Solution Brief

Tenable and Cisco

Device and User Context for Vulnerabilities

Key Challenges

The modern enterprise is an ever-changing landscape of network, security and identity solutions – owned and operated by different parts of the organization. This results in operational silos and manual overhead in obtaining data when decisive response to security and compliance issues is required. Consequently, organizations face key challenges in answering questions such as:

- What systems in my network are at risk or out of compliance?
- Who are the users associated with those systems? What risk do they pose?
- What are the risks that require immediate action?

Tenable Nessus® is essential for identifying risk and compliance violations across servers, hosts, databases and mobile devices. In addition to device-level information, IT organizations may also require detailed context, such as user identity, to prioritize and respond to critical vulnerabilities. Such data may not be available from vulnerability scanning alone and may reside on other systems in the customer environment.

What is not needed is another product. What is required is a framework that allows the sharing of user and device context with the vulnerability management solution. This allows the reuse of existing investments and offers a unified view to identify the offending device as well as the user and initiate response.

Solution Overview

Tenable Nessus Manager integrates with the Cisco® Identity Services Engine (ISE) to deliver in-depth vulnerability assessment along with relevant identity and device data. This integration provides security analysts with the context they need to quickly assess and prioritize the severity of vulnerabilities by answering questions such as “Who is this vulnerability associated with?” and “What level of access do they have on the network?” Administrators can then quickly initiate actions from the Nessus management console on the users or devices within the Cisco network infrastructure.

For example, in response to a severe vulnerability, administrators can take mitigation actions through the ISE Dynamic Network Control capabilities, which can quarantine or isolate users or devices. This suite of capabilities reduces vulnerability review and response time.

The solution includes Tenable Nessus and Cisco ISE (with ISE Plus or Advanced Feature License) for context exchange. ISE is part of Cisco’s pxGrid unified framework that enables multi-vendor, cross-platform network system collaboration. pxGrid integrates security monitoring and detection systems, network policy platforms, identity and access management platforms, and virtually any other IT platform.

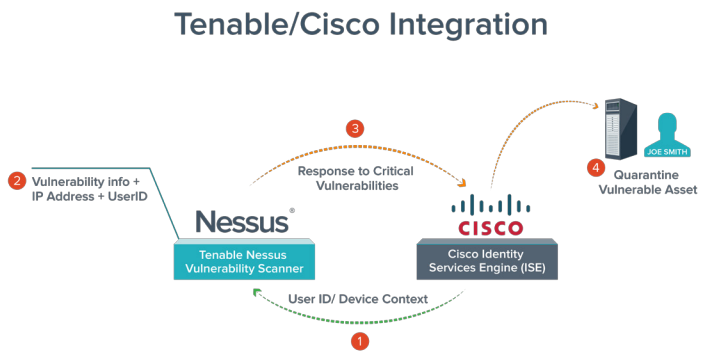
Components:

- Tenable Nessus Manager
- Cisco Identity Services Engine (ISE)

Benefits:

- Decreases time and increases granularity of risk analysis by fusing user identities and permissions with vulnerability scan results
- Facilitates faster response by prioritizing critical issues based on device and user context
- Allows immediate response directly from within Nessus
- Enables Nessus to isolate systems and users that pose a risk by requesting a quarantine action
- Enables fast, closed loop management of the issue or event

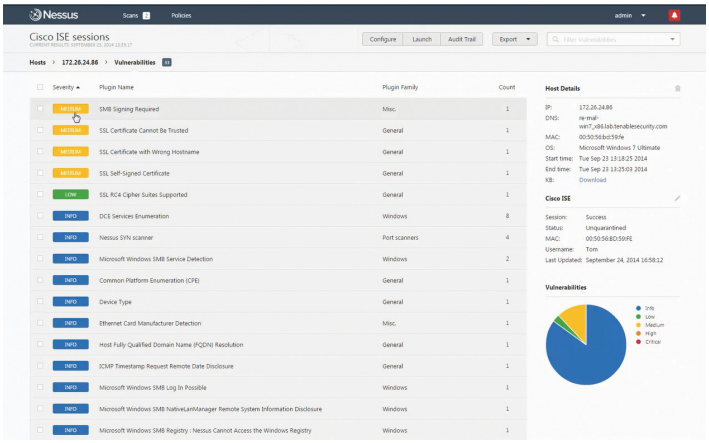
By utilizing Cisco ISE, Nessus administrators enhance their traditional vulnerability assessments with user identity, network authorization level, network access method and security posture information. This results in a "single-pane-of-glass" view of the vulnerability from the Nessus management console. Nessus users can take advantage of ISE integration by investigating the event, and then initiating network mitigation actions directly from the Nessus management console.



How It Works

Here's how the Nessus + ISE integration works:

1. Cisco ISE provides user identity and device information to Nessus.



2. Nessus uses this contextual data to provide a comprehensive view of the vulnerability event, user and device data along with vulnerability severity. This helps staff prioritize vulnerability events and leads to quick response.

3. If the severity of the vulnerability justifies a response, a security specialist can initiate network quarantine action via ISE from the Nessus management console. This provides closed loop management of the event.

Supported Release Versions

The following software versions are required for this integration:

- Cisco ISE 1.3 or later
- Tenable Nessus Manager v6.3 or later

Additional Information

For more information about Cisco and Tenable integration, visit the Cisco Developer Network Marketplace at marketplace.cisco.com/catalog (Search for keyword "Tenable").

More details on Cisco ISE are at: cisco.com/c/en/us/products/security/identity-services-engine/index.html

For any business or technical inquiries, contact us directly at cisco-sales@tenable.com

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected.

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