



Tenable for HashiCorp Vault

Automating Credentialed Vulnerability Assessments

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 HashiCorp Vault 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 HashiCorp Vault Key Value (KV) store 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 HashiCorp Vault KV 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 HashiCorp Vault KV 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
- HashiCorp Vault v1.2.2 Enterprise

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

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT HASHICORP

HashiCorp is the leader in cloud infrastructure automation software. Our suite of tools enables organizations to provision, secure, connect, and run any infrastructure for any application. We unlock the cloud operating model for every business and enable their digital transformation strategies to succeed. Learn more at hashicorp.com

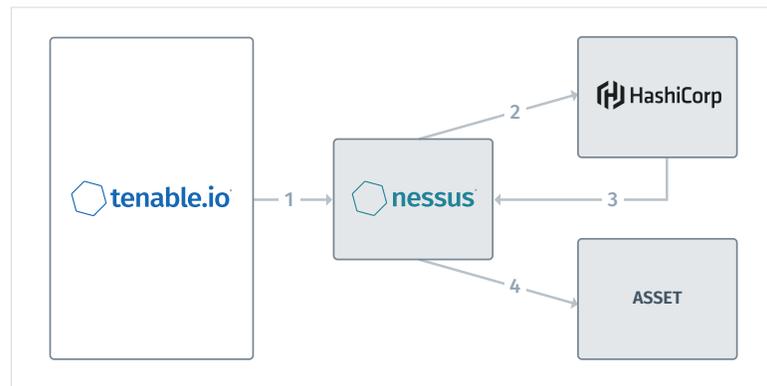
Features

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:
 - Get a password stored in “secret” this password will be used to login to every machine in the scan
 - Get a username and password from HashiCorp Vault KV

How It Works

1. Tenable requests a scan of asset(s) using HashiCorp Vault KV credentials
2. Nessus® requests credentials for the asset to be scanned
3. HashiCorp Vault KV 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/hashicorp/vault/Content/welcome.htm>

For support please contact: support@tenable.com

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.