QUICK SHEET

EXCLUSION LISTS TENABLE VULNERABILITY MANAGEMENT

Overview

This document describes exclusion lists in Tenable Vulnerability Management, and how to use them to designate the assets that should not be scanned during a vulnerability management scan.

Benefits Of An Exclusion List

Exclusions lists can help your organization to:

1. Exclude resources from scans that may affect performance, operations, or availability.
2. Configure a scan to target only a specific area of your network.
3. Prevent duplication of assets with multiple NICs.
4. Restrict the scanning of specific hosts based on a selected schedule. For example, you can avoid scanning specific assets during peak business hours, or pre-planned maintenance windows

How To Create An Exclusion List In Tenable Vulnerability Management

1. In the upper-left corner, click the ☰ button. The left navigation pane appears.
2. In the left navigation, click Settings. The Settings page appears.
3. Click the Exclusions tile. The Exclusions page appears, and displays the exclusions table.
4. In the upper right corner of the page, click the +Create Exclusions button. The Create an Exclusion page appears.
5. Set the Exclusions settings.
6. Click Save. Tenable.io saves the exclusion.

Learn how to create, edit, import, export, or delete an exclusion list in the Tenable Vulnerability Management User Guide.

WHAT IS AN EXCLUSION LIST?

An exclusions list designates specific assets that you do not want your vulnerability management solution to scan.

ADDITIONAL RESOURCES

Tenable Vulnerability Management User Guide: Exclusions

Tenable Vulnerability Management Scanning Best Practices

Exclusion List Recommendations

1. Always assess the risk of removing an asset from vulnerability scans. Ensure you track the data on the asset, as well as the controls that are in place to protect the asset, and the reason it is excluded.
2. Exclusion lists are technically a protection gap. Always consider additional mitigations when defining exclusions.
3. Run periodic reports of all the assets that are excluded from vulnerability scans. Ensure you track the date and reason for the exclusion. Periodically verify that the asset should remain excluded.
4. Avoid defining proactive exclusions. For example, do not exclude something just because you think it might be a problem in the future.

Using An Exclusion List To Remove Duplicate Assets

When scanning an asset that has multiple network interface controllers (NICs), there are circumstances that could change the way an asset is counted, causing each NIC to be counted as a separate asset. For example, a non-credentialed scan may not collect enough data to confidently merge the multiple NICs into one asset.

To use exclusion lists to remove duplicate assets caused by counting each NIC on the asset as a separate asset you should:

1. Scan the asset(s) with credentials to uniquely identify assets and deduplicate multiple NICs.
2. Exclude any extra IP addresses for an asset if they do not provide reporting value. Some customers may use network scanning to pentest an asset, and visibility into different vulnerabilities or open ports on a different network interface may provide insight and value. To correct any reporting accuracy issues, delete the asset using the UI or API.
3. To remove duplicates that were deleted, enable Asset Age Out to mirror your scan schedule.