Configuring a Malware Detection and Forensics SecurityCenter Scan

May 2, 2016
(Revision 3)
Table of Contents

Introduction .................................................................................................................................................. 3
Add Policy .................................................................................................................................................. 3
  Basic Settings ....................................................................................................................................... 3
  Enable Plugins ...................................................................................................................................... 5
Brute Force: General Settings .................................................................................................................. 7
Windows: Malware Files ......................................................................................................................... 8
  Expanded Malware Scanning .................................................................................................................. 8
Report: Output .......................................................................................................................................... 9
Authentication: Windows .......................................................................................................................... 10
Add Credential .......................................................................................................................................... 11
Add Scan .................................................................................................................................................. 12
  Policy and Credential ............................................................................................................................ 14
  Settings: Advanced ............................................................................................................................... 15
Add Dashboard .......................................................................................................................................... 16
  Choose the Monitoring Related Dashboards and Components ............................................................... 16
  Locate the Indicators Dashboard ........................................................................................................... 17
  Review the Details of the Indicators Dashboard .................................................................................... 18
  Wait for the Dashboard to be Added ....................................................................................................... 19
  Wait for the Dashboard Components to Update .................................................................................... 20
Add Asset .................................................................................................................................................. 21
  Choose to Add an Asset List .................................................................................................................. 21
  Create Dynamic Asset List .................................................................................................................... 21
  Verify Asset List Created Successfully .................................................................................................. 22
Vulnerabilities (Cumulative View) ........................................................................................................... 22
  Look at the Cumulative View of Results ............................................................................................... 23
  Filter on the Executable Code File Name that has been Identified as Malware ..................................... 24
  Review the List of Plugin Results that Contain References to the Malware ........................................ 24
  Change the View to “IP Summary” ......................................................................................................... 25
ThreatLists and Watches: ....................................................................................................................... 25
About Tenable Network Security .............................................................................................................. 25
Introduction

This document offers a suggested approach to configure a malware detection and forensics credentialed scan in Tenable SecurityCenter™ that will work in most environments without modification. It also offers suggested steps to configure additional objects in SecurityCenter to help with interpreting scan results.

A basic understanding of the SecurityCenter GUI to find the menu options for adding objects such as repositories, policies, scans, asset lists, and performing queries is highly recommended. This document is not intended as a replacement for official Tenable training or documentation. For more details on adding objects through SecurityCenter, please refer to the SecurityCenter User Guide.

When following the configuration steps, please note that some settings may be set correctly by default, depending on the SecurityCenter version and plugin versions being used. Screenshots are provided below configuration steps to help avoid any confusion.

Add Policy

Basic Settings

1. As a Security Manager user, add an Advanced Scan policy.
2. Under “Network Port Scanners”, ensure “TCP” is disabled and enable “SYN”, “WMI (netstat)”, and “Ping Host”.

3. Set the “Port scan range” to “139,445”.
Enable Plugins

Enable the following Nessus® plugins:

Authentication Diagnostic Help
- 10919 Open Port Re-check
- 19506 Nessus Scan Information
- 21745 Authentication Failure - Local Checks Not Run
- 10394 Microsoft Windows SMB Log In Possible
- 10395 Microsoft Windows SMB Shares Enumeration
- 10400 Microsoft Windows SMB Registry Remotely Accessible
- 24269 Windows Management Instrumentation (WMI) Available
- 26917 Microsoft Windows SMB Registry: Nessus Cannot Access the Windows Registry

Host Identification
- 10150 Windows NetBIOS / SMB Remote Host Information Disclosure
- 12053 Host Fully Qualified Domain Name (FQDN) Resolution
- 45590 Common Platform Enumeration (CPE)
- 55472 Device Hostname
- 35716 Ethernet Card Manufacturer Detection

Botnet
- 52669 Host is Listed in Known Bot Database
- 58429 DNS Server Listed in Known Bot Database
- 58430 Active Outbound Connection to Host Listed in Known Bot Database
- 59713 Active Inbound Connection From Host Listed in Known Bot Database

Malicious Processes
- 59275 Malicious Process Detection
- 59641 Malicious Process Detection: Potentially Unwanted Software
- 64687 Malicious Process Detection: APT1 Software Running
- 64788 Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate
- 65548 Malicious Process Detection: User Defined Malware Running

Windows Processes
- 70329 Window Process Information
- 70331 Window Process Module Information

Autoruns
- 70613 Microsoft Windows AutoRuns LSA Providers
- 70614 Microsoft Windows AutoRuns Appinit DLLs
- 70615 Microsoft Windows AutoRuns Boot Execute
- 70616 Microsoft Windows AutoRuns Codecs
- 70617 Microsoft Windows AutoRuns Explorer
- 70618 Microsoft Windows AutoRuns Registry Hijack Possible Locations
- 70619 Microsoft Windows AutoRuns Internet Explorer
- 70620 Microsoft Windows AutoRuns Known DLLs
- 70621 Microsoft Windows AutoRuns Logon
- 70622 Microsoft Windows AutoRuns Network Providers
- 70623 Microsoft Windows AutoRuns Print Monitor
- 70624 Microsoft Windows AutoRuns Report
- 70625 Microsoft Windows AutoRuns Scheduled Tasks
- 70626 Microsoft Windows AutoRuns Services and Drivers
- 70627 Microsoft Windows AutoRuns Setup
- 70628 Microsoft Windows AutoRuns Unique Entries
- 70629 Microsoft Windows AutoRuns Winlogon
- 70630 Microsoft Windows AutoRuns Winsock Provider
- 70628 Microsoft Windows AutoRuns Scheduled Tasks

**Reputation**

- 70767 Reputation of Windows Executables: Known Process(es)
- 70768 Reputation of Windows Executables: Unknown Process(es)
- 70943 Reputation of Windows Executables: Never seen process(es)
- 71262 Reputation of Linux Executables: Never seen process(es)
- 71264 Reputation of Mac OS X Executables: Never seen process(es)
Brute Force: General Settings

Enable "Only use credentials provided by the user".
Windows: Malware Files

Upload custom MD5 hashes, if any. Skip this step if you do not have any MD5 hashes to provide.

Expanded Malware Scanning

With Nessus 6.6, malicious file detection is expanded to now scan directories of files on disk. When specific directories you want to scan are entered into a scan policy, Nessus will report any malware or suspicious files discovered in the scan.
Enable "Display hosts that respond to ping".
Authentication: Windows

1. Enable “Start the Remote Registry service during the scan”.

2. Enable “Enable administrative shares during the scan”.

![SecurityCenter interface showing Windows authentication settings](image-url)
Add Credential

Consider setting up a dedicated Active Directory domain user account for credentialed scanning. Test the account in a lab environment or on one or two hosts to ensure the account has the correct permissions.
Add Scan

Enter a scan name per your company naming policy. Include a description that informs users about the purpose of the scan.

Create the scan with its schedule set to "On Demand". Scans can be launched on demand, or scheduled to launch automatically at a specified time.
Set the targets for the scan under "Targets" using an asset list, IP address(es), IP range, or CIDR block.
Policy and Credential

1. Use the scan policy created in the "Add Policy" section for the "Policy" selection.

2. Use the Windows credentials entered in the "Add Credential" section in the available "Windows Credential" selections.
**Settings: Advanced**

1. Enable "Track hosts which have been issued new IP address (e.g. DHCP)".

2. Enable "Immediately remove vulnerabilities from scanned hosts that do not reply".
Add Dashboard

Use the Indicators dashboard that Tenable provides as a starting point to experiment with the visual alerting of malware detection results. Please note that the Indicators dashboard covers far more than the results returned by a standard malware audit.

Choose the Monitoring Related Dashboards and Components

Click the "Monitoring" panel to view the selection of monitoring related dashboards and components.
Locate the Indicators Dashboard

Filter the selection by using the word “Indicators” and click the “Indicators” dashboard.
Review the Details of the Indicators Dashboard

Review the Indicator dashboard details and click "Add It Now".
Wait for the Dashboard to be Added

Click "Add" to add the dashboard to SecurityCenter, which will notify when the dashboard has successfully been added.
Wait for the Dashboard Components to Update

In the screenshot below, a malware detection and forensics audit has already been run and the results, as highlighted by the dashboard, contain malicious process detection results.
Add Asset

We can build a dynamic asset list to filter in dashboards, reports, alerts, and querying on those hosts identified as running a Windows operating system but did not have credentialed checks executed. The majority of malware detection and forensic checks are credentialed checks.

Choose to Add an Asset List

Create Dynamic Asset List

1. Click "Dynamic".

2. Enter the name and description.

3. Ensure "All of the following are true" is selected, and not "Any of the following are true".

4. Create two clauses: the first, Plugin Text, containing the pattern "Credentialed checks: no:" where the plugin ID is 19506; the second, Operating System, containing the pattern "windows" (omitting the quotation marks in each entry).

5. Click "Submit" when done.
Verify Asset List Created Successfully

Ensure that a non-zero number is shown for the number of systems scanned for the new dynamic asset list.

Vulnerabilities (Cumulative View)

The malware and botnet detection plugins follow the general policy of indicating an issue when a result has a severity rating of low, medium, high, or critical. The Indicators dashboard highlights these types of issues. We could also set up alerts and filter on the new malware repository for any plugin result with a severity rating of low, medium, high, or critical. A query can be filtered in the same fashion, as can a SecurityCenter API query.
However, in addition to potentially having malware detection plugin results, we also have a rich dataset of forensics information in the form of Windows process and auto-run plugin results. Through reviewing the results of plugin 70330, "Window Process Unique Process Name" and plugin 70768, "Reputation of Windows Executables: Unknown Process(es)" and forensic investigation, we may find some executable code that has not been flagged by the malware detection plugins but actually is malware. We could upload hashes (see “Windows: Malware Files”), and perform a new enterprise malware scan to determine how widespread a newly discovered malware infection is, or we could turn to the forensic plugin results to determine the scope of an infection.

The steps that follow offer a method for a quick search for executable code that has been identified as malware; however, there are many ways to use the filters in SecurityCenter, which are available across dashboards, reporting, alerting, and the API.

**Look at the Cumulative View of Results**
Filter on the Executable Code File Name that has been Identified as Malware

Review the List of Plugin Results that Contain References to the Malware

We could drill in further to see the individual plugin report details for the context of the malware matches.
Change the View to “IP Summary”

If we change the view to “IP Summary”, we can see the list of hosts that have plugin results with matches for the malware.

ThreatLists and Watches:

SecurityCenter integrates multiple threat intelligence feeds focusing on three areas:

- Passive Web Traffic Analysis
- Malicious Process Detection
- Botnet Detection based on IP reputation

Dashboards check against these areas and display real-time data of the results. Administrators can also leverage custom whitelists and blacklists when customizing dashboard output.

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.