Security Monitoring for the vSphere Infrastructure

Nessus® audits VMware® vSphere® ESX™/ESXi™ and vCenter™

The Unique Challenges of Virtual Machines

While there has been significant growth over the last several years in the use of virtualization technology in modern data centers, organizations are still learning how to migrate their work loads.

Although virtualization significantly reduces the need for incremental hardware, it adds another layer that can be attacked, creating unique management and security challenges.

- The host OS used to run and maintain your virtualized environment must be protected from attacks, or your entire infrastructure could be at risk.
- Attackers could “jump” from guest-to-guest and from guest-to-host with VMware escape attacks.
- The ease with which administrators can quickly and easily create new virtual servers often results in virtual machine (VM) sprawl.
- Guest OS vulnerabilities, like unpatched virtual desktops, create additional security exposure.

Tenable Nessus Vulnerability Scanner

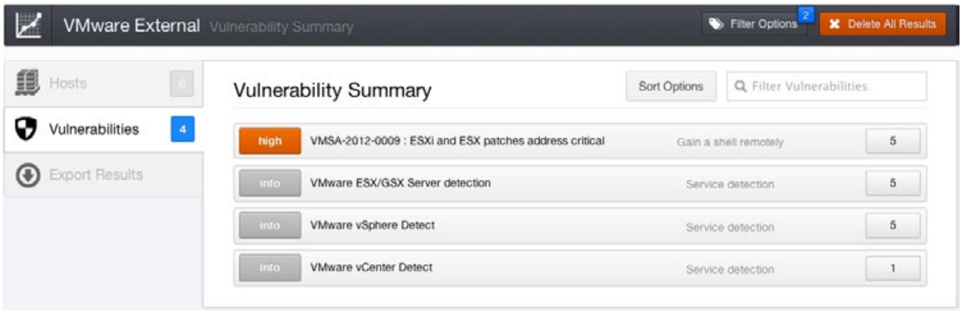
Nessus® is the market-defining vulnerability scanner that allows you to monitor and manage the security of your virtualized infrastructure. Deploy Nessus on a VM or run the Tenable Appliance VM, and configure either to scan your virtual infrastructure as often as you like.

Using a variety of remote and credentialed checks, Nessus performs a wide range of audits against the virtualization platform as well as the software running on it. Nessus detects virtualization servers, discovers vulnerabilities, audits patches, enumerates VMs, and performs configuration and compliance audits. This provides complete visibility into your infrastructure to deal with the challenges of VM sprawl, unpatched software, and misconfigured ports and services.

Nessus supports the following VMware products: VMware vSphere® ESX™, VMware vSphere ESXi™, and VMware vCenter™ Server.

Network-based Vulnerability Scanning for VMware

Without credentials, Nessus first determines how many VMware ESX/ESXi/vCenter servers are on your network and their location. Nessus not only detects virtualized servers, but it also identifies vulnerabilities using network-based vulnerability checks.



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

Figure 1: The Nessus research team creates plugins to detect network-based vulnerabilities for VMware products where available.

Nessus Key Features for VMware

- Unlimited scanning
- Cross-platform VMware vulnerability scanning: hypervisors, VMs, databases, web servers
- VM discovery
- Multi-platform patch auditing
- Comprehensive malware & botnet detection
- Configuration auditing
- Compliance auditing

Deployment Options for VMware

- Flexible deployment
  - Native Nessus software on numerous OSs
  - Tenable Appliance VM for VMware Server, Player, ESX, Workstation, & Fusion
- Agentless architecture
  - Automatic plugin and user-interface updates

Scanning Configuration & Management

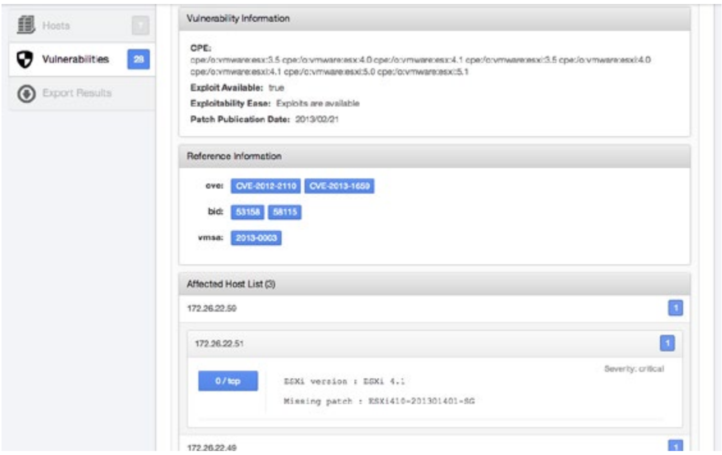
- Easy-to-use GUI (HTML5)
- Extensible API for scripting & integration
- Built-in scanning templates
- Smart scheduling with Scheduled Scan Templates

Vulnerability & Compliance Reporting

- Executive summary
- Customizable reports
- Risk-based severity levels & remediation recommendations
- Scan result comparison tool
- Native (XML), PDF, CSV, & HTML formats

VMware Patch Auditing

Once the virtualization platforms are identified, Nessus can scan them using credentials. This allows Nessus to log in via the VMware SOAP API to perform patch auditing and pull information about hosted VMs. Nessus reports the missing patches for each VMware ESX/ESXi/ vCenter server that is scanned.



Vulnerability Information

CPE:
cpe:/o:vmware:esx:3.5 cpe:/o:vmware:esx:4.0 cpe:/o:vmware:esx:4.1 cpe:/o:vmware:esxi:3.5 cpe:/o:vmware:esxi:4.0 cpe:/o:vmware:esxi:4.1 cpe:/o:vmware:esxi:5.0 cpe:/o:vmware:esx:5.1
Exploit Available: true
Exploitability Ease: Exploits are available
Patch Publication Date: 2013/02/21

Reference Information

cve: CVE-2012-2110 CVE-2013-1659
bid: 53158 58115
vmsa: 2013-0003

Affected Host List (3)

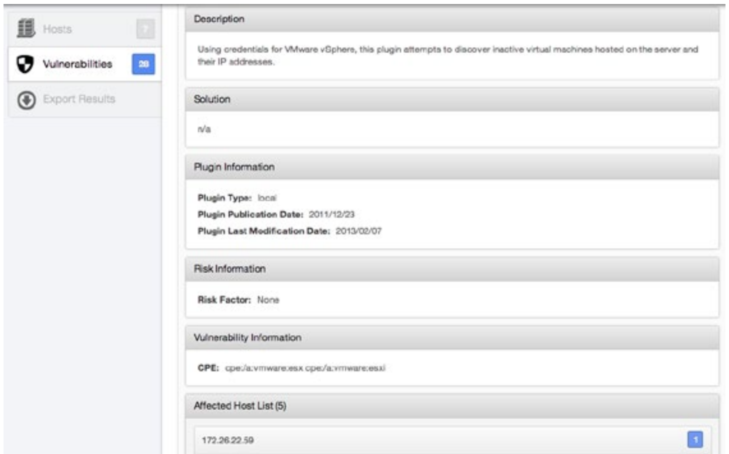
172.26.22.50 1
172.26.22.51 1
0 / tcp
Severity: critical

```
ESXi version : ESXi 4.1
Missing patch : ESXi410-201301401-SG
```

172.26.22.49 1

Figure 2: Nessus found an ESX server running version 4.1 that is missing a critical-severity-level patch.

Nessus can also log in and pull information from ESX/ESXi servers, such as active and inactive VMs on the host. This information is extremely useful to continually audit your virtualized environment, and acting on this information can help prevent VM sprawl.



Description

Using credentials for VMware vSphere, this plugin attempts to discover inactive virtual machines hosted on the server and their IP addresses.

Solution

n/a

Plugin Information

Plugin Type: local
Plugin Publication Date: 2011/12/23
Plugin Last Modification Date: 2013/02/07

Risk Information

Risk Factor: None

Vulnerability Information

CPE: cpe:/a:vmware:esx cpe:/a:vmware:esxi

Affected Host List (5)

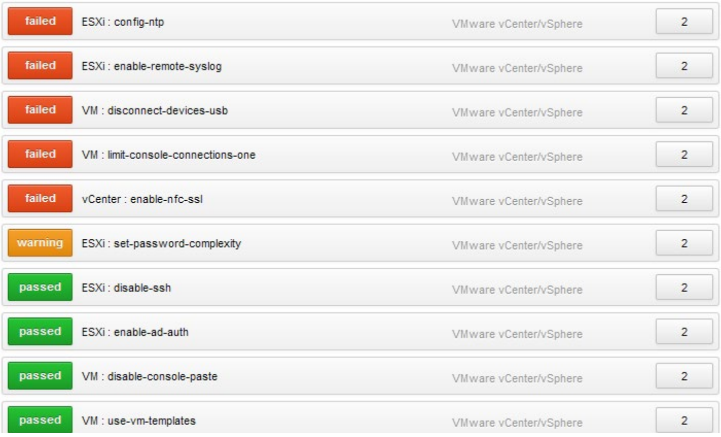
172.26.22.59 1

Figure 3: Nessus lists all the ESX/ESXi servers that were scanned and active/ inactive VMs.

Configuration and Compliance Auditing for VMware

In addition to detecting VMs, identifying vulnerabilities, and auditing patches, Nessus can also perform VMware configuration and compliance audits. Tenable's checks use the VMware SOAP API and support VMware ESXi 4.x/5.x and vCenter 4.5 (or later)/5.x.

Tenable supplies Nessus users with customizable compliance auditing files that provide more than double the checks currently available in VMware's compliance checking tool. Nessus provides users with reports to show how the user's configuration compares to VMware's hardening guidelines and the DISA VMware ESXi/vCenter 5 Security Technical Implementation Guide (STIG). Nessus is also able to examine and report on additional information useful to VMware administrators, such as if VMware Tools is installed, Guest IP addresses, overall VM status, and more.



failed	ESXi : config-ntp	VMware vCenter/vSphere	2
failed	ESXi : enable-remote-syslog	VMware vCenter/vSphere	2
failed	VM : disconnect-devices-usb	VMware vCenter/vSphere	2
failed	VM : limit-console-connections-one	VMware vCenter/vSphere	2
failed	vCenter : enable-nfc-ssl	VMware vCenter/vSphere	2
warning	ESXi : set-password-complexity	VMware vCenter/vSphere	2
passed	ESXi : disable-ssh	VMware vCenter/vSphere	2
passed	ESXi : enable-ad-auth	VMware vCenter/vSphere	2
passed	VM : disable-console-paste	VMware vCenter/vSphere	2
passed	VM : use-vm-templates	VMware vCenter/vSphere	2

Figure 4: Results from the "Tenable VMware Best Practices Audit" show a list of warnings, plus failed and passed checks, for the VMware ESXi target.

Tenable SecurityCenter for Simplified Administration

If your organization has a large number of Nessus scanners or a complex deployment, SecurityCenter™ provides a single management console to manage hundreds of Nessus scanners, gather and review scan results, and update plugins. In addition, SecurityCenter's role-based administration, monitoring, and reporting support organizations that distribute responsibilities across multiple teams.

Next Steps to Secure Your VMware-based Virtualized Environments

Getting a handle on your virtualized environments can be a challenging task, but Tenable can help. For more information on how Nessus can monitor the security of your VMware-based infrastructure, please contact a Tenable Authorized Partner.

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