Solution Brief

Tenable and Thycotic

Automating Credentialed Vulnerability Assessments

The Challenge

One of the most common attack vectors is through stolen credentials, especially privileged account credentials that unlock exceptional access to systems, applications and sensitive data. About 63% of confirmed data breaches involved weak, default or stolen passwords, according to the Verizon 2016 Data Breach Investigations Report.

Privileged account credentials are important for security because they can also unlock the discovery of vulnerabilities. Privileged account access permits deep scanning and analysis of targeted networks and systems for highly detailed results. Without this access, unauthenticated network scanning only scratches the surface by finding open ports and associated listening services. Unauthenticated scans reveal some issues – but these may or may not give you the entire picture of the device's security posture.

Maintaining privileged account credentials for security can be a huge challenge. It entails getting access to and navigating an ever-changing sea of usernames, passwords and privileges. Storing the credentials in your vulnerability management solution results in decentralized security policies and extra work to maintain those passwords. Keeping privileged account credentials in multiple locations also creates an additional attack vector for internal and external threats.

Without integration between your organization's credentials management solution and vulnerability management solution, you may encounter:

- Risks from decentralized management of privileged or administrative credentials
- Increased time and effort for adding or changing credentials used for vulnerability management assessments
- Failure to meet government and industry compliance rules to account for the management of organizational credentials

The Solution

Tenable™ has partnered with Thycotic to integrate Tenable Nessus® with Thycotic Secret Server. The integrated solution delivers a comprehensive authenticated scanning solution that gives security teams more insight while protecting sensitive privileged accounts.

The integrated solution supports storage of privileged credentials in Thycotic Secret Server and their automatic retrieval at scan time by Nessus. This ensures that sensitive passwords are controlled in a single, secure vault, don't proliferate and can be audited and changed without having to manually update the password after the fact.

The integrated solution makes it easy to manage and conduct secure credentialed scans. With the integrated solution, your security team will be able to automatically conduct credentialed assessments with Tenable Nessus to detect critical missing security patches, client-side vulnerabilities, read password policies and much more. Authenticating to the target system during Nessus scans produces more accurate results and gives complete visibility of vulnerabilities in selected targets and in the entire environment. These results will help your security team identify threats and vulnerabilities sooner.

Components:

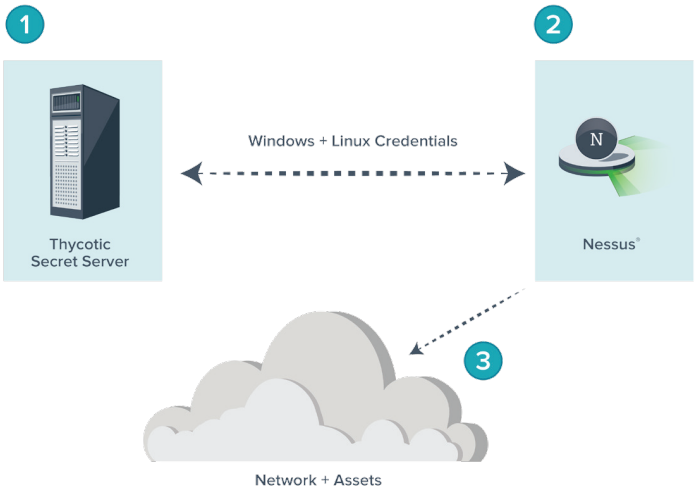
- Tenable Nessus Manager 6.7 or higher
- Tenable.io™
- Thycotic Secret Server 8.9 or higher Enterprise Plus Edition
- Thycotic Secret Server API

Benefits:

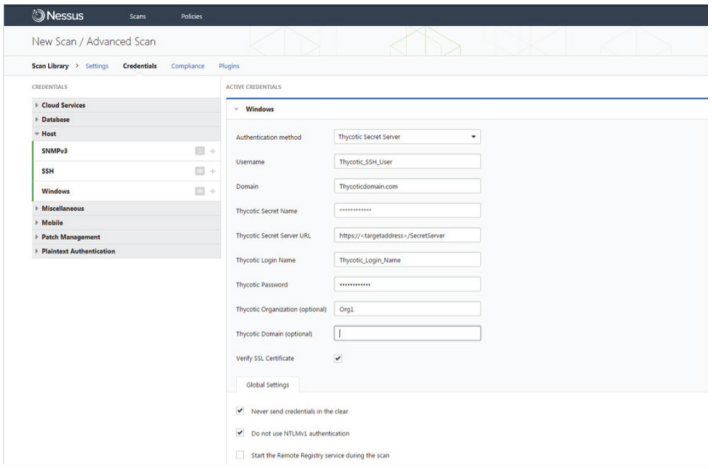
- **Automates** credential retrieval at scan time for deeper analysis
- **Simplifies** secure scanning
- **Reduces** time and effort needed for credential additions and changes
- **Shrinks** the attack surface
- **Improves** compliance with regulations requiring management of credentials

Results with the solution are better than unauthenticated assessments, which merely rely on exposed services or ports to try and determine issues. Credentialed scanning will give the precise reporting required for compliance security audits. Privileged account access in Thycotic Secret Server is audited, and security policies ensure passwords can be centrally changed regularly without manual steps to update stored credentials in Nessus.

How It Works



1. Create a Thycotic Secret Server account for Nessus to call for credentials
2. Configure Tenable.io or Nessus Manager for credentialed scans of Windows and Linux systems using Thycotic Secret Server
3. Tenable.io or Nessus Manager authenticates with Thycotic Secret Server to obtain credentials, then authenticates with the target machine for scanning



The integration of Tenable Nessus and Thycotic Secret Server automatically enables credentialed scanning for deeper visibility of threats and vulnerabilities.

Faced with today's constant threats of breaches and attacks, organizations need to protect privileged accounts and ensure accountability of use. Together, Tenable and Thycotic enable organizations to easily perform credentialed assessments to find the most accurate vulnerability information without compromising accountability or control of privileged credentials.

About Thycotic

Thycotic, a global leader in IT security, is the fastest growing provider of Privilege Management solutions that protect an organization's most valuable assets from cyber-attacks and insider threats. Thycotic secures privileged account access for more than 3,500 organizations worldwide, including Fortune 500 enterprises. Thycotic's award winning Privilege Management Security solutions minimize privileged credential risk, limits user privileges and controls applications on endpoints and servers. Thycotic was founded in 1996 with corporate headquarters in Washington, D.C. and global offices in the U.K. and Australia. For more information, please visit thycotic.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