Solution Brief

Tenable and Red Hat

Securing Your Red Hat Enterprise Linux Environment While Simplifying Regulatory Compliance

Key Challenges

Maintaining compliance with a myriad of internal security standards (e.g., SANS 20 CSC, COBIT, ITIL) and/or external industry and government regulations (e.g., PCI, HIPAA, PCI) is a challenging task by any measure. IT security standards and regulations call for monitoring systems for unpatched vulnerabilities, but generating adequate audit reports is nearly impossible without performing credentialed network scans. And for some environments, credentialed scanning is either impractical or against internal IT policy.

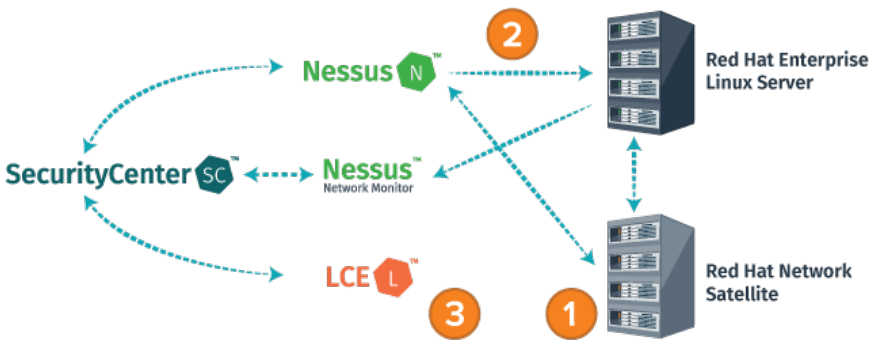
Furthermore, some rudimentary vulnerability scanning solutions are only equipped with checks for recent system vulnerabilities, while others lack adequate coverage for certain Linux-based platforms. Also, most scanners cannot properly identify backported Linux patches, making accurately depicting Linux vulnerabilities next to impossible. Also required is the ability to independently verify if systems are correctly patched and critical vulnerabilities are appropriately resolved and also track how quickly your patch management process is resolving critical risk or if improvements need to be made to reduce your window of exposure.

Without a best-of-breed vulnerability management solution, Red Hat customers, in particular, face the following challenges:

- Inability to generate adequate vulnerability management reports for compliance auditors depicting the patch status of internal IT Red Hat Enterprise Linux (RHEL) systems when credentialed scanning is not possible
- Inability to detect both recent and legacy vulnerabilities and security misconfigurations within RHEL hosts
- Inability to identify backported patches to avoid false positive Linux vulnerabilities
- Difficulty in verifying if systems are correctly patched and vulnerabilities are timely resolved

Solution Overview

Red Hat Network Satellite is an easy-to-use systems management platform that makes managing hundreds of RHEL hosts as easy as managing one. It provides powerful systems administration capabilities, including provisioning, monitoring and patch management. For RHEL environments where credentialed scanning is not possible, Tenable Nessus® interfaces with Red Hat Network Satellite API to automatically import the patch status of all monitored RHEL hosts. This intelligence is then shared with the Tenable SecurityCenter® management console to be incorporated into compliance reports.



Components:

- Tenable SecurityCenter
- Tenable Nessus
- Tenable Nessus Network Monitor
- Tenable Log Correlation Engine
- Red Hat Network Satellite
- Red Hat Network Satellite API
- Red Hat Enterprise Linux

Benefits:

- Import patch status of RHEL hosts into SecurityCenter management console for simpler compliance reporting
- Actively scan RHEL hosts for both current and legacy vulnerabilities and security misconfigurations
- Passively scan RHEL hosts in between periodic Nessus active scans
- Detect new RHEL hosts for scanning on network segments not monitored by Nessus Network Monitor
- Eliminate false positive Linux vulnerabilities by properly identifying backported RHEL patches
- Leverage RHEL as a Tenable-supported platform for hosting SecurityCenter, Nessus, Nessus Network Monitor and LCE software

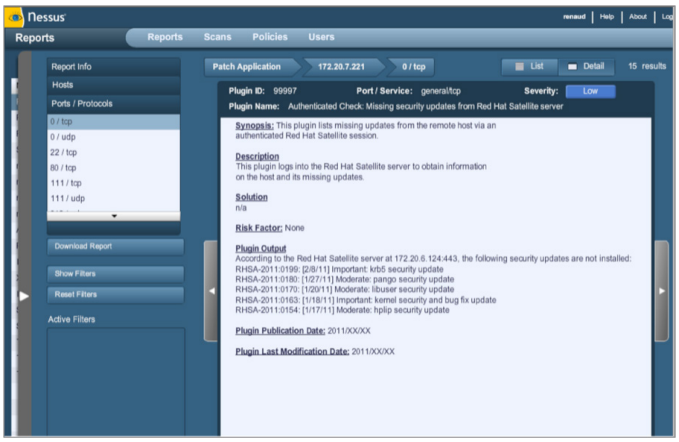
Tenable™ offers thousands of plugins/checks for detecting both recent and legacy vulnerabilities and security misconfigurations within your RHEL environment. Tenable Nessus Network Monitor passively monitors RHEL hosts for vulnerabilities in between periodic Nessus active scans, and Tenable Log Correlation Engine® (LCE®) identifies new RHEL hosts for scanning on network segments not monitored by Nessus Network Monitor.

How It Works

Step 1: Nessus interfaces with Red Hat Network Satellite API and imports the patch status of each monitored RHEL host—including identifying backported patches. This intelligence is then shared with SecurityCenter for compliance reporting.

Step 2: Nessus actively scans RHEL hosts for vulnerabilities and security misconfigurations.

Step 3: Nessus Network Monitor passively scans RHEL hosts in between periodic Nessus scans, and LCE aggregates log data from network infrastructure devices to identify new RHEL hosts for scanning on network segments not monitored by Nessus Network Monitor.



By importing patch status of all RHEL hosts monitored by Red Hat Network Satellite into Nessus, compliance auditors can incorporate RHEL patch intelligence into their SecurityCenter compliance reports.

Integration Benefits

Tenable makes it easy to incorporate the patch status of RHEL hosts monitored by Red Hat Network Satellite into SecurityCenter compliance reports. This is particularly important for Red Hat customers that have restrictions on performing credentialed scans of internal systems.

Also, since Nessus and Nessus Network Monitor are equipped with thousands of plugins/checks specifically designed to detect vulnerabilities and security misconfigurations within RHEL hosts—while LCE identifies new RHEL hosts to be scanned by Nessus—Red Hat customers gain peace of mind knowing that their Tenable vulnerability management solution will protect their RHEL investment.

The benefits of a joint Tenable-Red Hat solution can be summarized as follows:

- Incorporate RHEL systems' patch status into SecurityCenter compliance reports
- Detect recent and legacy vulnerabilities and security misconfigurations within RHEL hosts
- Passively detect security concerns within RHEL hosts in between periodic Nessus active scans
- Identify new RHEL hosts to be scanned by Nessus on network segments not monitored by Nessus Network Monitor
- Eliminate false positive Linux vulnerabilities by properly identifying backported RHEL patches
- Leverage RHEL as an ideal platform to host SecurityCenter, Nessus, Nessus Network Monitor and LCE software

About Red Hat

Red Hat is the world's leading provider of open source software solutions, taking a community-powered approach to reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As the connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT. For more information about Red Hat, please visit redhat.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.

tenable™

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