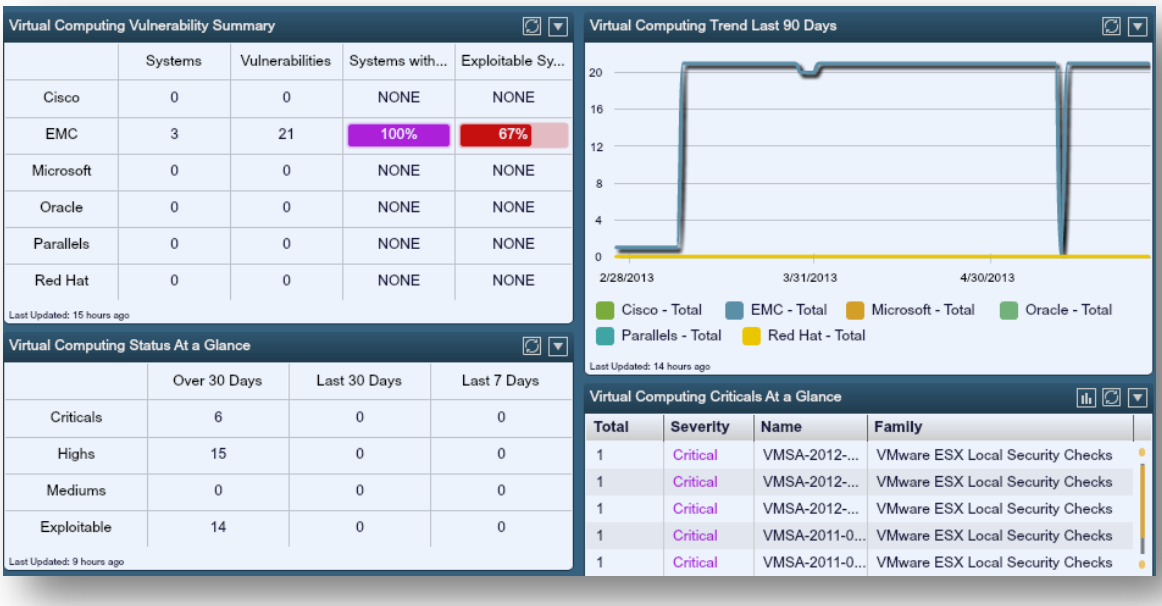
Plugin ID	Total	Severity	Name	Family
51971	1	Critical	VMSA-2011-0003 : Third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX	VMware ESX Local Security Checks
59966	1	Critical	VMSA-2012-0012 : VMware ESXi update to third party library	VMware ESX Local Security Checks
50611	1	Critical	VMSA-2010-0016 : VMware ESXi and ESX third party updates for Service Console and Likewise components	VMware ESX Local Security Checks
58362	1	Critical	VMSA-2012-0005 : VMware vCenter Server, Orchestrator, Update Manager, vShield, vSphere Client, Workstation, Player, ESXi, and ESX ad...	VMware ESX Local Security Checks
56665	1	Critical	VMSA-2011-0013 : VMware third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX	VMware ESX Local Security Checks
58535	1	Critical	VMSA-2012-0006 : VMware Workstation, ESXi, and ESX address several security issues	VMware ESX Local Security Checks
54968	2	High	VMSA-2011-0009 : VMware hosted product updates, ESX patches and VI Client update resolve multiple security issues	VMware ESX Local Security Checks
56508	2	High	VMSA-2011-0012 : VMware ESXi and ESX updates to third party libraries and ESX Service Console	VMware ESX Local Security Checks
57749	2	High	VMSA-2012-0001 : VMware ESXi and ESX updates to third party library and ESX Service Console	VMware ESX Local Security Checks
58977	2	High	VMSA-2012-0009 : VMware Workstation, Player, Fusion, ESXi and ESX patches address critical security issues	VMware ESX Local Security Checks
59506	2	High	VMSA-2012-0011 : VMware hosted products and ESXi and ESX patches address security issues	VMware ESX Local Security Checks
53592	1	High	VMSA-2011-0007 : VMware ESXi and ESX Denial of Service and third party updates for Likewise components and ESX Service Console	VMware ESX Local Security Checks
52582	1	High	VMSA-2011-0004 : VMware ESX/ESXi SLPD denial of service vulnerability and ESX third party updates for Service Console packages bind, ...	VMware ESX Local Security Checks
58744	1	High	VMSA-2012-0007 : VMware hosted products and ESXi/ESX patches address privilege escalation	VMware ESX Local Security Checks
62944	1	High	VMSA-2012-0016 : VMware security updates for vSphere API and ESX Service Console	VMware ESX Local Security Checks

Uncover patch level problems for the virtualization software layer, categorized by severity

For configuration auditing, Tenable provides an audit policy based on a combination of VMware's security guide and Tenable best practices. You can edit and fine-tune these audit policies depending on your own policies (as determined in step 1).

Step 5 and 6: Distributing and fixing problems

SecurityCenter lets you create role-specific dashboards and reports for the different participants in the security environment, so you can easily distribute exactly the information people need. In addition, you can monitor remediation efforts by tracking vulnerability trends over time.



A SecurityCenter dashboard shows the current status as well as ongoing vulnerability trends

Step 7: Continuous Monitoring
With a combination of active and passive scanning, Tenable SecurityCenter Continuous View helps you continuously monitor your environment for changes to physical and virtual systems and to initiate active scans of new or changed systems automatically. Using SecurityCenter, you can implement true continuous monitoring even to the virtual machine level.

Summary

Virtualization technology introduces security and compliance challenges that traditional vulnerability management practices do not address. It's easy for unscanned, unpatched virtual machines to become active in your network without your knowledge. And virtualization introduces new attack surfaces in the hypervisor and the virtualization management interface.

Managing risk in the virtual environment requires a combination of policies based on business needs, procedures for enforcing compliance, and technologies for finding, tracking and managing vulnerabilities and compliance issues in the virtual environment and beyond. Tenable SecurityCenter Continuous View is a powerful solution for addressing the scanning, reporting, and ongoing monitoring requirements of server virtualization. Tight integration with the VMware API makes SecurityCenter a particularly valuable solution for VMware environments.

To listen to the full discussion or access other, related webcasts, visit www.tenable.com/webcasts. You can find more white papers, videos and webinars in the Resources section at www.tenable.com

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are used by many Global 2000 organizations and government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.