Tenable Scan Strategy
Tenable Professional Services

Last Revised: December 06, 2018

Table of Contents

Introduction 3

Network Assessment 4

Network Topology 5

Scan Target Identification 7

Customer Requirements 9

Tenable Resource Allocation 10

Scanning Methodology 11

Active Scan Schedule Options 12

Scan Policy Configuration 13

Host Discovery 14

Vulnerability Scan 16

External Vulnerability Scan 17

Compliance Checks 18

Scan Policy Settings 19

Related Documents 22

Introduction

The purpose of this document is to describe scan strategies that Tenable Professional Services Consultants recommend for their various customer environments. This document focuses on Tenable.io and SecurityCenter active scans that utilize Nessus.

Network Assessment

The scan strategy that Tenable™ recommends depends on several factors:

- Network Topology
- Scan Target Identification
- Customer Requirements
- Tenable Resource Allocation

Network Topology

The organization's network topology determines Nessus scanner placement and Scan Zone configuration.

- **Flat Network**
  - The Nessus scanner(s) can directly access all targets without firewall or other network device configuration.
  - One or more scanners can be configured to scan network targets in a single Scanner Group/Scan Zone.
- **Segmented Network**
  - If a network is behind a firewall or is VLAN separated, such as a DMZ, the Nessus Scanner may not be able to successfully scan its target.
  - A Nessus Scanner should be placed in each network segment.
  - Nessus requires port TCP/443 to communicate with Tenable.io and TCP/8834 for SecurityCenter.
  - If a Nessus Scanner cannot be placed in the network segments, then firewall rules must be configured so the scanner can reach all intended target ports and protocols.
- **Geographically Separated**
  - To minimize network bandwidth utilization and potentially decrease scan duration, consider placing a Nessus Scanner at geographically separated sites.
- **Operational Technology (OT)** (e.g., ICS/SCADA, or other sensitive networks)
  - Nessus Network Monitor is highly recommended.
  - If Nessus Scanners are used, first test in a non-production environment.
- Combination of the previous examples

Scanner Groups (Tenable.io) / Scan Zones (SecurityCenter)

Example Scanner Groups/ Scan Zones:

- Default/Primary
  - Flat network
  - Nessus can reach all targets
- <Site> or <DMZ> Zone(s)
  - Scanner at geographically separated site
  - Scanner in DMZ
- Public
  - The Tenable.io cloud-based scanner is in the External Nets scan zone that contains public-facing IP ranges.

Reference	Location
Tenable.io Scanner Groups	https://docs.tenable.com/cloud/Content/Scans/AboutScannerGroups.htm
SecurityCenter Scan Zones	https://docs.tenable.com/sccv/Content/ScanZones.htm

Scan Target Identification

Scan strategy depends on the scan targets. A list of targets, such as IP addresses, ranges, subnets, DNS names, can be used to create Tenable.io Target Groups or SecurityCenter Static Asset Lists.

- Operating Systems (Windows, Linux, macOS)
    - OS type, quantity of each, and use of credentials, will impact the scan duration.
- Application (DB, vCenter, etc)
    - Scan duration varies based on application server type. Conduct a scan of a sample of systems to estimate scan duration and target system behavior.
- Network Devices (switch, router, firewall, etc)
    - Credentialed scans are typically the fastest and will provide the most thorough vulnerability scan results.
- Public External
    - Use a Nessus Scanner that is able to communicate to the target public IP address. The Scanner can be cloud-based or internal.
        - Cloud-based scanner examples:
            - Tenable.io Scanner
            - AWS BYOL scanner
            - Azure
            - Nessus Scanner installed on Linux/UNIX/Windows virtual instance.
- Quantity of targets
    - To reduce the scan duration of a large number of targets:
        - Add additional scanners
        - Pool scanners in a Scanner Group / Scan Zone
        - Scan by network segment / VLAN
        - Adjust scan policy performance settings

- Sensitive hosts
    - Create an Advanced Network Scan policy to finely tune each policy setting and monitor the effect on the target.
    - Nessus Agent installed on a target will rely on local target resources.
    - Nessus Network Monitor can passively listen to the target's network traffic so its ports are not scanned.
- Transient Devices, e.g., laptops
    - Nessus Agents scans
    - If Nessus Agentsare not an option, scan transient device subnets when users are most likely to be on the network, such as during business hours.
- AWS Machine Instances
    - Utilize the AWS Connector feature in Tenable.io and deploy the Nessus Pre-Authenticated Scanner found in the AWS marketplace.

Customer Requirements

Each customer has various requirements that can influence scan strategy.

- Software patch and scan cadence
  - Many organizations have configuration management processes in place that define patch schedules.
- Regulation and compliance
  - NIST, HIPAA, NERC CIP, etc.
  - Local requirements
- Change management process
  - If prior approval is required to conduct scans, create a baseline scan policy and propose a scan schedule that can be automated and predictable.
- Maintenance windows
  - If active scanning can only occur within a specific time window, e.g., after business hours, adapt the scan strategy to adapt to the restrictions.
    - Add additional Nessus Scanners and pool them in a Scanner Group / Scan Zone.
    - Increase the scan policy performance settings, such as Max hosts per scan.
    - Set Active Scans to Rollover and launch at the same time on the following day.

Tenable Resource Allocation

Depending on scan policy settings, the Nessus scanner minimum hardware requirements may not be sufficient to meet scan frequency or duration goals.

Nessus Scanner

Tenable recommends using a Linux-based operating systems. If your organization has an established Linux team, use their recommended RHEL image or CentOS build. If Linux expertise is limited, use Tenable virtual appliance 4.7, which is a hardened CentOS 6 SELinux build.

A Windows-based Nessus scanner must have its scan policy performance (max number of concurrent TCP sessions per scan) throttled to ensure accuracy. Refer to the Advanced Settings in the Nessus guide.

Recommended Nessus hardware settings: 4 CPU cores, 8 GB RAM, and 30 GB storage. Scan policy performance settings will impact CPU and RAM utilization, so monitor Nessus scanner resource and adjust as necessary.

SecurityCenter

Ensure SecurityCenter hardware resources meet minimum requirements for in-scope IPs. Refer to the SecurityCenter Hardware Requirements.

Tenable.io

Tenable maintains Tenable.io hardware resources.

Scanning Methodology

- Active Scan Schedule Options
- Scan Policy Configuration
- Scan Policy Settings

Active Scan Schedule Options

You can choose from the following active scan scheduling options to match your scan cadence.

- **On-demand**: Manually launched by the user.
- **Scheduled**: Scheduled scans can be set to automatically launch daily, weekly, or monthly.
- **Dependent**: The active scan will launch when a scheduled parent scan completes. Dependent scans can be daisy-chained to other dependent scans.

Scan Policy Configuration

Use the following scan policies to fit your desired scan strategy:

- Host Discovery
- Vulnerability Scanning
- External Vulnerability Scan
- Compliance Checks

Host Discovery

Using the **Advanced Network Scan** policy for host discovery, you can configure the policy to meet your scanner's hardware resources for speed, accuracy, and thoroughness, while also choosing only plugins that do not count against the license. Refer to Table 1 for individual Host Discovery plugins.

Notable policy setting changes include:

- **Advanced > Performance > Max simultaneous hosts per scan**
    - SecurityCenter: 128
        - SecurityCenter scans in multiples of 8 hosts.
    - Tenable.io: 100
- **Port Scanning > Network Port Scanners**
    - SYN
        - For speed, choose only SYN. Leave TCP and UDP disabled. If you are only attempting to find hosts that are alive, then disable SYN as well and just rely on ping methods.

Discovery Plugins

Go to **Plugins > Disable All** and then manually select the desired plugins from the table below. The plugins in the table do not count against your license count.

Note: The Port Scanners plugin family is not listed in the interface; the plugins are controlled by toggle switches in the Host Discovery and Port Scanning policy categories.

Plugin ID	Name	Family
45590	Common Platform Enumeration	General
54615	Device Type	General
12053	Host Fully Qualified Domain Name (FQDN)	General
11936	OS Identification	General
10287	Traceroute Information	General
22964	Service Detection	Service Detection

11933	Do not scan printers	Settings
87413	Host Tagging	Settings
19506	Nessus Scan Information	Settings
33812	Port scanners settings	Settings
33813	Port scanner dependency	Settings
10180	Ping the remote host	Port scanners
10335	Nessus TCP scanner	Port scanners
11219	Nessus SYN scanner	Port scanners
14274	Netstat Portscanner (SSH)	Port scanners
14272	Netstat Portscanner (WMI)	Port scanners
34220	Nessus SNMP Scanner	Port scanners
34277	Nessus UDP Scanner	Port scanners

Vulnerability Scan

A **Basic Network Scan** template is suitable for any host. All plugins are enabled in this policy.

Using the **Advanced Network Scan** policy for vulnerability scanning allows you to configure the policy to meet your scanner's hardware resources for speed, accuracy, and thoroughness.

Notable policy setting changes include:

- **Advanced > Performance > Max simultaneous hosts per scan**
  - 64
    - SecurityCenter scans in "chunks" of 8 hosts.
  - This is on the high end and Nessus scanners and network utilization should be monitored.
  - Lower this setting if resources are impacted.

    > **Note:** Scan duration is increased, which may be to be factored in for organizations with blackout windows.
- **Plugins > Enable All**
  - Many plugin families will not launch if other policy settings override them.
  - **<software> Local Security Checks** family plugins will only run if valid credentials for that software platform are entered in the active scan.

External Vulnerability Scan

When scanning external (internet-facing) hosts, external firewalls or other boundary protection devices may block the scan's host discovery ping packets. If you disable **Ping the Remote Host** in the scan policy, port scanning is forced to run against every target IP in the active scan regardless if it is alive or dead.

- **Host Discovery > Ping the Remote Host**
    - Disable

Additional notable policy setting changes include:

- **Port Scanning > Ports > Port scan range**
    - 1-65535 (or all)
        - This port range will perform an assessment that mimics what an outside attacker would see. Using this policy, you will discover more public-facing servers than before and because the external vulnerability scan policy is reasonably quick, it may eliminate the need for separate external host discovery scans.
- **Plugins > Enable All**

Compliance Checks

For information on compliance checks, see the following documents:

- Nessus User Guide
- Nessus Compliance Checks Reference
- Nessus Compliance Checks PDF

Scan Policy Settings

The table below describes scan policy settings to adjust to meet an organization's scan strategy.

Policy Location	Setting Name	Host Discovery	Vulnerability Scan Policy	Full Port Scan Policy	Comments
Advanced > Performance	Network timeout (in seconds)	5	5	2	Increased scan speed for the Full Port Scan policy
	Max simultaneous checks per host	5	5	5	2 or 1 for old boxes max is 15 hard-coded
	Max simultaneous hosts per scan	96	64	96	64 hosts if Nessus with 8GB RAM 96 for host discovery Lower for slow links Keep divisible by 8
	Max number of concurrent TCP sessions per host	unlimited	unlimited	unlimited	Set to 19 to increase Windows-based Nessus Scanner accuracy.
Host Discovery	Ping the Remote Host	enable	enable	disable	Disabled in the full port scan policy to force a TCP/UDP scan.

Port Scanning > Ports	Port scan range	default	default	1-65535	Full Port Scan policy will scan all ports instead of the SC default list of 4,790 common ports.
	UDP	disable	disable	enable	Enable UDP scanning for those targets that require a Full Port scan.
Service Discovery > General Settings	Search for SSL/TLS services	disable	enable	disable	Enable for Vulnerability scan to scan for additional services.
Windows > Enumerate Local Users	Start UID - End UID	disable	1 - 1200	default	Gather information on local Windows accounts with credentialed scans.
Report > Processing	Show missing patches that have been superseded	disable	disable	disable	Reduces scan result clutter. Allows system owners to focus on latest patches.
Report > Output	Display hosts that respond to ping	enable	enable	enable	Provides more details in scan results.
Authentication > Windows	Start the Remote Registry service during the scan	disable	enable	enable	Increases scan result accuracy.

	Enable administrative shares during the scan	disable	enable	enable	Increases scan result accuracy.
Plugins	Plugin Family	User Defined	Enable All	Enable All	Increase scan result accuracy.

Note: Scan policy settings are described in the Nessus User Guide.

Related Documents

Document Name
SecurityCenter 5 User Guide
Nessus 7 User Guide
Nessus 6 User Guide
Tenable.io User Guide
Nessus Network Monitor 5 User Guide
Nessus Compliance Checks Reference Guide
Tenable Appliance 4 User Guide