tenable®

Tenable for Thycotic Secret Server
Automating Credentialed Vulnerability Assessments

thycotic

Business Challenge

Organizations are constantly challenged with the ability to control, manage and monitor privileged access to its most valuable assets. Vulnerability scans require gaining access to and navigating an ever-changing sea of usernames, passwords and privileges. Without integrating Thycotic Secret Server and Tenable, managing credentials becomes increasingly complex and assets could be left at risk with an alarming increase in the attack surface.

Solution

The Tenable® integration with Thycotic Secret Server delivers a comprehensive authenticated scanning solution that provides security teams better vulnerability insight in order to further protect privileged accounts. This integration supports the storage of privileged credentials in Thycotic Secret Server and their automatic retrieval at scan time by Tenable. This ensures that sensitive passwords are safely stored, controlled, auditable and easily changed without manual intervention.

Value

The Tenable integration for Thycotic Secret Server provides the ability to:

- Eliminate risks from decentralized management of privileged or administrative credentials

- Simple management of credentials necessary for vulnerability management assessments

- Meet government and industry compliance rules to account for the management of organizational credentials

- Fully automated credentialed scanning across your organization

Technology Components

- Tenable.io or Tenable.sc 5.5 or higher

- Thycotic Secret Server Version 10.4 or higher

Key Benefits

- **Automates** credential retrieval at scan time for deeper analysis

- **Simplifies** secure scanning with less management required

- **Reduces time and effort** needed for credential additions and changes

- **Reduces the risk** of unsecured privileged accounts and credentials

- **Improves compliance** with regulation requiring management of credentials

- **Improve data accuracy** with credentialed scanning compared to non-credentialed scanning

Features

With this integration, you can:

- Perform credentialed scans of Windows Hosts

- Perform credentialed scans of Unix (SSH) hosts

- For the above credential types this integration supports 1 or more methods of gathering credentials to be used:
    - For each machine to be scanned get a unique password based on static username and machine ip/hostname
    - Get a password stored in "secret" this password will be used to login to every machine in the scan

How It Works

1. Tenable requests a scan of asset(s) using Thycotic Secret Server credentials

2. Nessus® requests credentials for the asset to be scanned

3. Thycotic Secret Server provides the credentials for the asset

4. Nessus scans the asset using the provided credentials
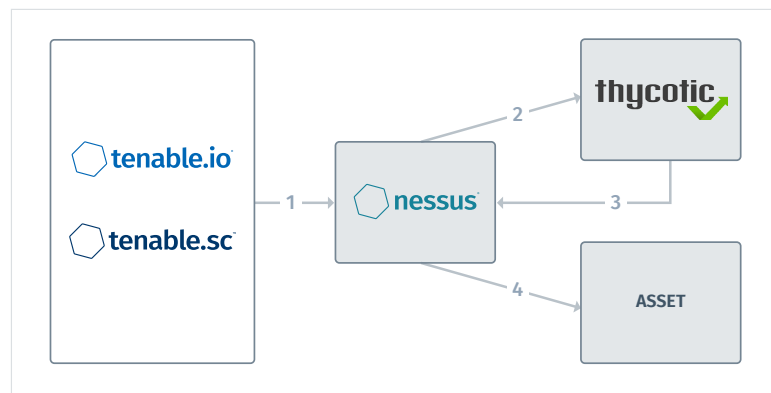
More Information

Installation and configuration documentation:
https://docs.tenable.com/integrations/PDFs/Integration_Guide-Tenable.io_Thycotic.pdf

https://docs.tenable.com/integrations/PDFs/Integration_Guide-SC_Thycotic.pdf

For support please contact: **support@tenable.com**