



Validating Anti-Virus Software with Tenable Solutions

June 9, 2016



Table of Contents

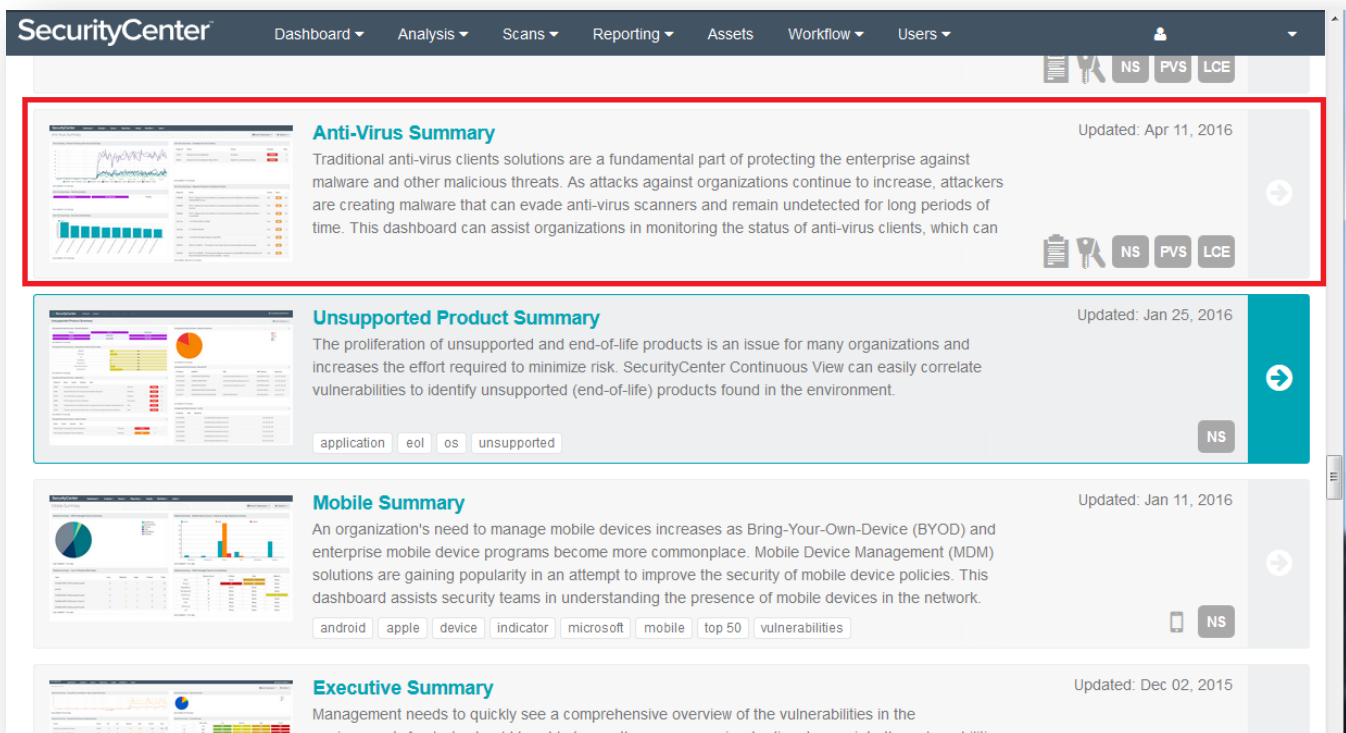
Introduction	3
Checking the Health of Anti-Virus Systems	3
Creating an Active Scan in SecurityCenter	7
Creating an Active Scan in Nessus	10
Conclusion	14
About Tenable Network Security	14

Introduction

Over time, malware has evolved from the boot and file infectors that were initially discovered starting in 1986. Modern malware is less concerned about simple replication and more about surviving and communicating. To this end, one of the most successful strategies used by malware is to disable host security products, including anti-virus (AV) software. While some anti-virus software has its own control panel for managing host security, reports from the software can be spoofed back to end users and system administrators. In most cases, the report states that the software is installed, but malware has been known to disable AV software while leaving one file or registry entry untouched, so the parent control panel still reports the software as being functional without it actually being operational. Tenable SecurityCenter Continuous View™ (CV) and Nessus® have specific checks to detect both anti-virus products and signature update traffic. This provides Tenable's customers with a safety net of checks (and double checks) to ensure that their protection is complete and functional.

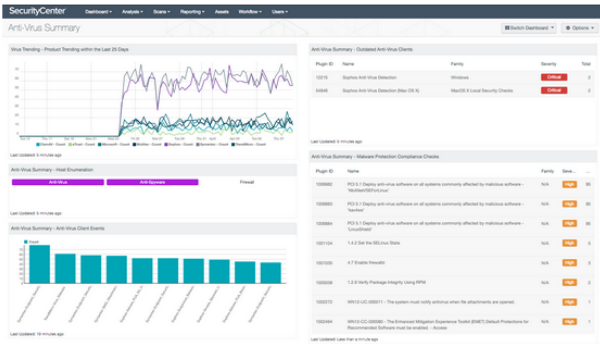
Checking the Health of Anti-Virus Systems

Tenable SecurityCenter CV allows you to evaluate vulnerability data gathered from multiple active and passive sensors distributed across your enterprise. There are no special steps needed to enable these checks; the anti-virus Summary dashboard is part of the basic SecurityCenter installation under the name of "Anti-Virus Summary", and will display active and passive checks for AV client detection.



The screenshot displays the SecurityCenter dashboard interface. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The main content area features several summary dashboards. The 'Anti-Virus Summary' dashboard is highlighted with a red border. It includes a line graph, a table of data, and a description: 'Traditional anti-virus clients solutions are a fundamental part of protecting the enterprise against malware and other malicious threats. As attacks against organizations continue to increase, attackers are creating malware that can evade anti-virus scanners and remain undetected for long periods of time. This dashboard can assist organizations in monitoring the status of anti-virus clients, which can'. The dashboard is updated on Apr 11, 2016. Below it are the 'Unsupported Product Summary' (updated Jan 25, 2016), 'Mobile Summary' (updated Jan 11, 2016), and 'Executive Summary' (updated Dec 02, 2015). Each dashboard includes a brief description and a set of filters.

Anti-Virus Summary



Components

- ✓ Virus Trending - Product Trending within the Last 25 Days
- ☐ Anti-Virus Summary - Outdated Anti-Virus Clients
- ☐ Anti-Virus Summary - Host Enumeration
- ☐ Anti-Virus Summary - Malware Protection Compliance Checks
- ☐ Anti-Virus Summary - Anti-Virus Client Events

Focus

Targets: All Systems

Schedule

Schedule* Every day at 11:24 -04:00

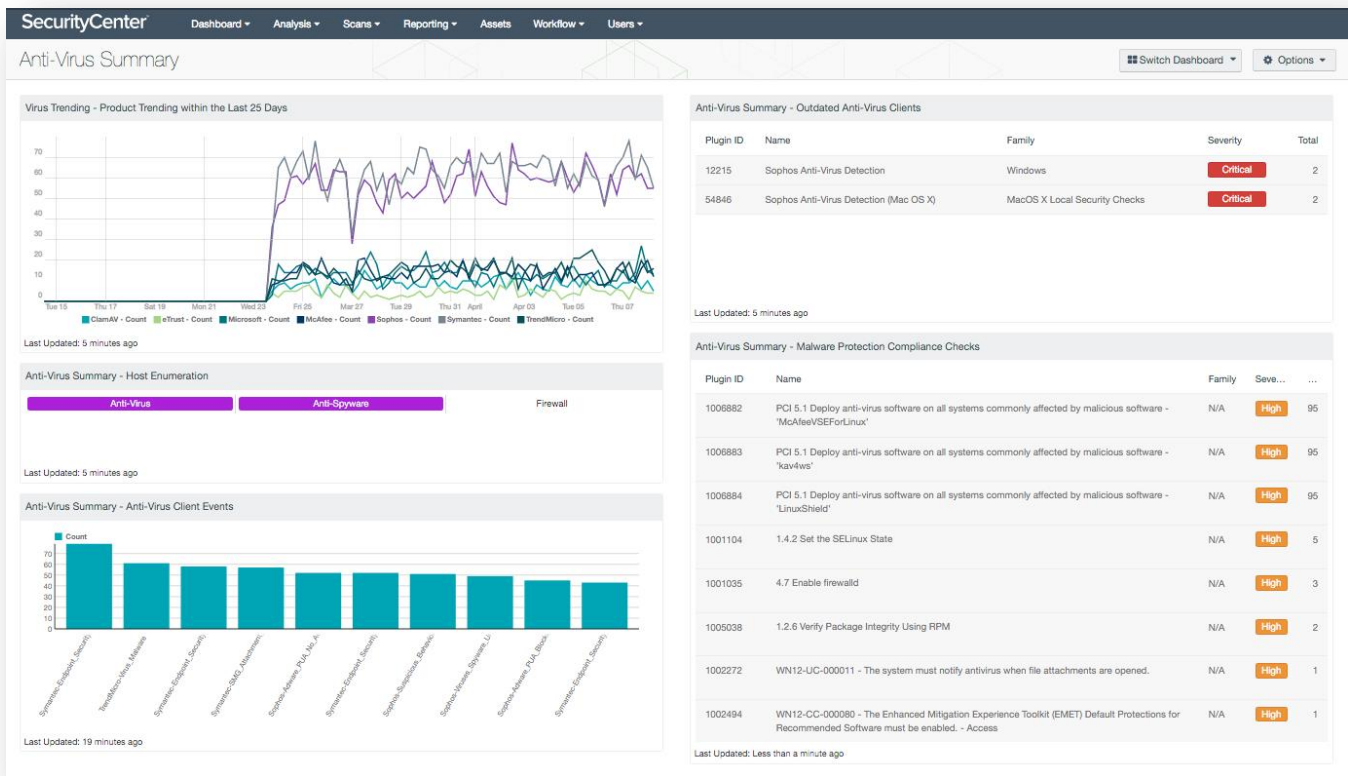
Add Cancel

Description

Many organizations frequently use managed anti-virus solutions to assist with remotely administering scans and pushing updates out to clients. However, issues with anti-virus clients can be the result of misconfigured policies or loss of communication between the client and anti-virus server. Although managed anti-virus solutions can provide greater visibility and control over clients, many organizations do not apply additional controls needed to protect systems from potential attacks. Information presented within this dashboard will allow organizations to quickly identify and remediate issues from AV solutions. Nessus utilizes several WMI-based checks to determine if anti-virus, anti-spyware, and desktop firewalls are installed and have been updated to the latest release on Windows systems. The Log Correlation Engine (LCE) monitors activity from anti-virus clients, which can alert analysts to potential malware infections or other malicious activity. Several components include event

Category: Discovery & Detection
 Created: Apr 12, 2016 00:57
 Updated: Apr 12, 2016 00:57
 Requirements: nessus 6.5.6 ice 4.8.0 pvs 5.0.0 complianceData localChecks
 Tags: None

Adding this dashboard will provide results similar to the following:



At the time of this writing, SecurityCenter CV actively audits networks for the following:

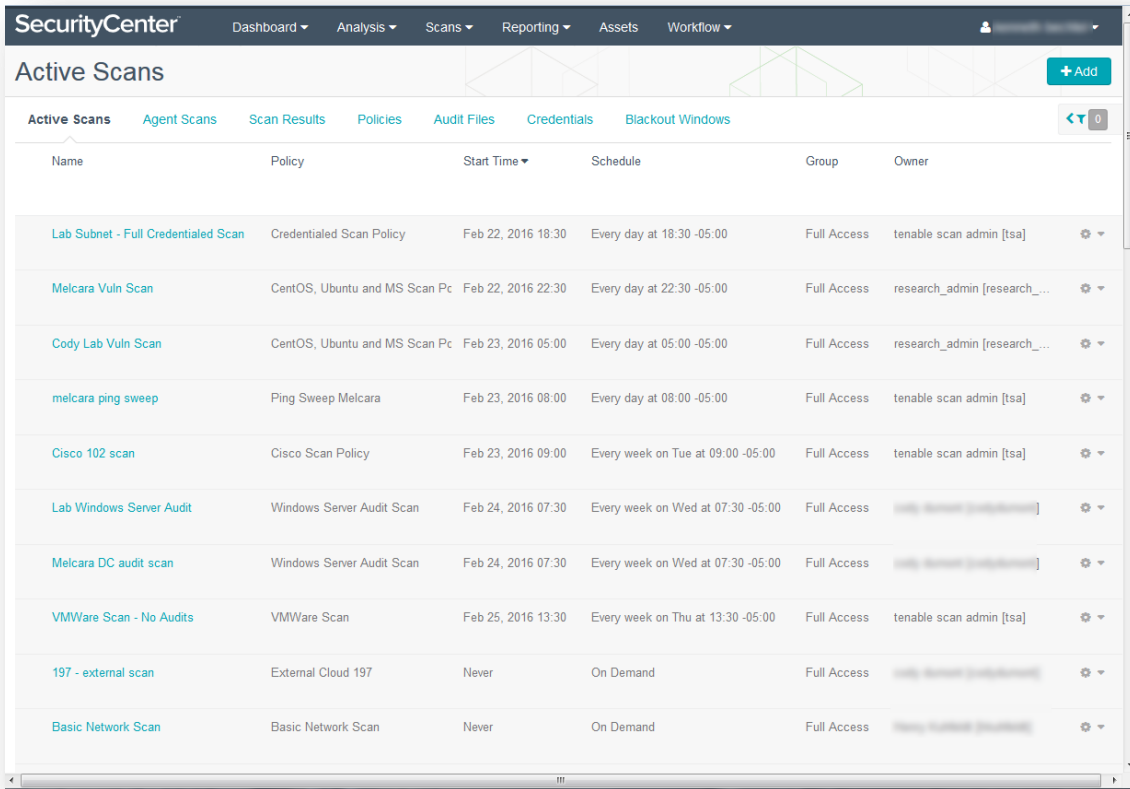
Plugin ID	Name	Family
12106	Norton AntiVirus Detection	Windows
12107	McAfee Antivirus Detection	Windows
16192	Trend Micro Antivirus Detection	Windows
16193	Antivirus Software Check	Windows
20283	Panda Antivirus Detection	Windows
21608	NOD32 Antivirus Detection	Windows
21725	Symantec AntiVirus Detection (Corporate Edition)	Windows
24232	BitDefender Antivirus Detection	Windows
24344	Windows Live OneCare Antivirus Detection	Windows
31857	Symantec AntiVirus Scan Engine Detection	Windows
87777	Avast Antivirus Detection	Windows

SecurityCenter CV also passively monitors networks for the following anti-virus products:

Plugin ID	Name
8231	Avira Anti-Virus Detection
8230	Avast Client Detection
6549	Sophos Antivirus Version Detection
5363	eScan Anti-Virus Detection
5199	Sophos Enterprise Anti-virus Version Detection
5014	Avira Antivirus Version Detection
5013	ESET AntiVirus Version Detection
4592	F-PROT Antivirus Version Detection
4188	TrendMicro Server Detection
4145	Panda Antivirus Agent Detection
4036	eScan Agent Detection
3960	F-Secure Product Detection (TCP)
3891	Symantec Antivirus Detection
3889	BitDefender Detection
3863	CA Antivirus Client Detection
3838	Kaspersky Antivirus Client Detection
3676	F-Secure Product Detection (UDP)
3343	Sophos Control Center Detection
3007	AVG AntiVirus Version Detection
2353	Symantec Norton Antivirus Detection

Creating an Active Scan in SecurityCenter

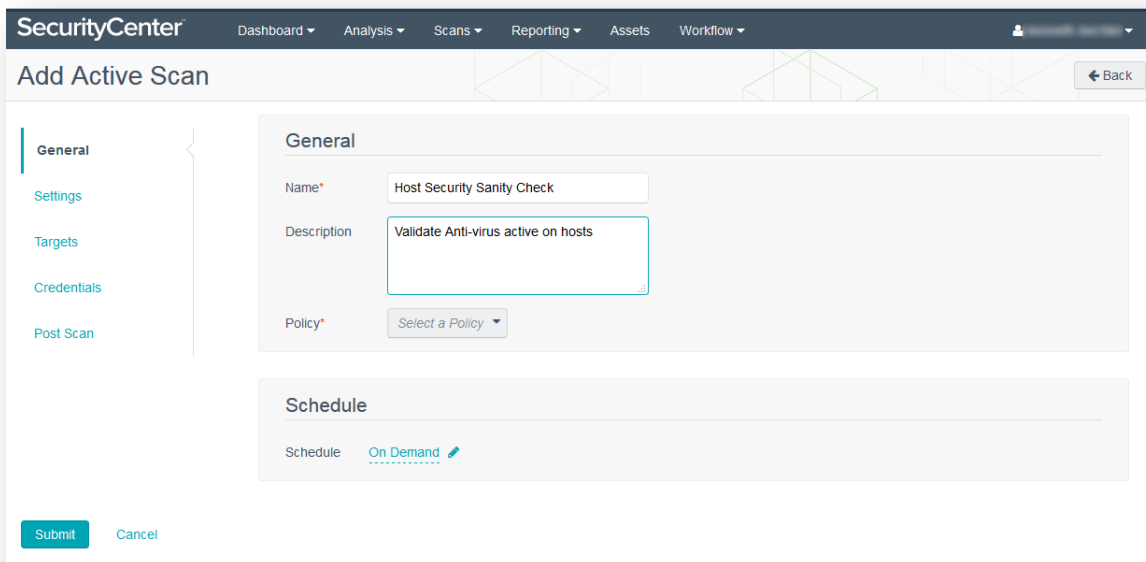
Log in to SecurityCenter. Select “Scans” > “Active Scans” and then click the “+Add” button in the upper right corner.



The screenshot shows the SecurityCenter interface with the 'Active Scans' page. The page has a navigation bar with 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', and 'Workflow'. Below the navigation bar, there are tabs for 'Active Scans', 'Agent Scans', 'Scan Results', 'Policies', 'Audit Files', 'Credentials', and 'Blackout Windows'. A '+ Add' button is in the top right corner. The main content is a table with the following columns: Name, Policy, Start Time, Schedule, Group, and Owner. The table contains ten rows of scan entries.

Name	Policy	Start Time	Schedule	Group	Owner
Lab Subnet - Full Credentialed Scan	Credentialed Scan Policy	Feb 22, 2016 18:30	Every day at 18:30 -05:00	Full Access	tenable scan admin [tsa]
Melcara Vuln Scan	CentOS, Ubuntu and MS Scan Pc	Feb 22, 2016 22:30	Every day at 22:30 -05:00	Full Access	research_admin [research_...]
Cody Lab Vuln Scan	CentOS, Ubuntu and MS Scan Pc	Feb 23, 2016 05:00	Every day at 05:00 -05:00	Full Access	research_admin [research_...]
melcara ping sweep	Ping Sweep Melcara	Feb 23, 2016 08:00	Every day at 08:00 -05:00	Full Access	tenable scan admin [tsa]
Cisco 102 scan	Cisco Scan Policy	Feb 23, 2016 09:00	Every week on Tue at 09:00 -05:00	Full Access	tenable scan admin [tsa]
Lab Windows Server Audit	Windows Server Audit Scan	Feb 24, 2016 07:30	Every week on Wed at 07:30 -05:00	Full Access	[redacted]
Melcara DC audit scan	Windows Server Audit Scan	Feb 24, 2016 07:30	Every week on Wed at 07:30 -05:00	Full Access	[redacted]
VMWare Scan - No Audits	VMWare Scan	Feb 25, 2016 13:30	Every week on Thu at 13:30 -05:00	Full Access	tenable scan admin [tsa]
197 - external scan	External Cloud 197	Never	On Demand	Full Access	[redacted]
Basic Network Scan	Basic Network Scan	Never	On Demand	Full Access	[redacted]

In the “General” tab, provide a name that is descriptive and within your organization’s naming standards. Examples would include “Host Security Sanity Check” or “Anti-Virus Software Check”. Enter a complete description in the description box (optional), and select the appropriate policy.

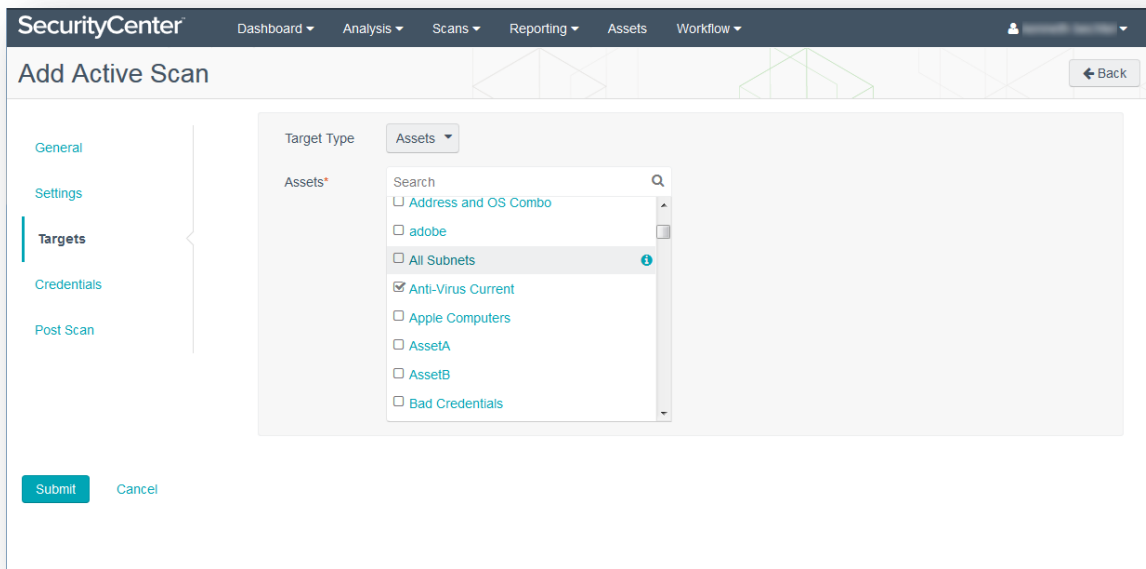


The screenshot shows the 'Add Active Scan' form in SecurityCenter. The form has a navigation bar with 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', and 'Workflow'. Below the navigation bar, there are tabs for 'General', 'Settings', 'Targets', 'Credentials', and 'Post Scan'. The 'General' tab is selected. The form contains the following fields:

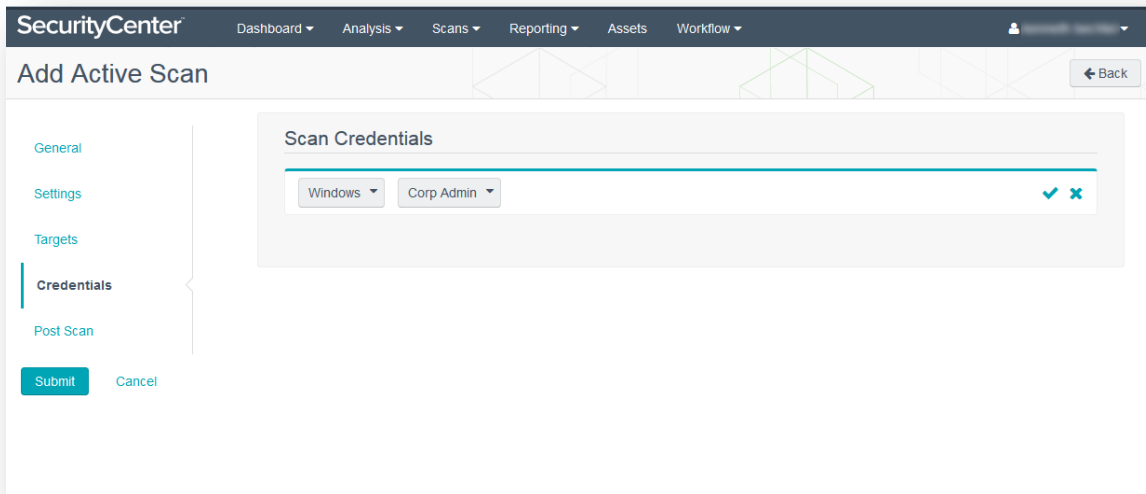
- Name*: Host Security Sanity Check
- Description: Validate Anti-virus active on hosts
- Policy*: Select a Policy
- Schedule: On Demand

At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

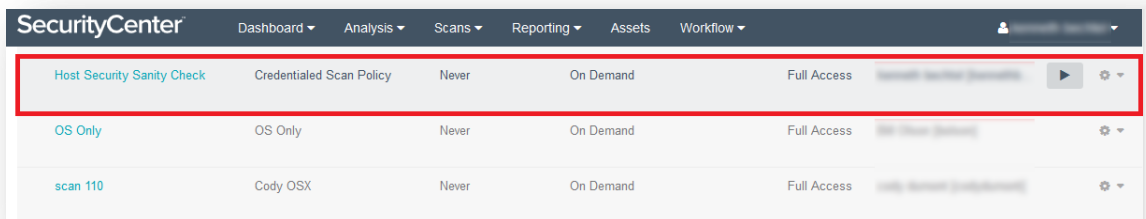
Under “Targets”, select “Anti-Virus Current”.



Under “Credentials”, add the administrative-level credentials you will be using for the scan, and select “Submit” in the lower left.



If you chose to run the scan manually, you can now select it from the list of available scans. Click the “Launch” arrow to the right of your new scan to launch it against your selected targets.



Results will populate in your reports when the scan is complete.

The screenshot shows the SecurityCenter interface with the 'Scan Results' tab selected. The table lists various scans with columns for Name, Type, Scan Policy, S..., Group, Owner, Duration, Import Time, and Status.

Name	Type	Scan Policy	S...	Group	Owner	Duration	Import Time	Status
Host security sanity check	Active	Credentialed Scan Policy	768	Full Acc...	kenneth bechtel	15 Minutes	Less than a minute ago	Completed
Cisco 102 scan	Active	Cisco Scan Policy	256	Full Acc...	kenneth bechtel	7 Minutes	4 hours ago	Completed
melcara ping sweep	Active	Ping Sweep Melcara	768	Full Acc...	kenneth bechtel	7 Minutes	5 hours ago	Completed
Cody Lab Vuln Scan	Active	CentOS, Ubuntu and M...	768	Full Acc...	kenneth bechtel	38 Minutes	7 hours ago	Completed
All OS Scan [All OS Scan (Scheduled)]	Agent	Advanced Agent Scan	2	Full Acc...	kenneth bechtel	12 Hours	13 hours ago	Completed
Melcara Vuln Scan	Active	CentOS, Ubuntu and M...	768	Full Acc...	kenneth bechtel	29 Minutes	14 hours ago	Completed

Click on the name for the scanning results.

The screenshot shows the 'Vulnerability Analysis' page for the 'Host security sanity check' scan. It displays a table of vulnerability results with columns for Plugin ID, Name, Family, Severity, and Total.

Plugin ID	Name	Family	Severity	Total
16193	Antivirus Software Check	Windows	Info	1
17651	Microsoft Windows SMB : Obtains the Password Policy	Windows : User management	Info	1
19506	Nessus Scan Information	Settings	Info	1
20811	Microsoft Windows Installed Software Enumeration (credentialed check)	Windows	Info	1
24269	Windows Management Instrumentation (WMI) Available	Windows	Info	1
24270	Computer Manufacturer Information (WMI)	Windows	Info	1
24272	Network Interfaces Enumeration (WMI)	Windows	Info	1
33545	Oracle Java Runtime Environment (JRE) Detection	Windows	Info	1
34096	BIOS Version (WMI)	Windows	Info	1
38153	Microsoft Windows Summary of Missing Patches	Windows : Microsoft Bulletins	Info	1
44401	Microsoft Windows SMB Service Config Enumeration	Windows	Info	1
44871	WMI Windows Feature Enumeration	Windows	Info	1
46742	Microsoft Windows SMB Registry : Enumerate the list of SNMP communities	Windows	Info	1
48337	Windows ComputerSystemProduct Enumeration (WMI)	Windows	Info	1
48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture	Windows	Info	1

Creating an Active Scan in Nessus

In Nessus, create a new Advanced Scan. Under the “**Settings**” tab, provide a name that is descriptive and within your organization’s naming standards. Examples would include “Host Security Sanity Check” or “Anti-Virus Software Check”. Enter a complete description in the description box (optional), and enter or upload your target system(s).

New Scan / Advanced Scan

Scan Library > **Settings** Credentials Compliance Plugins

BASIC **General** Schedule Notifications DISCOVERY ASSESSMENT REPORT ADVANCED

Settings / Basic / General

Name: Host Security Sanity Check

Description: Check to ensure Host security and anti-malware software is running

Folder: My Scans

Targets: 192.168.1.0-192.168.255.255

Upload Targets Add File

Under “**Credentials**,” add the administrative-level credentials you will be using for the scan and select “**Submit**” in the lower left.

Nessus Scans Policies kbechtel

New Scan / Advanced Scan Search Credentials

Scan Library > **Credentials** Settings Compliance Plugins

CREDENTIALS

- Cloud Services
- Database
- Host
 - SNMPv3
 - SSH
 - Windows
- Miscellaneous
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Authentication method: Password

Username: administrator

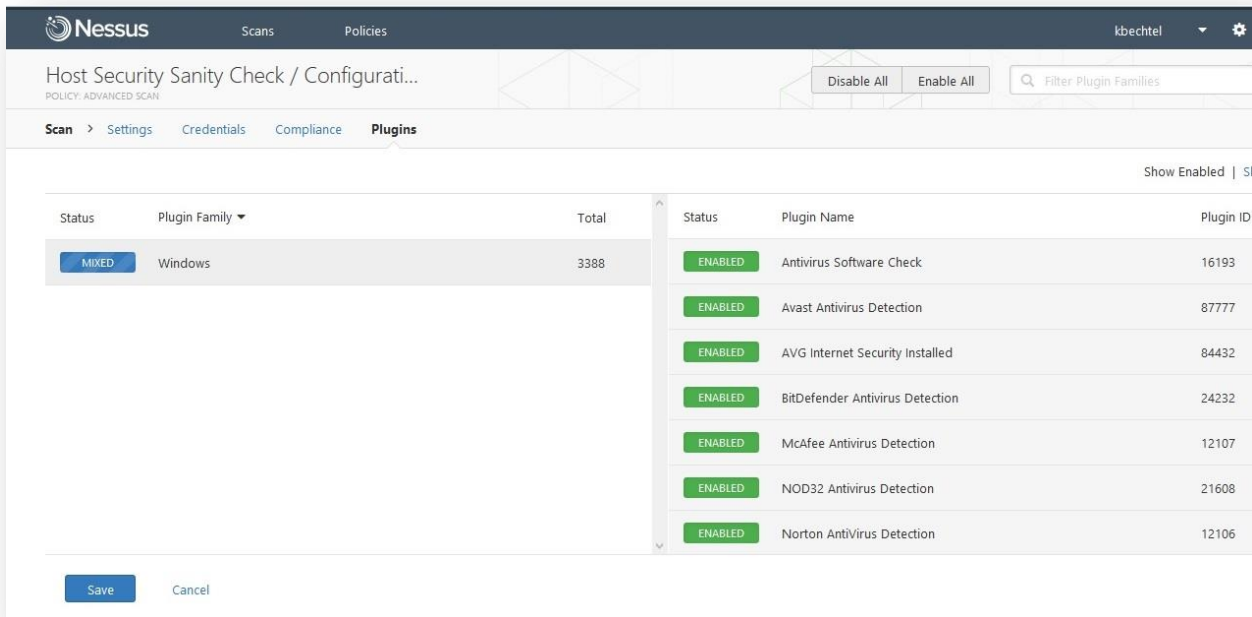
Password:

Domain: mysample

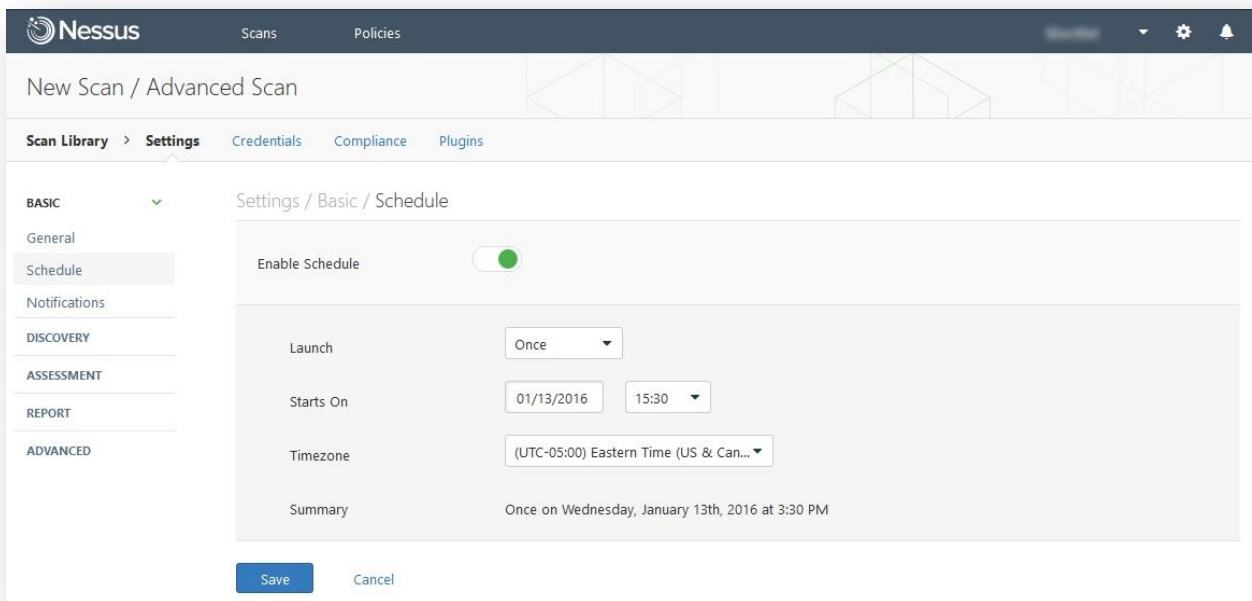
Global Settings

- Never send credentials in the clear
- Do not use NTLMv1 authentication
- Start the Remote Registry service during the scan

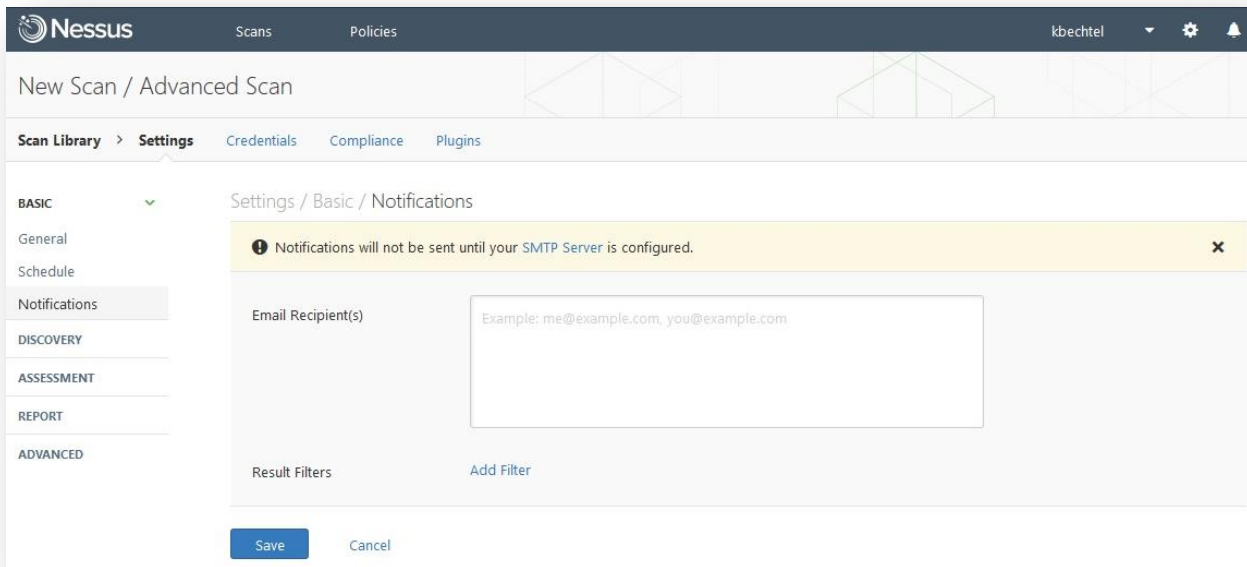
Under the “**Plugins**” section, filter for any or all of the anti-virus detection plugins, based on your need.



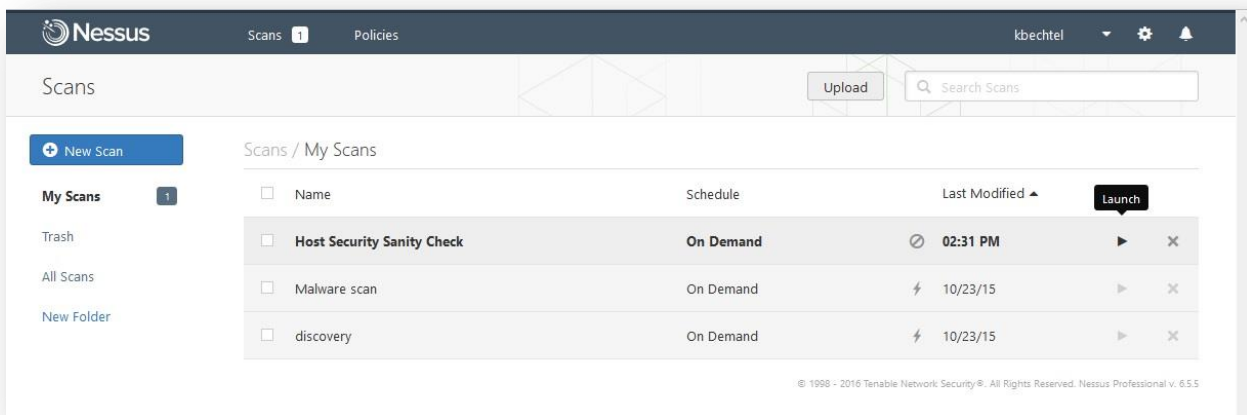
Under the “**Schedule**” tab, you can enable a schedule or leave as a manual scan, depending on your organization’s security policies and procedures.



If available, enter the email addresses of the security analysts who should be notified when the scan is complete (not all organizations will enable SMTP for this, so perform this step only if organizational policy permits).



Click "Save", and then manually launch the scan by clicking on the "Launch" arrow to the right of the scan name, or wait for the scheduled scan to launch.



When the scan is complete, log in to Nessus and click on the scan to review the results.

Hosts > 172.26.24.235 > Vulnerabilities 19

Severity	Plugin Name	Plugin Family	Count
INFO	Netstat Portscanner (WMI)	Port scanners	19
INFO	DCE Services Enumeration	Windows	8
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Antivirus Software Check	Windows	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1
INFO	Microsoft Windows SMB Registry Remotely Accessible	Windows	1
INFO	Microsoft Windows SMB Service Enumeration	Windows	1
INFO	SSL / TLS Versions Supported	General	1
INFO	Terminal Services Use SSL/TLS	Misc.	1
INFO	Windows Management Instrumentation (WMI) Available	Windows	1

Host Details

IP: 172.26.24.235
 Start: Today at 1:16 PM
 End: Today at 1:16 PM
 Elapsed: a few seconds
 KB: [Download](#)

Vulnerabilities

Hosts > 172.26.24.235 > Vulnerabilities 19

INFO Antivirus Software Check

Description
 The remote host has an antivirus installed and running, and its engine and virus definitions are up to date.

See Also
<http://www.nessus.org/u?b145ae41>
<http://www.tenable.com/blog/auditing-anti-virus-products-with-nessus>

Output

```

Check Point ZoneAlarm :
Check Point ZoneAlarm is installed on the remote host :
Product name      : ZoneAlarm Extreme Security
Path              : C:\Program Files (x86)\CheckPoint\ZoneAlarm\
Version          : 14.1.057.000
Engine version    : 8.6.0.97
Virus signatures  : 05/06/2016
    
```

Plugin Details

Severity: Info
 ID: 16193
 Version: \$Revision: 1.35 \$
 Type: local
 Family: Windows
 Published: 2005/01/18
 Modified: 2016/02/24

Risk Information

Risk Factor: None

Port	Hosts
445 / tcp / cifs	172.26.24.235

Conclusion

Malware continues to evolve, and will continue the successful tactic of targeting security software for the purpose of evading or disabling it. By leveraging alternate sanity checks that are provided with Tenable's solutions, hosted off the potentially compromised hosts, you will be able to notice the modifications by hostile software sooner, limiting your exposure to that malware. Tenable does its best to simplify the process of verifying compliance with corporate counter-malware policies and provides solutions to reduce administrator workload and increase incident response time.

Tenable has published multiple resources on utilizing SecurityCenter Continuous View and Nessus solutions to detect malware and abnormalities. These papers include:

- [Comprehensive Malware Detection with SecurityCenter Continuous View and Nessus](#)
- [24/7 Visibility into Advanced Malware on Networks and Endpoints](#)
- [Tenable Malware Detection: Keeping Up With An Increasingly Sophisticated Threat Environment](#)
- [Auditing Anti-Virus Products with Nessus](#)
- [Auditing Anti-virus Software without an Agent](#)

These resources are available for free from the Tenable Network Security [Resource Library](#). Tenable also hosts a Discussions Forum for [Indicators of Compromise and Malware](#).

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.