Tenable for CyberArk

Introduction

This document describes how to deploy Tenable SecurityCenter® and Nessus® for integration with CyberArk Enterprise Password Vault. Please email any comments and suggestions to support@tenable.com.

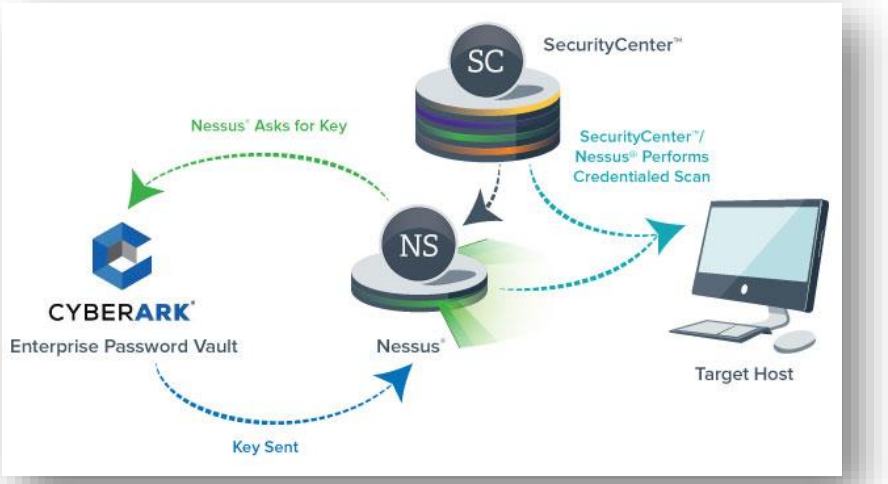
Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever- changing sea of usernames, passwords, and privileges. By integrating the CyberArk Enterprise Password Vault with Tenable's solutions, customers are now granted even more choice and flexibility for reducing the credentials headache.

Benefits of integrating Tenable SecurityCenter with CyberArk Enterprise Password Vault include:

- Credentials stored in CyberArk Enterprise Password Vault no longer need to be managed and updated directly within a Tenable solution
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise

Communication Architecture

The combined Tenable-CyberArk solution works when a SecurityCenter scan policy is configured to query a CyberArk Enterprise Password Vault for privileged credentials. At the time of the scan, SecurityCenter (via Nessus) sends a request to CyberArk to request the privileged account credentials to be used. CyberArk then provides the privileged account credentials back to Nessus, and the provided credentials are then used to log into the target system to identify vulnerabilities and misconfigurations.



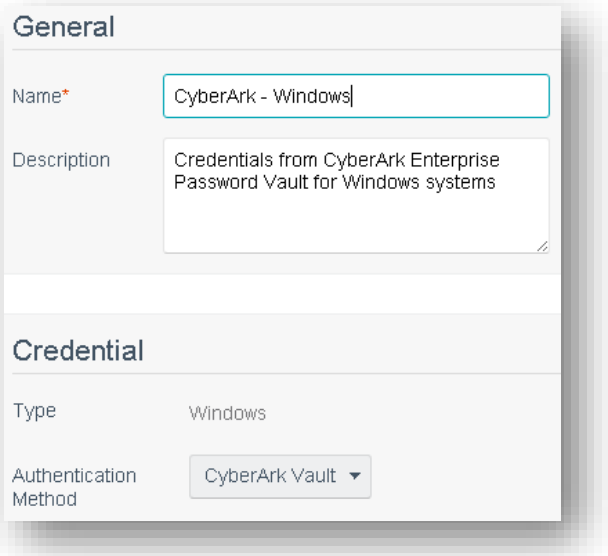
Nessus Manager, Nessus Cloud, SecurityCenter, and SecurityCenter Continuous View support CyberArk integration starting with versions 6.4 and 5.0.1 respectively. Both Nessus and SecurityCenter solutions work with CyberArk Enterprise Password Vault version 7.x, 8.x, and 9.0.

Integrating with CyberArk Enterprise Password Vault

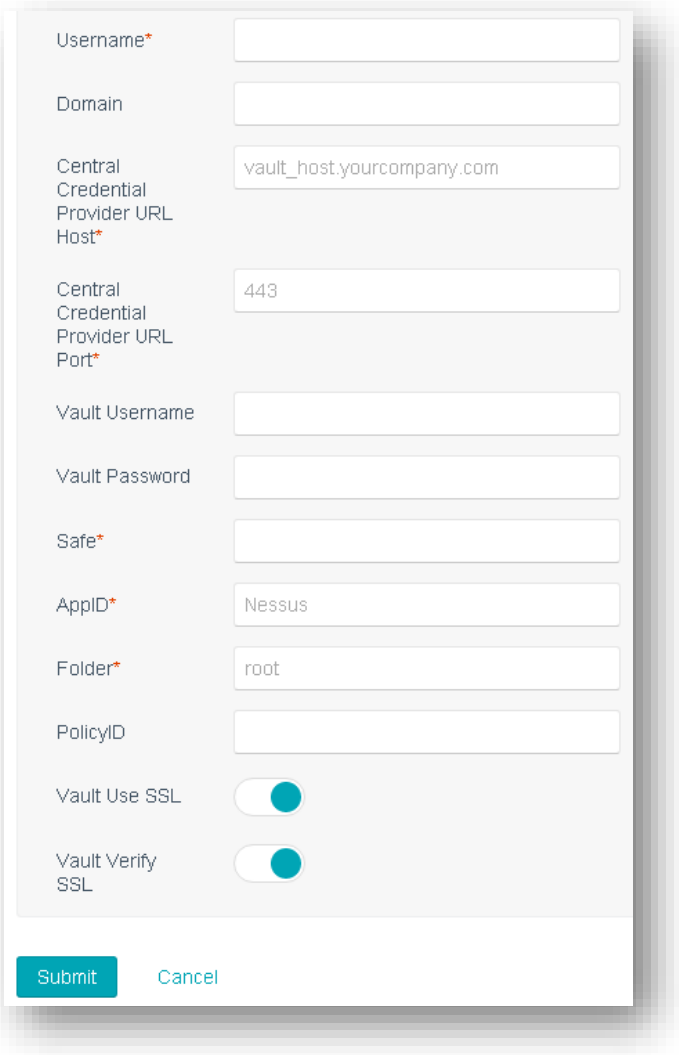
Configuring credentialed network scans using CyberArk's password management solution is a simple process. CyberArk integration with Tenable's solutions is seamless, so credentials are configured similarly to other credentialed network scans.

After logging in to SecurityCenter, navigate to the "Scans" tab and select the "Credentials" option. Click "+Add".

Name the new credential set to be used with CyberArk Enterprise Password Vault (for this example, the credential set is named "CyberArk – Windows"), provide a description (optional), and select a credential type of either "Windows" or "SSH" depending on the operating system of the targets to be scanned. For the following example, "Windows" is selected as the "Type". For the "Authentication Method", select "CyberArk Vault":



After selecting the Authentication Method as “CyberArk Vault”, a new set of options will appear:



The table below contains a description of each option:

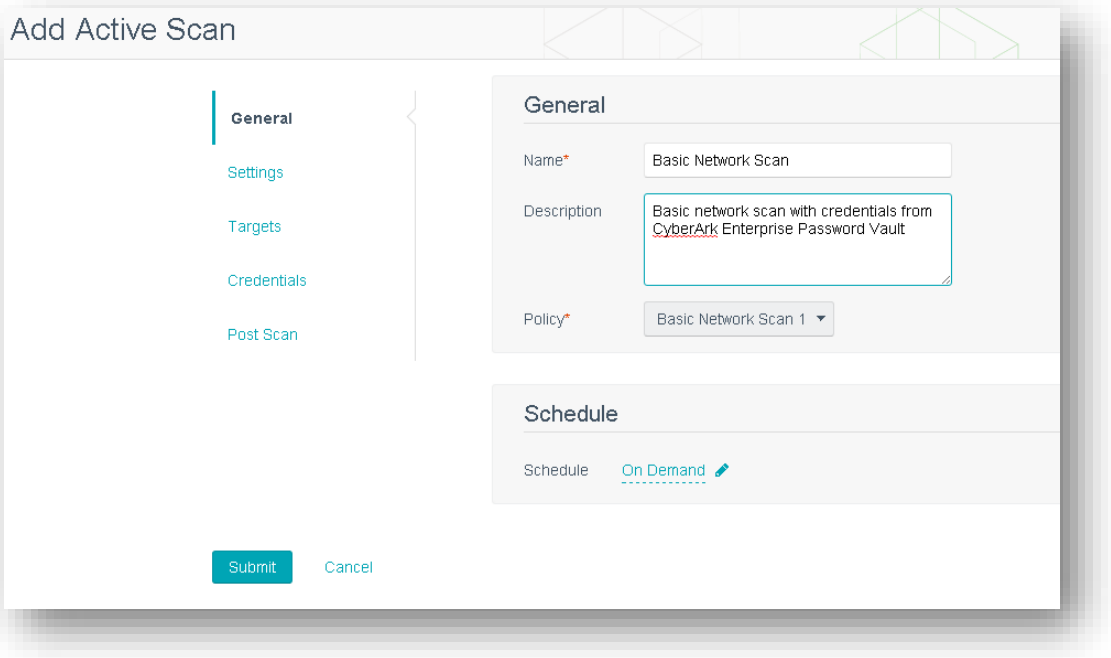
Option	Description
Username	The target system’s username
Domain	This is an optional field if the above username is part of a domain
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS address
Central Credential Provider URL Port	The port on which the CyberArk Central Credential Provider listens
Vault Username (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.

Vault Password (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
AppID	The AppID that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
PolicyID	The PolicyID assigned to the credentials to be retrieved from the CyberArk Central Credential Provider
Vault Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option for secure communication. (Recommended)
Vault Verify SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option to validate the certificate. (Recommended)

Tenable strongly recommends encrypting communication between the Nessus scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to the "Nessus 6.8 User Guide" and the "Central Credential Provider Implementation Guide" located at http://www.cyberark.com (login required).

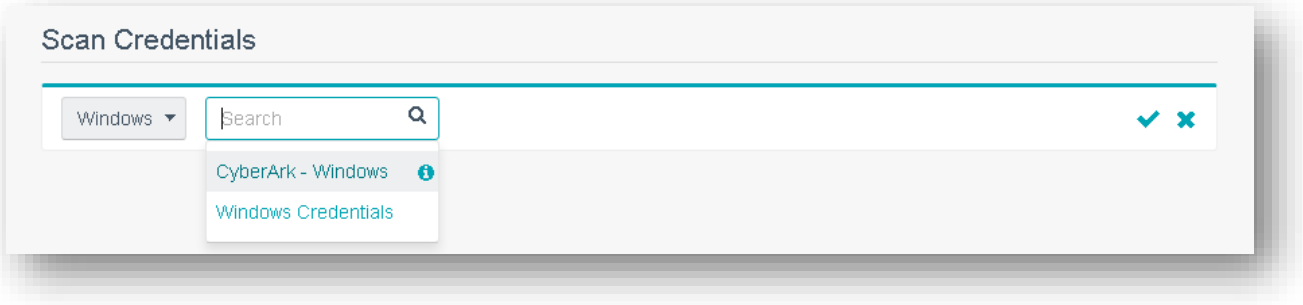
Once the options to reach the CyberArk Enterprise Password Vault are set, click "Submit" to save the changes.

Next, add a scan in SecurityCenter using credentials from CyberArk Enterprise Password Vault. Select Scans > Active Scans, and click "+Add". Under the "General" option, name the new scan, provide a description (optional), and select a scan policy. For an initial scan, it is recommended to set the "Schedule" option to "On Demand" for testing and verification.

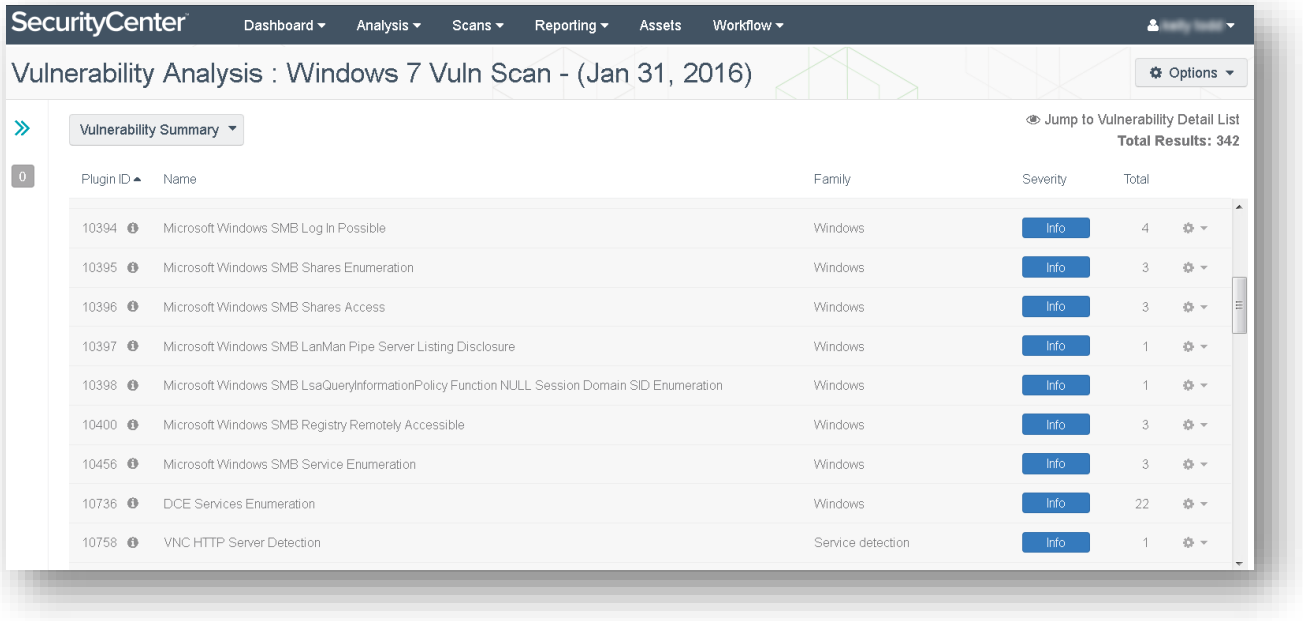


Configure the options under the “Settings” and “Targets” sections that are needed for the scan.

Navigate to the “Credentials” section, and click “+Add credential”. Under “Scan Credentials”, select “Windows” in the first drop-down window and “CyberArk – Windows” for the credential set. Click the checkmark icon to the right to save the scan credentials, and then click “Submit” to save the scan.



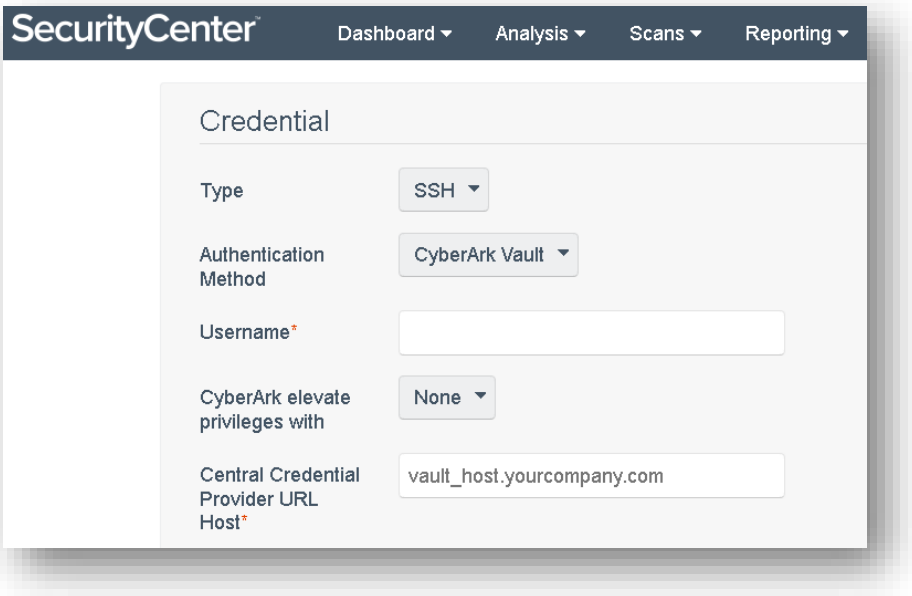
You can verify that the integration is working simply by running the credentialed scan from the “Scans > Active Scans” screen in SecurityCenter and viewing the output of the scan under “Scan Results”. If integration is correctly configured, your results will show successful authentication (see Plugin ID 10394 in the screenshot below). For troubleshooting, check plugin ID 14273 (SSH settings) or 10870 (Login configurations).



For instructions on how to configure CyberArk Enterprise Password Vault to share credentials with Tenable's solutions, please refer to CyberArk's technical product documentation.

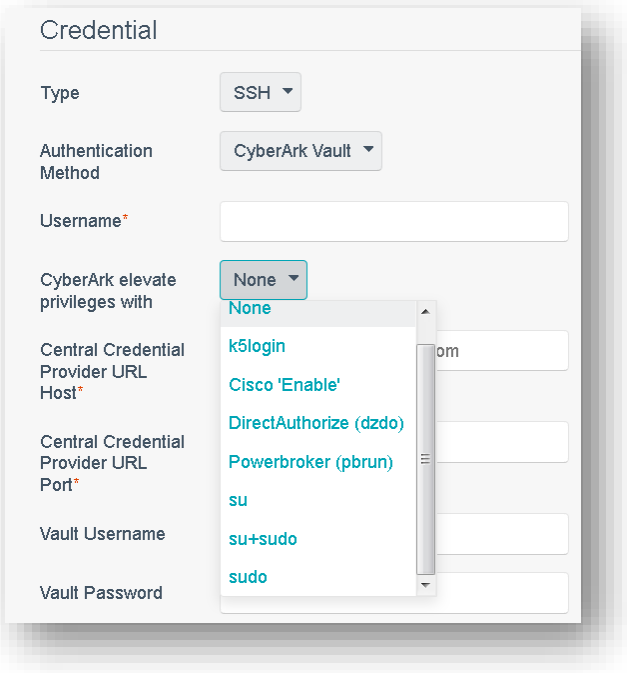
Privilege Escalation with CyberArk Credentials

Tenable supports the use of privilege escalation, such as "su" and "sudo", when using SSH through the CyberArk authentication method. When adding a CyberArk Password Vault credential set, select "SSH" as the "Type" and "CyberArk Vault" as the "Authentication Method":



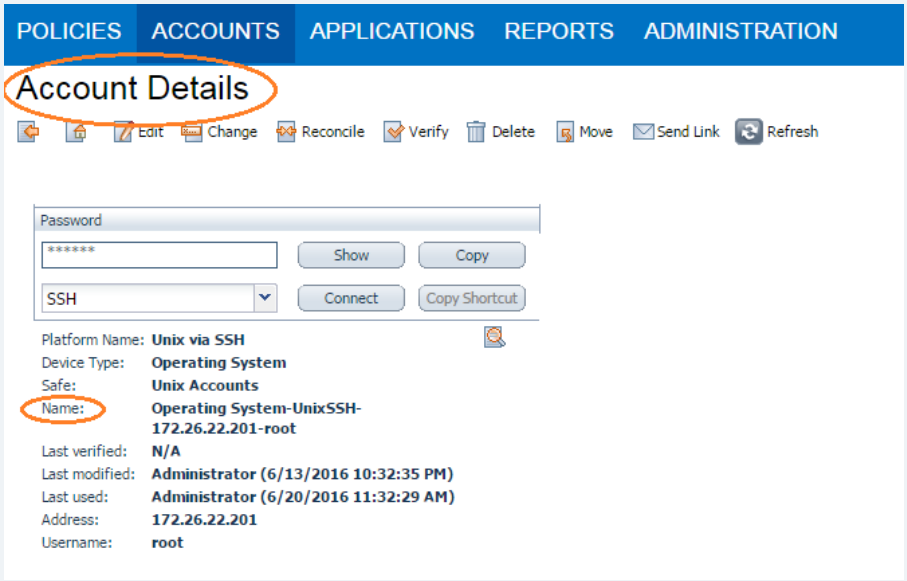
As shown above, an option for "CyberArk elevate privileges with" appears under the "Username" option. Multiple options for privilege escalation are supported, including "su", "su+sudo", and "sudo". For example, if "sudo" is selected, additional fields for "sudo login", "CyberArk Account Details Name", and "Location of sudo (directory) are provided and can be completed to

support authentication and privilege escalation through CyberArk Password Vault. Additional information about all of the supported privilege escalation types and their accompanying fields can be found in the "SecurityCenter CV User Guide".



When asked for a "CyberArk Account Details Name", perform the following steps to obtain the correct value:

1. Log in to CyberArk Password Vault
2. Choose the secret (password) you wish to use
3. Look at the name parameter (such as in the image below) in the Account Details page; this is the value to supply in the "CyberArk Account Details Name" field.



Additional Information about CyberArk Enterprise Password Vault

CyberArk Domain and DNS Support

Tenable's support for CyberArk has been extended to allow Nessus to use its target list to query CyberArk Enterprise Password Vault for the target system's credentials, and Tenable's solutions can now use a flexible system to allow for DNS and domain support. Below is the explanation of the logic used by Nessus for scans using credentials from CyberArk Enterprise Password Vault.

Nessus Priority Scanning for CyberArk

Nessus sets a priority system that allows for flexible querying. The following is set out to describe the order Nessus tries values and the logic behind it.

1. Nessus will query CyberArk with the target value entered into the Nessus or SecurityCenter "Targets" configuration field. For example, if you put a FQDN in the target list, Nessus will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.168.1.1-20, Nessus will try to query using the IP address or IP range of the target system(s) in the CyberArk "Address" value. If the target system uses FQDN and can be resolved, then it will be contacted.

2. If the target value fails, Nessus will then look to see if there is a domain value (for a Windows system). If a domain value is present, Nessus will query CyberArk using the domain value for the address value to attempt to use domain credentials.

3. If the configured target value and the domain value both fail, Nessus will then pull the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Nessus will then query CyberArk using the IP address of the target itself. This is checked against the target value in the configuration to prevent querying CyberArk twice with the same value.

Retrieving Addresses to Scan from CyberArk

Nessus is able to use a feature in CyberArk to pull a list of targets to scan. Below is a description of how to pull the target system values and how to use them.

The following method of target address retrieval cannot be done from the default administrator account. You must create an account that is a member of the PVWAMonitor group to generate the following reports.

1. Click on Report at the top of the CyberArk Enterprise Password Vault web interface.
2. Click "Generate Report" at the top of the Report page.
3. Choose "Privileged Account Inventory".
4. Click "Next".
5. Specify the search parameters for the systems you want to scan.
6. Click "Next".
7. Click "Finish".
8. Download the CSV or XLS report.
9. Confirm the targets for Nessus to scan.
10. Confirm the values can all be resolved by Nessus.

11. Copy the values from the "Target system address" column.
12. Enter the values into Nessus. Either:
    a. Paste the values from addresses into the target list in Nessus.
    b. Paste the values into a file and use a file target list in Nessus.

Debugging CyberArk Issues

To enable debugging when you configure a scan in Nessus, go to Settings->Advanced->Debug Settings and Check “Enable plugin debugging”. If an issue is found, review the results of plugin “Debugging Log Report” (84239). If debug output for the system exists in the debug log, one or more of the following files will be present:

- logins.nasl: Used for Windows credentials. Shows higher level failures in Windows authentication
- logins.nasl~CyberArk: Used to output specific CyberArk- related debug information
- ssh_settings: Used for SSH credentials. Shows higher level failures in SSH authentication
- ssh_settings~CyberArk: Used to output specific CyberArk-related debug information

Example of output:

```
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP004E Password object matching query [Safe=Unix
      Accounts;UserName=credtester;Folder=Root;Address=172.26.22.26] was not found
      (Diagnostic Info: 5). Please check that there is a password object that answers
      your query in the Vault and that both the Provider and the application user
      have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP004E Password object matching query [Safe=Unix
      Accounts;UserName=admin;Folder=Root;Address=172.26.22.26] was not found
      (Diagnostic Info: 5). Please check that there is a password object that answers
      your query in the Vault and that both the Provider and the application user
      have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP229E Too many password objects matching query [Safe=Unix
      Accounts;UserName=admin;Folder=Root] were found: (Safe=Unix
      Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-172.26.22.205-
      admin, Safe=Unix Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-
      172.26.22.66-admin and more. See trace log for more information). (Diagnostic
      Info: 41)
```

The first section in this document (Nessus Priority Scanning for CyberArk) shows that a single system may send multiple requests that fail before finding a successful one. Because of this, the output to the debugging log may not show an issue with the scan, but it can be used as an audit trail if there is an issue. To address issues using the log, look for the parameters to match the intended query and see what error output was reported for that query. For example, if you intended to scan target 172.26.22.66 using parameters of (`Safe=Unix Accounts;UserName=admin;Folder=Root`), then you could discern from the log above that the reason the scan failed is because there were too many matching items to this query, and therefore no results were returned.

About Tenable Network Security

Tenable Network Security 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 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses 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.