Tenable.io Integration with Centrify Privileged Access Service to Strengthen Credential Management

Privileged credentials continue to be a focus for attackers in their data breach efforts. Successfully compromising an application, such as Tenable.io, that may contain hundreds of Windows and Linux server superuser account credentials, is a bonanza. Centrify's plugin for Tenable.io, along with the Centrify Privileged Access Service vault, mitigates this risk while bringing incremental value in automation and centralized policy management.

The Challenges Faced by Tenable.io Customers

Simply put, it's a matter for privileged access management, i.e., how to manage and secure access to privileged system accounts that, if compromised, could cost your organization millions. Millions in terms of stolen identities, fines, shareholder value, or the cost to clean up the resulting mess.

Many enterprise applications, especially those in the IT Service Management (ITSM), IT Operations Management (ITOM), and Continuous Configuration and Automation (CCA) spaces, such as Tenable.io, ServiceNow Discovery, and Red Hat Ansible Tower, must log into IT systems to do their job. In the case of the Tenable.io vulnerability management platform, the underlying Nessus scanner must log into Windows and Linux systems with superuser credentials to conduct its vulnerability scans.

Not Designed for Privileged Identity and Access Management

To enable scanning, Tenable customers must configure privileged credentials within Tenable.io. It's not unusual for larger organizations to require dozens, if not hundreds of them, each one representing a potential vector of attack if a threat actor (internal or external) gains unauthorized access to them. Unfortunately, Tenable.io was not designed for resilient storage, management, automation, and auditing the use of these credentials.

Nessus started life as an open source project in 1998. Tenable put a commercial skin on Nessus in 2005 with its first paid version. Back then, identity-centric data breaches were not a significant concern, so identity and credential management and security were not core design considerations. Today, although Tenable.io has evolved, the core design hasn't materially changed; those identity and credential management challenges persist. In fact, they're exacerbated due to IT infrastructure extending to the cloud and identity-based attacks spiraling by capitalizing on the resulting expanded attack surface.

Overhead of an Additional Silo of Identities

Having to configure potentially hundreds of system accounts within Tenable.io introduces yet another silo of identities that IT must now administer manually, increasing overhead for a team already stretched thin. When IT adds new systems or removes existing ones, they must add or remove the equivalent credentials in Tenable.io. When passwords on local systems change, IT must update their equivalent in Tenable.io. This additional silo of identities in Tenable.io represents a considerable overhead for IT.

Keeping Passwords Fresh and Synchronized

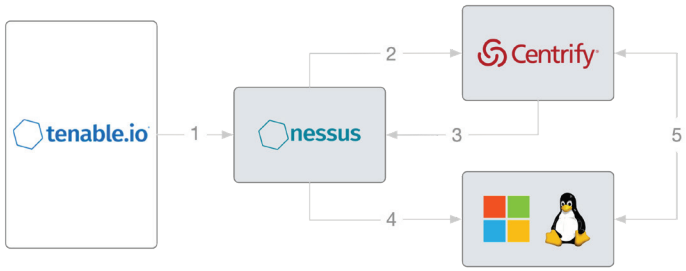
Security practitioners know that passwords are weak. Especially for privileged accounts that give broad access to critical IT systems, IT must strictly manage their passwords. You can't afford to simply set it and forget it. A best practice is to frequently rotate them and make them long and complicated, so they're more challenging for an attacker to predict. The overhead for IT in manually rotating hundreds of system account passwords frequently, often results in no change at all, increasing the risk of a compromise. If they do, however, when IT changes local account passwords on systems, they must also revisit those same account passwords configured in Tenable.io to ensure they match, adding to the overhead. Not doing this or not doing it promptly will cause Tenable.io to fail when attempting to log into target systems during a scan. Left uncorrected, this can result in exposed vulnerabilities and hence, additional risk.

Because of all this, Tenable customers are looking for a better way to protect and manage critical privileged account credentials, with a solution designed specifically for the job.

Centrify Privileged Access Service

Centrify has partnered with Tenable to provide joint customers with automated credentialed vulnerability assessments. Instead of storing privileged account passwords in Tenable.io, IT stores and centrally manages them in the Centrify Privileged Access Service vault. A Centrify plugin for Tenable integrates the two solutions.

Centrify designed its Privileged Access Service as a secure repository to store and control access to privileged credentials, ultimately overcoming the complexities of multiple identity silos with weak security and management. At heart is a secure vault used to store system account passwords, protecting them with strong encryption and role-based access controls (RBAC). RBAC strictly governs who can access the vault (interactively through the GUI or programmatically via APIs), what credentials they can see, and which ones they're allowed to check out. Tenable customers can immediately reduce risk and increase operational efficiency by leveraging this integration versus managing credentials directly within Tenable.io.



1. Tenable.io makes a request to Nessus to scan asset(s) using Centrify Privileged Access Service vaulted credentials.
2. Nessus requests credentials from the Centrify Privileged Access Service.
3. The Centrify Privileged Access Service validates the requestor, applies role-based access controls, and returns the credentials, optionally reconciling any out-of-sync passwords.
4. Nessus uses the credentials to log into the asset and performs its scan.
5. Independently, the Centrify Privileged Access Service automatically performs password rotation based on a scheduled frequency and according to password quality of service policies.

Even though Tenable.io still depends on weak passwords, Centrify helps customers compensate for their shortcomings. IT can schedule automatic password rotations to occur on a frequency of its choosing. During rotations, the vault will reach out to each system and change the password locally. Since this can amount to hundreds of accounts, automation is the only reasonable approach for IT to strengthen the quality of privileged account passwords effectively.

IT can also create strict password quality-of-service profiles in the vault to ensure they are arbitrarily long and complicated. That, along with a short rotation frequency, can mitigate the risk of an attacker cracking those passwords and using them to further their data breach agenda.

BENEFITS

- **Automates** credential retrieval at scan time and scheduled password rotation.
- **Simplifies** secure scanning with reduced operational overhead required to manage privileged credentials.
- **Reduces time and effort** for credential additions and changes.
- **Improves compliance** by satisfying requirements for secure, centralized management of privileged credentials and auditing of their use.
- **Improves data accuracy** with credentialed scanning compared to non-credentialed scanning.

When the vault rotates passwords, IT doesn't have to worry about keeping Tenable.io updated. In this scenario, Centrify's plugin to Tenable fetches current and valid passwords from the Centrify vault at scan time. Failed scans due to Tenable.io not being able to log in to systems can become a thing of the past.

Finally, when leveraging Centrify Privileged Access Service for Tenable.io, organizations also benefit from its built-in auditing and reporting to satisfy regulatory requirements. We continue to see regulations and guidance from industry standards bodies such as NIST and the PCI Security Council that require more robust control and management of privileged accounts. Centrify's auditing and reporting help organizations prove that these controls are in use and effective.

Better Together — Centrify Privileged Access Service and Tenable.io

With this combination, Tenable.io and Nessus Manager customers benefit from an industry-leading vault for controlled access to privileged accounts, automation to reduce operational overhead, and a centralized account management and policy framework to reduce the attack surface. IT continues to leverage Tenable.io's strengths without impacting its behavior or performance. Since the Centrify Privileged Access Service vault is a SaaS service, it is accessible from anywhere, facilitating Tenable.io scanning of systems on-premises or in the cloud.

Centrify enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid- and multi-cloud environments with Identity-Centric PAM based on Zero Trust principles. To learn more, visit www.centrify.com.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354

sales@centrify.com

www.centrify.com