Store QualysGuard-Authenticated Scan Credentials Securely in Secret Server

The QualysGuard cloud platform provides tools for organizations to identify their IT assets; it scans and analyzes large amounts of IT security data to find vulnerabilities, and then fixes them. The QualysGuard suite also delivers a full set of tools for addressing PCI compliance mandates, malware detection, and Zero-Day risk analyses.

QUALYSGUARD®

Secret Server

Authenticated vs. Unauthenticated Scanning

"Unauthenticated" security scanning is useful for seeing the network as an intruder would, where they have no credentials to access any systems. Unauthenticated scans reveal general configuration issues, such as open ports, code errors, or improperly defined permissions. An intruder can easily gain a username and password from the network (sniffing plain text traffic, malware and phishing) so authenticated scans are useful to ensure that the complete systems are secure.

Why use Authenticated Scanning?

- Authenticated scans are more thorough and are often able to find more sensitive issues, such as malware, registry problems, patches, incorrect software configuration, and other vulnerabilities.

- Unauthenticated testing will not find internal compliance issues; authenticated scanning is required by QualysGuard for compliance scans.

Authenticated Scanning Deployment Difficulties

- System administrators may be reluctant to give out credentials, especially when those credentials are stored by a third party.

- Performing password rotation can lead to failed scans if credentials aren't updated in every option profile and target asset simultaneously.

- Auditing the use of the shared credential becomes critically important when a single shared privileged ID is used across multiple targets.

Using Secret Server as a Credential Vault for Authenticated Scans

Secret Server is an on-premise, web-based password vault used to help organizations properly manage privileged account passwords. Secret Server allows users to control access and automate password changes for a variety of enterprise resources. Organizations can easily deploy Secret Server to be more secure, reduce labor costs, adopt password best practices, and satisfy audit requirements.

QualysGuard can use Secret Server as a Credential Vault for the accounts used for authenticated scanning. Instead of adding individual credentials for trusted scans, the Administrator can use named records stored in Secret Server. There are several benefits to this approach:

- Using Secret Server means that all the credentials used for authenticated scans will be stored securely on-premise and will not leave the network.

- Password rotation can happen frequently and automatically as Secret Server performs the password changes and QualysGuard retrieves the passwords as needed during scans.

- Credentials can still be securely controlled in Secret Server with full auditing over their usage.

Beyond Scanning – Managing Privileged Passwords in the Enterprise

Secret Server has usages beyond storing credentials for authenticated scans with QualysGuard. Service Accounts can also be managed in Secret Server, which will automatically update the dependent applications, such as a Windows Service, IIS App Pool, COM+ Service, Windows Scheduled Task, or flat files when a Service Account password change occurs. Application server passwords stored in build scripts, configuration files or source code can also be removed and retrieved from Secret Server at runtime using the Secret Server Application Server API.

Secret Server audits access to the privileged passwords, meaning it can help meet compliance requirements, such as PCI DSS, SOX, FISMA or HIPAA. Administrators or auditors can generate usage reports, force password changes on credentials when staff turnover occurs, and view recordings of Remote Desktop or SSH sessions.

QUALYS®

The QualysGuard® service is used today by more than 5,800 customers in over 100 countries, including a majority of the Forbes Global 100, and performs more than 600 million IP scans/audits per year.

thycotic

Thycotic Software is committed to providing password and AD group management solutions to IT administrators worldwide. With over 33,000 IT professionals using Secret Server, Thycotic helps securely manage all credentials critical to an organization's operations.