TENABLE Network Security®

Nessus 5.0 User Guide

July 24, 2012

(Revision 14)

The newest version of this document is available at the following URL:
http://static.tenable.com/documentation/nessus_5.0_user_guide.pdf

Table of Contents

INTRODUCTION

This document describes how to use Tenable Network Security's **Nessus user interface (UI)**. Please email any comments and suggestions to support@tenable.com.

The Nessus UI is a web-based interface to the Nessus vulnerability scanner. To use the client, you must have an operational Nessus scanner deployed and be familiar with its use.

STANDARDS AND CONVENTIONS

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd
/opt/nessus/
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

NESSUS UI OVERVIEW

DESCRIPTION

The Nessus User Interface (UI) is a web-based interface to the Nessus scanner that is made up of a simple HTTP server and web client, requiring no software installation apart from the Nessus server. As of Nessus 4, all platforms draw from the same code base eliminating most platform specific bugs and allowing for faster deployment of new features. The primary features are:

- Generates **.nessus** files that Tenable products use as the standard for vulnerability data and scan policy.
- A policy session, list of targets and the results of several scans can all be stored in a single **.nessus** file that can be easily exported. Please refer to the Nessus File Format guide for more details.
- The GUI displays scan results in real-time so you do not have to wait for a scan to complete to view results.
- Provides unified interface to the Nessus scanner regardless of base platform. The same functionalities exist on Mac OS X, Windows, and Linux.

- Scans will continue to run on the server even if you are disconnected for any reason.
- Nessus scan reports can be uploaded via the Nessus UI and compared to other reports.

Supported Platforms

Since the Nessus UI is a web-based client, it can run on any platform with a web browser.

> The Nessus web-based user interface is best experienced using Microsoft Internet Explorer 9, Mozilla Firefox 9.x, Google Chrome 16.x, or Apple Safari 5.x.

INSTALLATION

User management of the Nessus 5 server is conducted through a web interface or SecurityCenter and it is no longer necessary to use a standalone NessusClient. The standalone NessusClient will still connect and operate the scanner, but they will not be updated or supported.

Refer to the Nessus 5.0 Installation and Configuration Guide for instructions on installing Nessus. As of Nessus 5.0, Oracle Java (formerly Sun Microsystems' Java) is required for PDF report functionality.

OPERATION

Overview

Nessus provides a simple, yet powerful interface for managing vulnerability-scanning activity.

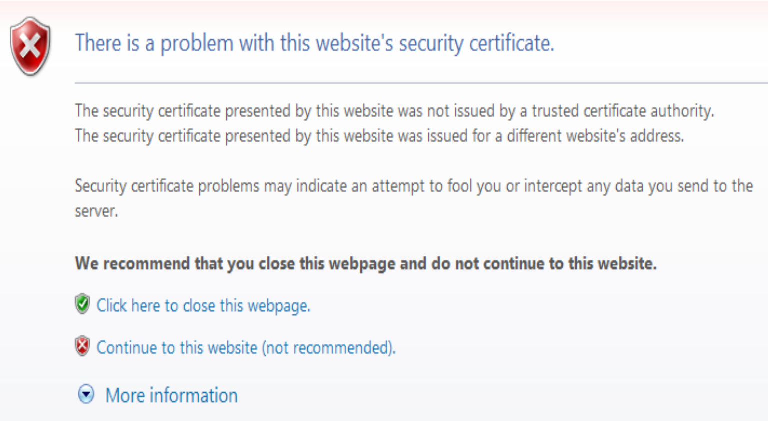
Connect to Nessus GUI

To launch the Nessus GUI, perform the following:

- Open a web browser of your choice.
- Enter `https://[server IP]:8834/` in the navigation bar.

> Be sure to connect to the user interface via HTTPS, as unencrypted HTTP connections are not supported.

The first time you attempt to connect to the Nessus user interface, most web browsers will display an error indicating the site is not trusted due to the self-signed SSL certificate:



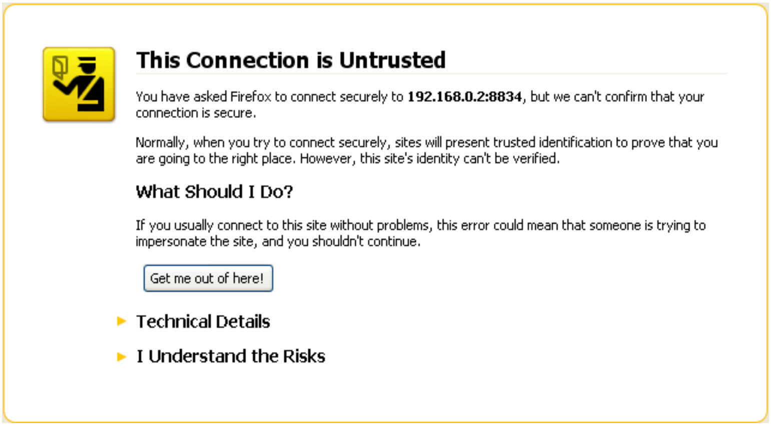
There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information



This Connection is Untrusted

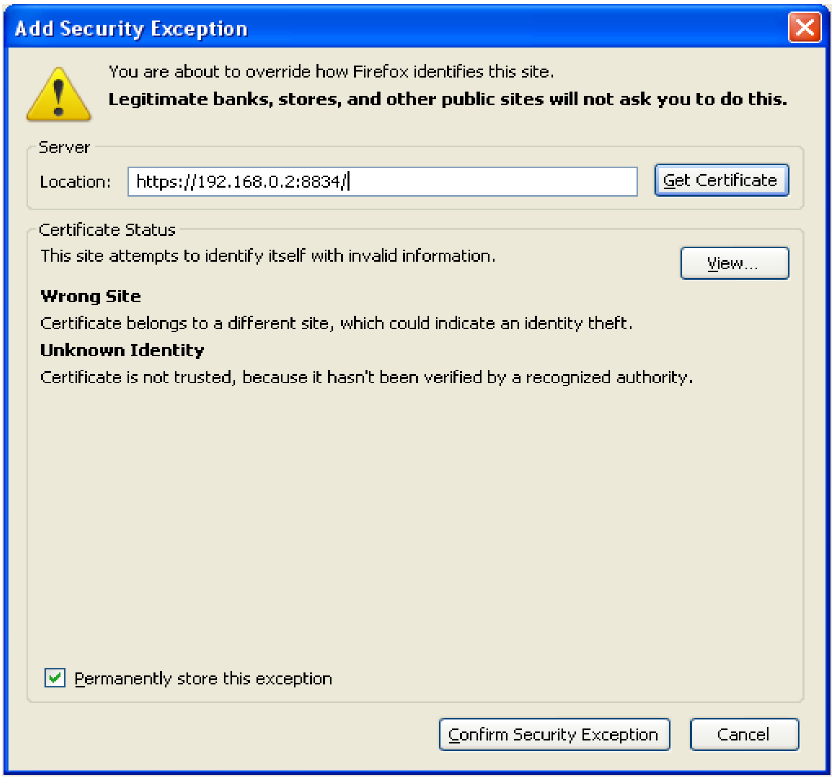
You have asked Firefox to connect securely to **192.168.0.2:8834**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Users of Microsoft Internet Explorer can click on "Continue to this website (not recommended)" to load the Nessus user interface. Firefox 3.x – 10.x users can click on "I Understand the Risks" and then "Add Exception…" to bring up the site exception dialog box:



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.0.2:8834/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

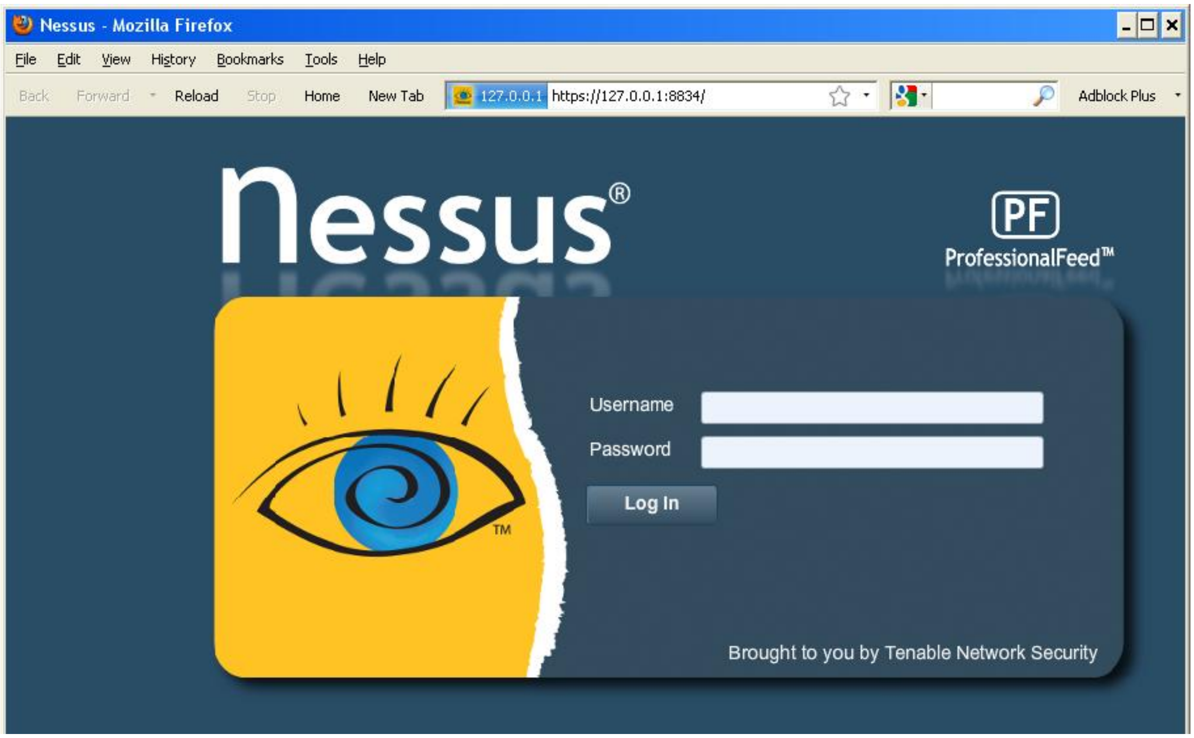
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Verify the "Location:" bar reflects the URL to the Nessus server and click on "**Confirm Security Exception**". For information on installing a custom SSL certificate, consult the Nessus Installation and Configuration Guide.

After your browser has confirmed the exception, a splash screen will be displayed as follows:

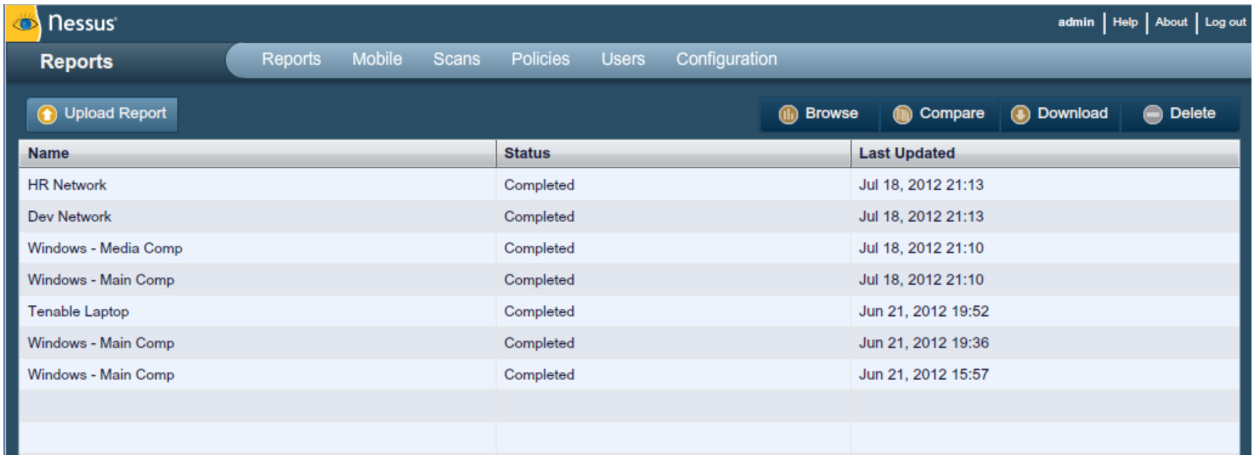

Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Back Forward Reload Stop Home New Tab
127.0.0.1 https://127.0.0.1:8834/
Adblock Plus
Nessus®
PF ProfessionalFeed™
Username
Password
Log In
Brought to you by Tenable Network Security

The initial splash screen will indicate whether Nessus is currently registered with a HomeFeed or ProfessionalFeed:

HF
HomeFeed

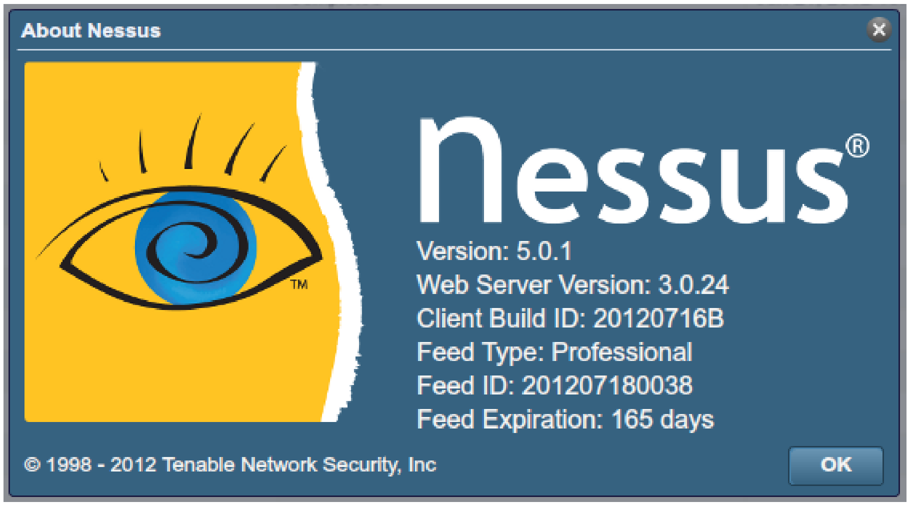
PF
ProfessionalFeed™

Authenticate using an account and password previously created during the installation process. After successful authentication, the UI will present menus for creating policies, conducting scans, and browsing reports:


Nessus
admin | Help | About | Log out
Reports
Reports Mobile Scans Policies Users Configuration
Upload Report
Browse Compare Download Delete

Name	Status	Last Updated
HR Network	Completed	Jul 18, 2012 21:13
Dev Network	Completed	Jul 18, 2012 21:13
Windows - Media Comp	Completed	Jul 18, 2012 21:10
Windows - Main Comp	Completed	Jul 18, 2012 21:10
Tenable Laptop	Completed	Jun 21, 2012 19:52
Windows - Main Comp	Completed	Jun 21, 2012 19:36
Windows - Main Comp	Completed	Jun 21, 2012 15:57

At any point during Nessus use, the top right options will be present. The “admin” notation seen on the upper right hand side in the screen above denotes the account currently logged in. Clicking on this will allow you to change your current password. “Help” is a link to the Nessus documentation, providing detailed instructions on the use of the software. “About” shows information about the Nessus installation including version, feed type, feed expiration, client build and web server version. “Log out” will terminate your current session.

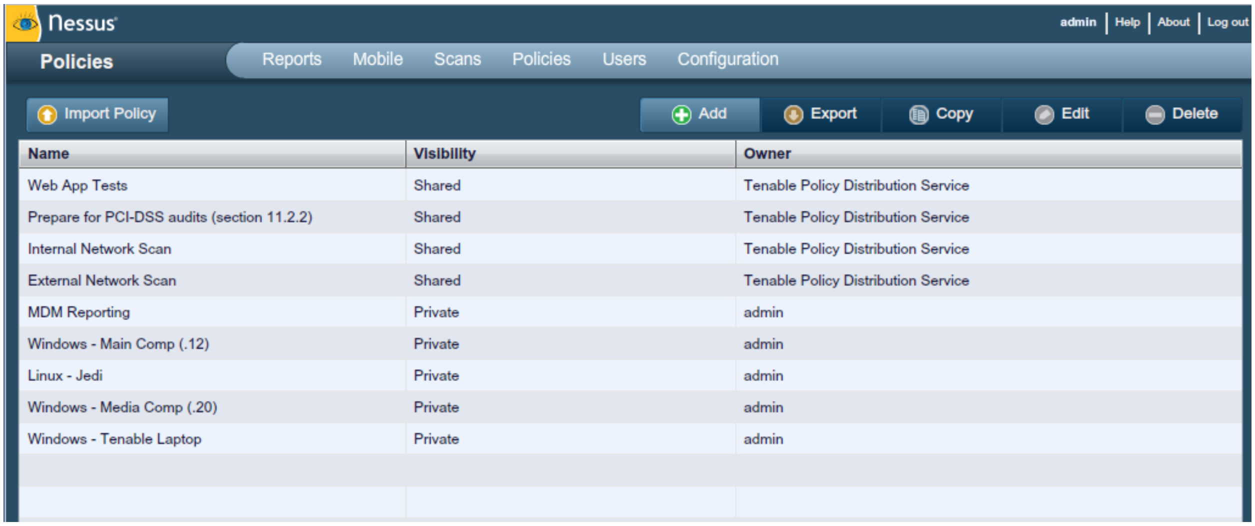


About Nessus

Version: 5.0.1
Web Server Version: 3.0.24
Client Build ID: 20120716B
Feed Type: Professional
Feed ID: 201207180038
Feed Expiration: 165 days

© 1998 - 2012 Tenable Network Security, Inc

Policy Overview



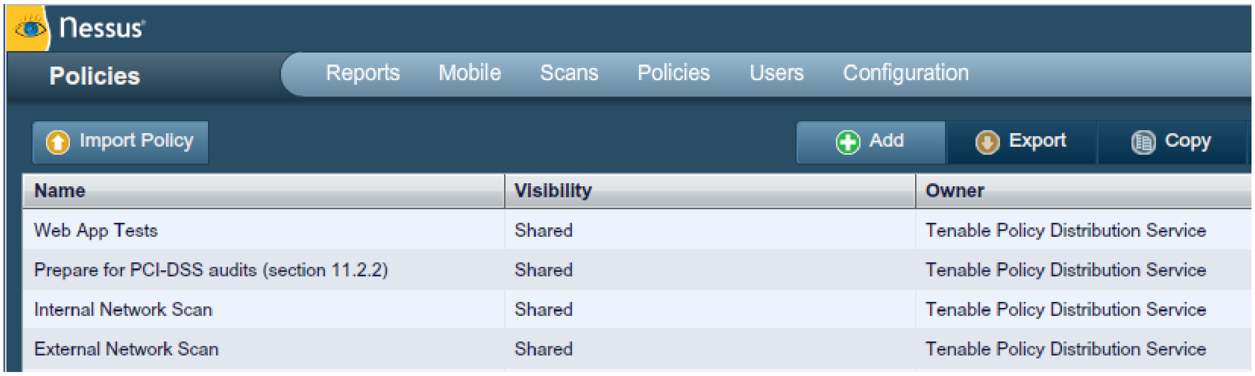
Name	Visibility	Owner
Web App Tests	Shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service
MDM Reporting	Private	admin
Windows - Main Comp (.12)	Private	admin
Linux - Jedi	Private	admin
Windows - Media Comp (.20)	Private	admin
Windows - Tenable Laptop	Private	admin

A Nessus “policy” consists of configuration options related to performing a vulnerability scan. These options include, but are not limited to:

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner and more.
- Credentials for local scans (e.g., Windows, SSH), authenticated Oracle database scans, HTTP, FTP, POP, IMAP, or Kerberos based authentication.
- Granular family or plugin based scan specifications.

- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks, and more.

Default Policies



Name	Visibility	Owner
Web App Tests	Shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service

Nessus ships with several default policies provided by Tenable Network Security, Inc. They are provided as templates to assist you in creating custom policies for your organization or to use as-is in order to start basic scans of your resources. Please be sure to read and understand the default policies before using them in scans against your resources.

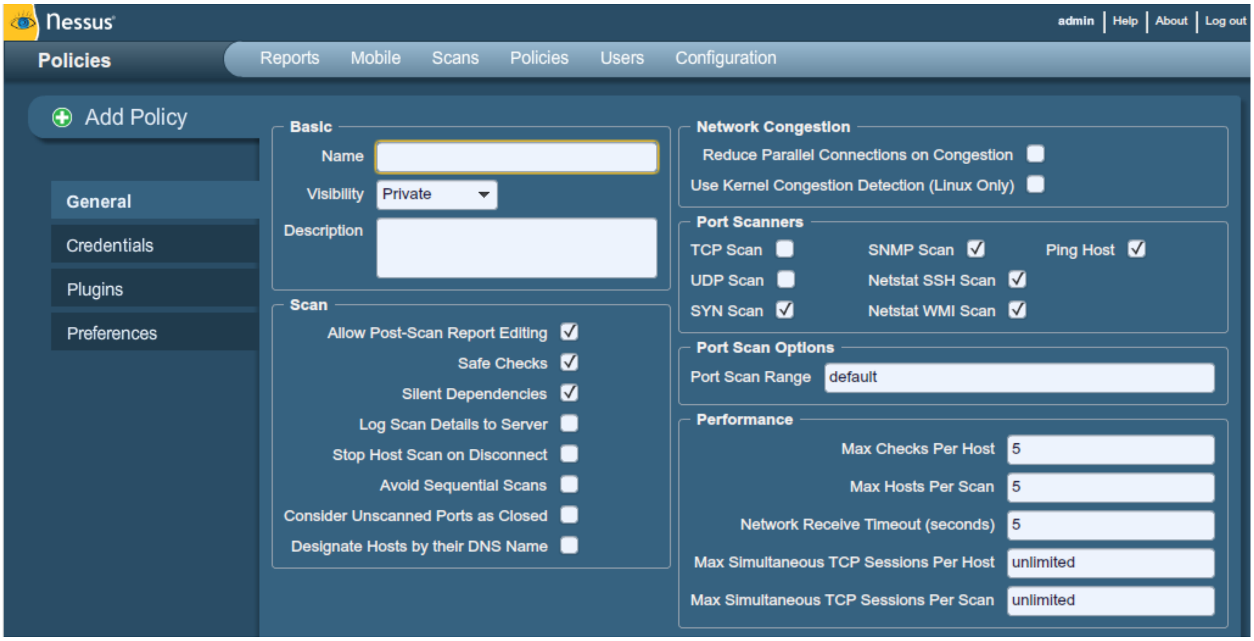
Policy Name	Description
External Network Scan	This policy is tuned to scan externally facing hosts, which typically present fewer services to the network. The plugins associated with known web application vulnerabilities (CGI Abuses and CGI Abuses: XSS plugin families) are enabled in this policy. In addition, all 65,536 ports (including port 0 via separate plugin) are scanned for on each target.
Internal Network Scan	This policy is tuned for better performance, taking into account that it may be used to scan large internal networks with many hosts, several exposed services, and embedded systems such as printers. CGI Checks are disabled and a standard set of ports is scanned for, not all 65,535.
Web App Tests	If you want to scan your systems and have Nessus detect both known and unknown vulnerabilities in your web applications, this is the scan policy for you. The fuzzing capabilities in Nessus are enabled in this policy, which will cause Nessus to spider all discovered web sites and then look for vulnerabilities present in each of the parameters, including XSS, SQL, command injection and several more. This policy will identify issues via HTTP and HTTPS.
Prepare for PCI DSS audits	This policy enables the built-in PCI DSS compliance checks that compare scan results with the PCI standards and produces a report on your compliance posture. It is very important to note that a successful compliance scan does not guarantee compliance or a secure infrastructure.

	Organizations preparing for a PCI DSS assessment can use this policy to prepare their network and systems for PCI DSS compliance.

If you intend to use a default policy provided by Tenable as a basis for your own custom policy, use the Copy feature. Editing a default policy will result in it becoming owned by the user and no longer appearing in the interface.

Creating a New Policy

Once you have connected to a Nessus server UI, you can create a custom policy by clicking on the "**Policies**" option on the bar at the top and then "**+ Add**" button on the right. The "**Add Policy**" screen will be displayed as follows:



Basic

Name

Visibility: Private

Description

Scan

Allow Post-Scan Report Editing ☑

Safe Checks ☑

Silent Dependencies ☑

Log Scan Details to Server ☐

Stop Host Scan on Disconnect ☐

Avoid Sequential Scans ☐

Consider Unscanned Ports as Closed ☐

Designate Hosts by their DNS Name ☐

Network Congestion

Reduce Parallel Connections on Congestion ☐

Use Kernel Congestion Detection (Linux Only) ☐

Port Scanners

TCP Scan ☐ SNMP Scan ☑ Ping Host ☑

UDP Scan ☐ Netstat SSH Scan ☑

SYN Scan ☑ Netstat WMI Scan ☑

Port Scan Options

Port Scan Range: default

Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 5

Network Receive Timeout (seconds): 5

Max Simultaneous TCP Sessions Per Host: unlimited

Max Simultaneous TCP Sessions Per Scan: unlimited

Note that there are four configuration tabs: **General**, **Credentials**, **Plugins**, and **Preferences**. For most environments, the default settings do not need to be modified, but they provide more granular control over the Nessus scanner operation. These tabs are described below.

General

The "**General**" tab enables you to name the policy and configure scan related operations. There are six boxes of grouped options that control scanner behavior:

The "**Basic**" frame is used to define aspects of the policy itself:

Option	Description
Name	Sets the name that will be displayed in the Nessus UI to identify the policy.

Visibility	Controls if the policy is *shared* with other users, or kept *private* for your use only. Only administrative users can share policies.
Description	Used to give a brief description of the scan policy, typically good to summarize the overall purpose (e.g., "Web Server scans without local checks or non HTTP services").

The "**Scan**" frame further defines options related to how the scan should behave:

Option	Description
Allow Post-Scan Report Editing	This feature allows users to delete items from the report when checked. When doing a scan for regulatory compliance or other audits, this should be unchecked to be able to prove that the scan was not tampered with.
Safe Checks	Safe Checks will disable all plugins that may have an adverse effect on the remote host.
Silent Dependencies	If this option is checked, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, uncheck the box.
Log Scan Details to Server	Save additional details of the scan to the Nessus server log (`nessusd.messages`) including plugin launch, plugin finish or if a plugin is killed. The resulting log can be used to confirm that particular plugins were used and hosts were scanned.
Stop Host Scan on Disconnect	If checked, Nessus will stop scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (e.g., IDS) has begun to block traffic to a server. Continuing scans on these machines will send unnecessary traffic across the network and delay the scan.
Avoid Sequential Scans	By default, Nessus scans a list of IP addresses in sequential order. If checked, Nessus will scan the list of hosts in a random order. This is typically useful in helping to distribute the network traffic directed at a particular subnet during large scans.
Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), Nessus will consider it closed.
Designate Hosts by their DNS Name	Use the host name rather than IP address for report output.

The "**Network**" frame gives options that better control the scan based on the target network being scanned:

Option	Description
Reduce Parallel Connections on Congestion	This enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Nessus will throttle the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus will automatically attempt to use the available space within the network pipe again.
Use Kernel Congestion Detection (Linux Only)	Enables Nessus to monitor the CPU and other internal workings for congestion and scale back accordingly. Nessus will always attempt to use as much resource as is available. This feature is only available for Nessus scanners deployed on Linux.

The "**Port Scanners**" frame controls which methods of port scanning should be enabled for the scan:

Option	Description
TCP Scan	Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. ⚠ On some platforms (e.g., Windows and Mac OS X), selecting this scanner will cause Nessus to use the SYN scanner to avoid serious performance issues native to those operating systems.
UDP Scan	This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets. ⚠ UDP is a "stateless" protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
SYN Scan	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines port state based on a reply, or lack of reply.
SNMP Scan	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings

	are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Netstat SSH Scan	This option uses `netstat` to check for open ports from the local machine. It relies on the `netstat` command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.
Netstat WMI Scan	This option uses `netstat` to check for open ports from the local machine. It relies on the `netstat` command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials. ⚠ A WMI based scan uses `netstat` to determine open ports, thus ignoring any port ranges specified. If any port enumerator (`netstat` or SNMP) is successful, the port range becomes "all". However, Nessus will still honor the "consider unscanned ports as closed" option if selected.
Ping Host	This option enables the pinging of remote hosts on multiple ports to determine if they are alive.

The "**Port Scan Options**" frame directs the scanner to target a specific range of ports. The following values are allowed for the "Port Scan Range" option:

Value	Description
"default"	Using the keyword "default", Nessus will scan approximately 4,790 common ports. The list of ports can be found in the `nessus-services` file.
"all"	Using the keyword "all", Nessus will scan all 65,535 ports.
Custom List	A custom range of ports can be selected by using a comma delimited list of ports or port ranges. For example, "21,23,25,80,110" or "1-1024,8080,9000-9200" are allowed. Specifying "1-65535" will scan all ports. You may also specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would specify "T:1-1024,U:300-500". You can also specify a set of ports to scan

	for both protocols, as well as individual ranges for each separate protocol ("1-1024,T:1024-65535,U:1025"). If you are scanning a single protocol, select only that port scanner and specify the ports normally.

⚠ The range specified for a port scan will be applied to both TCP and UDP scans.

The "**Performance**" frame gives two options that control how many scans will be launched. These options are perhaps the most important when configuring a scan as they have the biggest impact on scan times and network activity.

Option	Description
Max Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max Hosts Per Scan	This setting limits the maximum number of hosts that a Nessus scanner will scan at the same time.
Network Receive Timeout (seconds)	Set to five seconds by default. This is the time that Nessus will wait for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.
Max Simultaneous TCP Sessions Per Host	This setting limits the maximum number of established TCP sessions for a single host. ⚠ This TCP throttling option also controls the number of packets per second the SYN scanner will eventually send (e.g., if this option is set to 15, the SYN scanner will send 1500 packets per second at most).
Max Simultaneous TCP Sessions Per Scan	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. ⚠ For Nessus scanners installed on Windows XP, Vista, and 7 hosts, this value must be set to 19 or less to get accurate results.

Credentials

The "**Credentials"** tab, pictured below, allows you to configure the Nessus scanner to use authentication credentials during scanning. By configuring credentials, it allows Nessus to perform a wider variety of checks that result in more accurate scan results.

The “**Windows credentials**” drop-down menu item has settings to provide Nessus with information such as SMB account name, password, and domain name. Server Message Block (SMB) is a file sharing protocol that allows computers to share information transparently across the network. Providing this information to Nessus will allow it to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied. It is not necessary to modify other SMB parameters from default settings.

When multiple SMB accounts are configured, Nessus will try to log in with the supplied credentials sequentially. Once Nessus is able to authenticate with a set of credentials, it will check subsequent credentials supplied, but only use them if administrative privileges are granted when previous accounts provided user access.

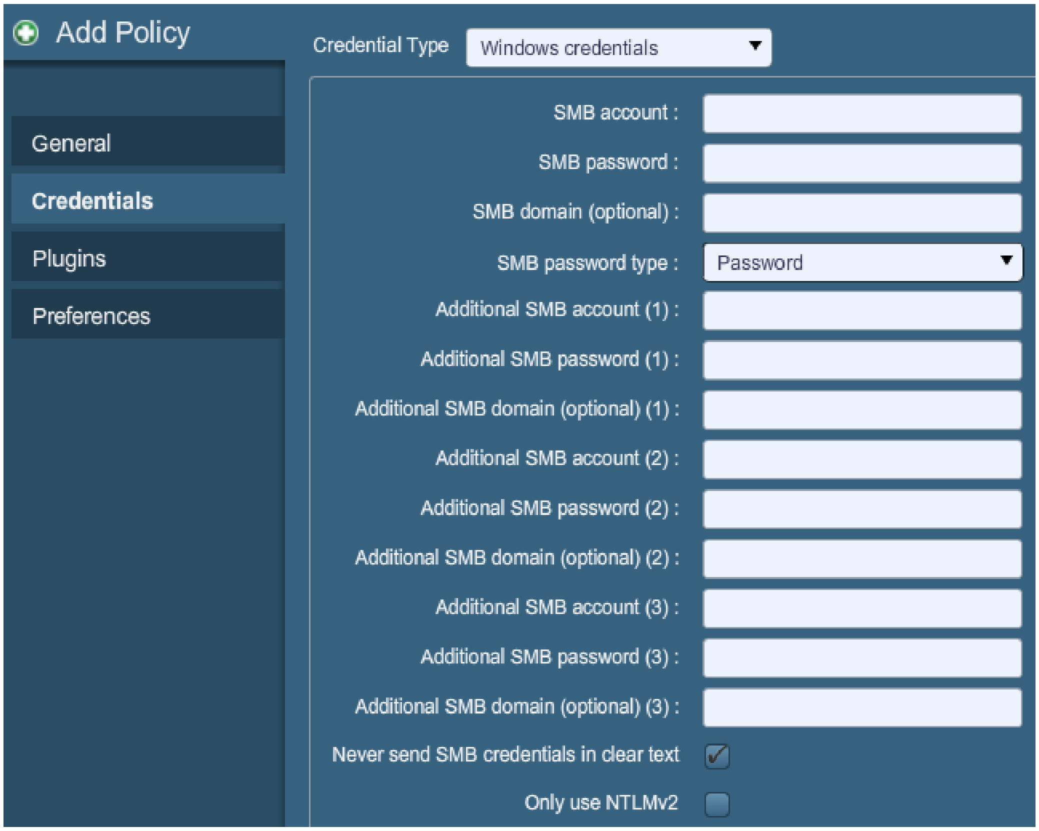
Some versions of Windows allow you to create a new account and designate it as an “administrator”. These accounts are not always suitable for performing credentialed scans. Tenable recommends that the original administrative account, named “Administrator” be used for credentialed scanning to ensure full access is permitted. On some versions of Windows, this account may be hidden. The real administrator account can be unhidden by running a DOS prompt with administrative privileges and typing the following command:

```
C:\> net user administrator /active:yes
```

If a maintenance SMB account is created with limited administrator privileges, Nessus can easily and securely scan multiple domains.

Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. Nessus includes a variety of security checks for Windows NT, 2000, Server 2003, XP, Vista, Windows 7, and Windows 2008 that are more accurate if a domain account is provided. Nessus does attempt to try several checks in most cases if no account is provided.

The Windows Remote Registry service allows remote computers with credentials to access the registry of the computer being audited. If the service is not running, reading keys and values from the registry will not be possible, **even with full credentials**. Please see the Tenable blog post titled “Dynamic Remote Registry Auditing - Now you see it, now you don’t!” for more information. This service **must be started** for a Nessus credentialed scan to fully audit a system using credentials.



Credential Type: Windows credentials

SMB account :

SMB password :

SMB domain (optional) :

SMB password type : Password

Additional SMB account (1) :

Additional SMB password (1) :

Additional SMB domain (optional) (1) :

Additional SMB account (2) :

Additional SMB password (2) :

Additional SMB domain (optional) (2) :

Additional SMB account (3) :

Additional SMB password (3) :

Additional SMB domain (optional) (3) :

Never send SMB credentials in clear text ☑

Only use NTLMv2 □

Users can select "**SSH settings**" from the drop-down menu and enter credentials for scanning Unix systems. These credentials are used to obtain local information from remote Unix systems for patch auditing or compliance checks. There is a field for entering the SSH user name for the account that will perform the checks on the target Unix system, along with either the SSH password or the SSH public key and private key pair. There is also a field for entering the Passphrase for the SSH key, if it is required.

Nessus 4 supports the **`blowfish-cbc`**, **`aes-cbc`**, and **`aes-ctr`** cipher algorithms.

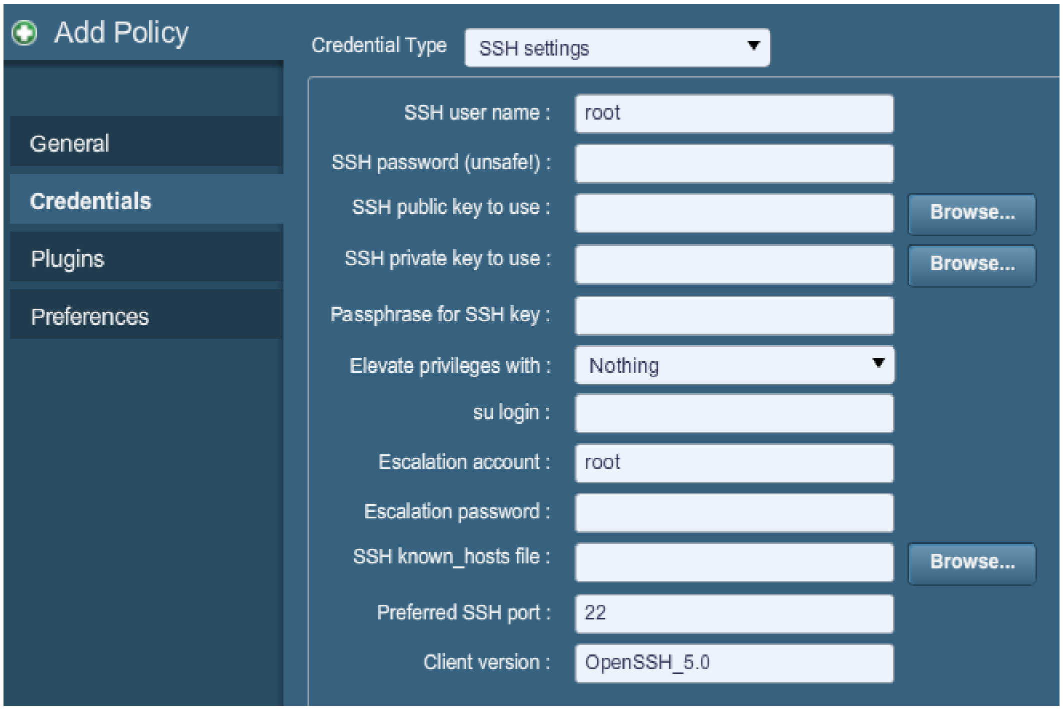
The most effective credentialed scans are those when the supplied credentials have "root" privileges. Since many sites do not permit a remote login as root, Nessus users can invoke "**`su`**", "**`sudo`**", "**`su+sudo`**", or "**`dzdo`**" with a separate password for an account that has been set up to have "**`su`**" or "**`sudo`**" privileges. In addition, Nessus can escalate privileges on Cisco devices by selecting "**`Cisco 'enable'`**".

Nessus can use SSH key-based access to authenticate to a remote server. If an SSH **`known_hosts`** file is available and provided as part of the scan policy, Nessus will only attempt to log into hosts in this file. Finally, the "Preferred SSH port" can be set to direct Nessus to connect to SSH if it is running on a port other than 22.

Nessus encrypts all passwords stored in policies. However, best practices recommend using SSH keys for authentication rather than SSH passwords. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log in to a system that may not be under your control. As such, it is not recommended to use SSH passwords unless absolutely necessary.

> Nessus also supports a “su+sudo” option that can be used in the event of a system not allowing privileged accounts remote login privileges.

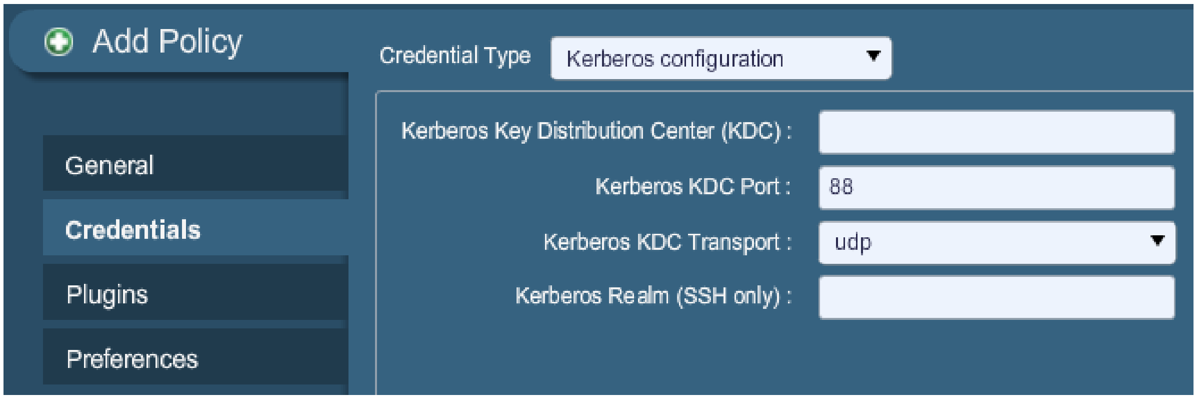
The following screen capture shows the SSH options available. The “Elevate privileges with” drop-down provides several methods of increasing privileges once authenticated.



Credential Type: SSH settings
SSH user name : root
SSH password (unsafe!) :
SSH public key to use :
SSH private key to use :
Passphrase for SSH key :
Elevate privileges with : Nothing
su login :
Escalation account : root
Escalation password :
SSH known_hosts file :
Preferred SSH port : 22
Client version : OpenSSH_5.0

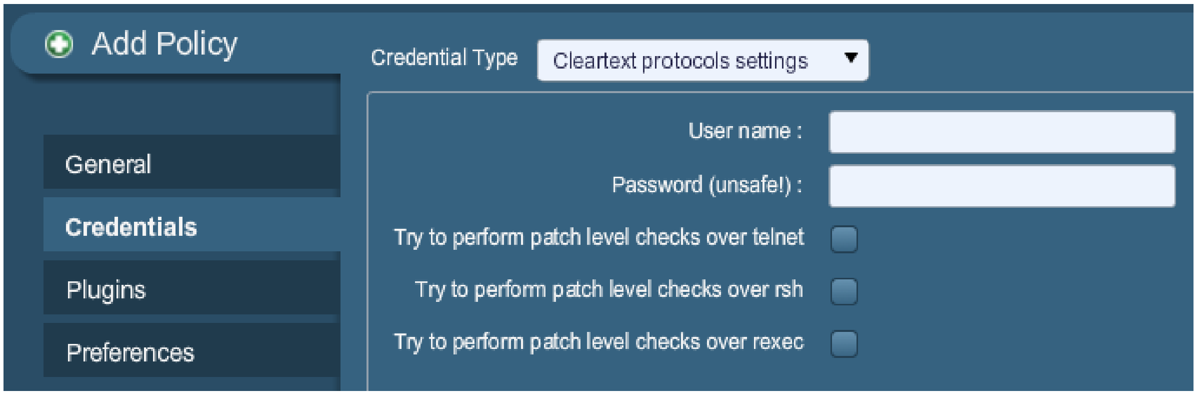
If an account other than `root` must be used for privilege escalation, it can be specified under the “**Escalation account**” with the “**Escalation password**”.

“**Kerberos configuration**” allows you to specify credentials using Kerberos keys from a remote system:



Credential Type: Kerberos configuration
Kerberos Key Distribution Center (KDC) :
Kerberos KDC Port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH only) :

Finally, if a secure method of performing credentialed checks is not available, users can force Nessus to try to perform checks over insecure protocols by configuring the "**Cleartext protocol settings**" drop-down menu item. The cleartext protocols supported for this option are **telnet**, **rsh**, and **rexec**.



Credential Type: Cleartext protocols settings ▼

User name :

Password (unsafe!) :

Try to perform patch level checks over telnet □

Try to perform patch level checks over rsh □

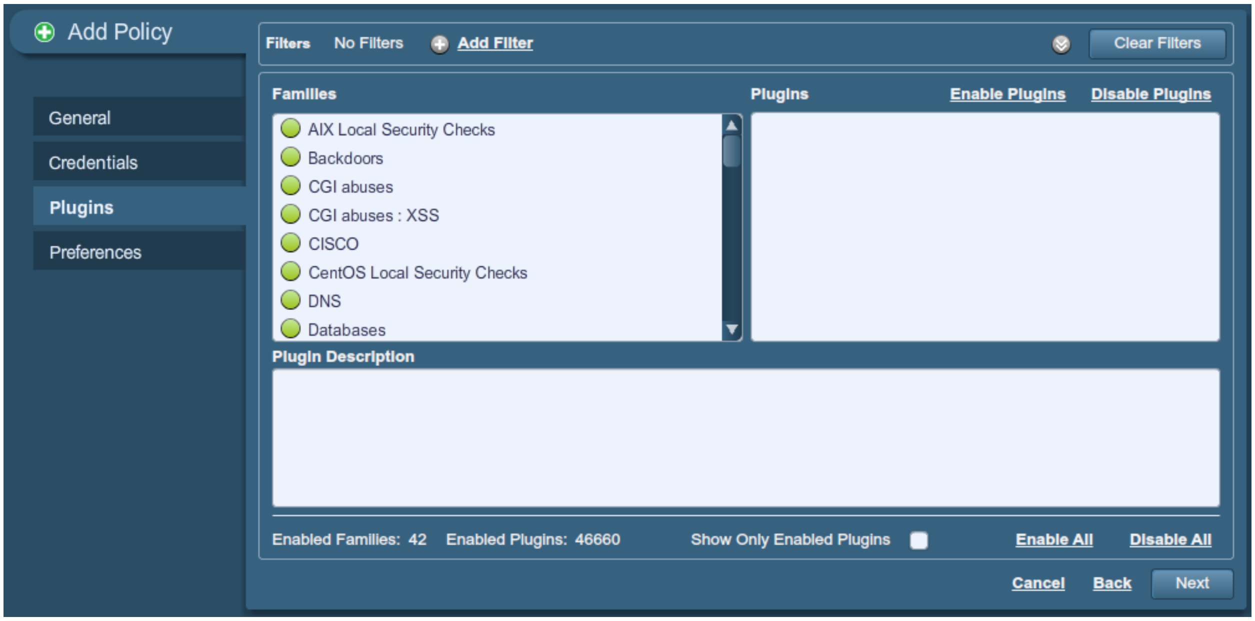
Try to perform patch level checks over rexec □

By default, all passwords (and the policy itself) are encrypted. If the policy is saved to a `.nessus` file and that `.nessus` file is then copied to a different Nessus installation, all passwords in the policy will be unusable by the second Nessus scanner as it will be unable to decrypt them.

> ⚠ Using cleartext credentials in any fashion is **not** recommended! If the credentials are sent remotely (e.g., via a Nessus scan), the credentials could be intercepted by anyone with access to the network. Use encrypted authentication mechanisms whenever possible.

Plugins

The "**Plugins**" tab enables the user to choose specific security checks by plugin family or individual checks.



Filters: No Filters

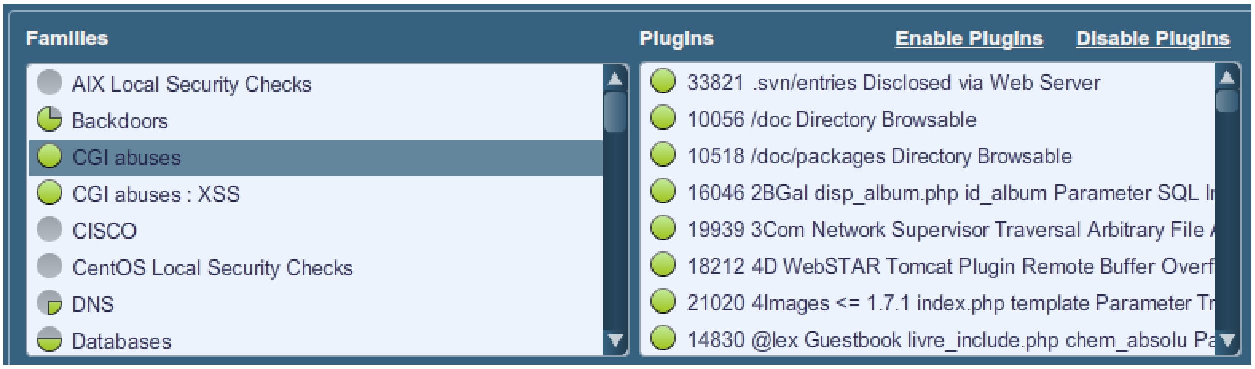
Families
- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS
- Databases

Plugins

Plugin Description

Enabled Families: 42 Enabled Plugins: 46660 Show Only Enabled Plugins □

Clicking on the circle next to a plugin family allows you to enable (green) or disable (gray) the entire family. Selecting a family will display the list of its plugins in the upper right pane. Individual plugins can be enabled or disabled to create very specific scan policies. As adjustments are made, the total number of families and plugins selected is displayed at the bottom. If the circle next to a plugin family shows 25%, 50%, or 75% green, it denotes that roughly that number of the plugins are enabled, but not all of them.

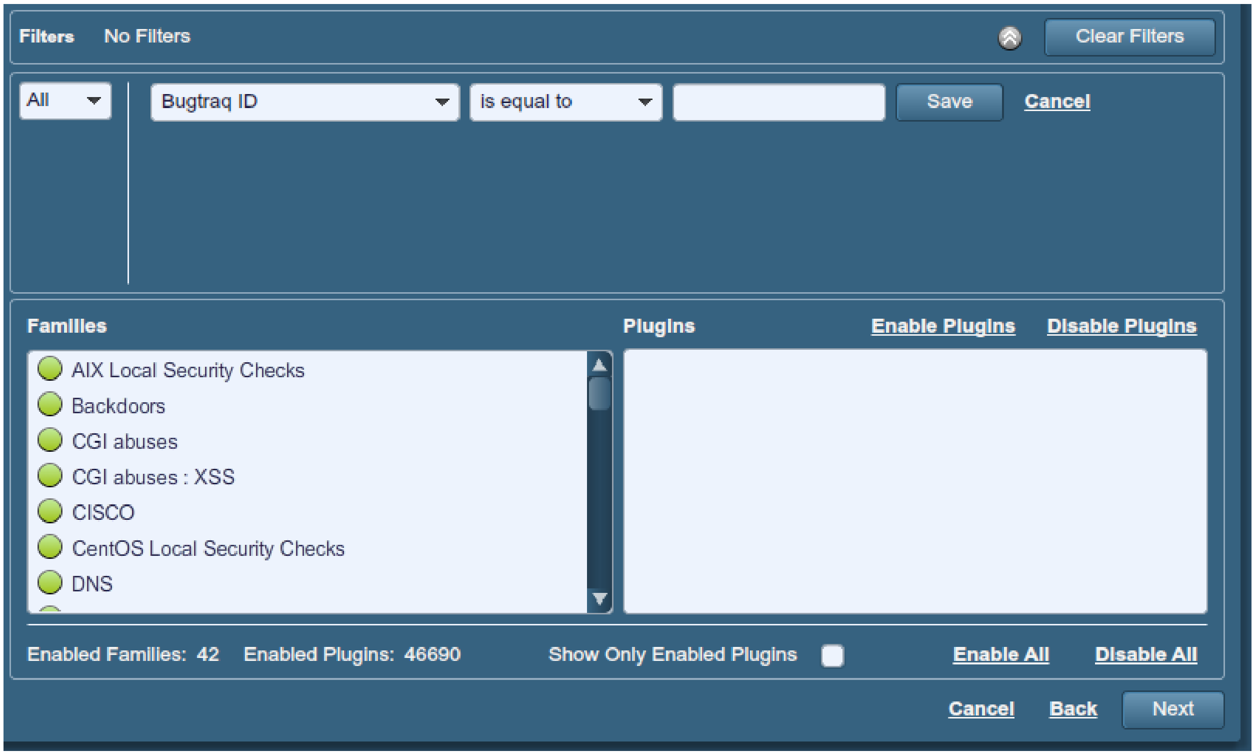


Families:
- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS
- Databases

Plugins:
- 33821 .svn/entries Disclosed via Web Server
- 10056 /doc Directory Browsable
- 10518 /doc/packages Directory Browsable
- 16046 2BGal disp_album.php id_album Parameter SQL I
- 19939 3Com Network Supervisor Traversal Arbitrary File
- 18212 4D WebSTAR Tomcat Plugin Remote Buffer Overf
- 21020 4Images <= 1.7.1 index.php template Parameter Tr
- 14830 @lex Guestbook livre_include.php chem_absolu Pa

Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in the "Plugin Description" pane will also show solution information, additional references if available, and the CVSSv2 score that provides a basic risk rating.

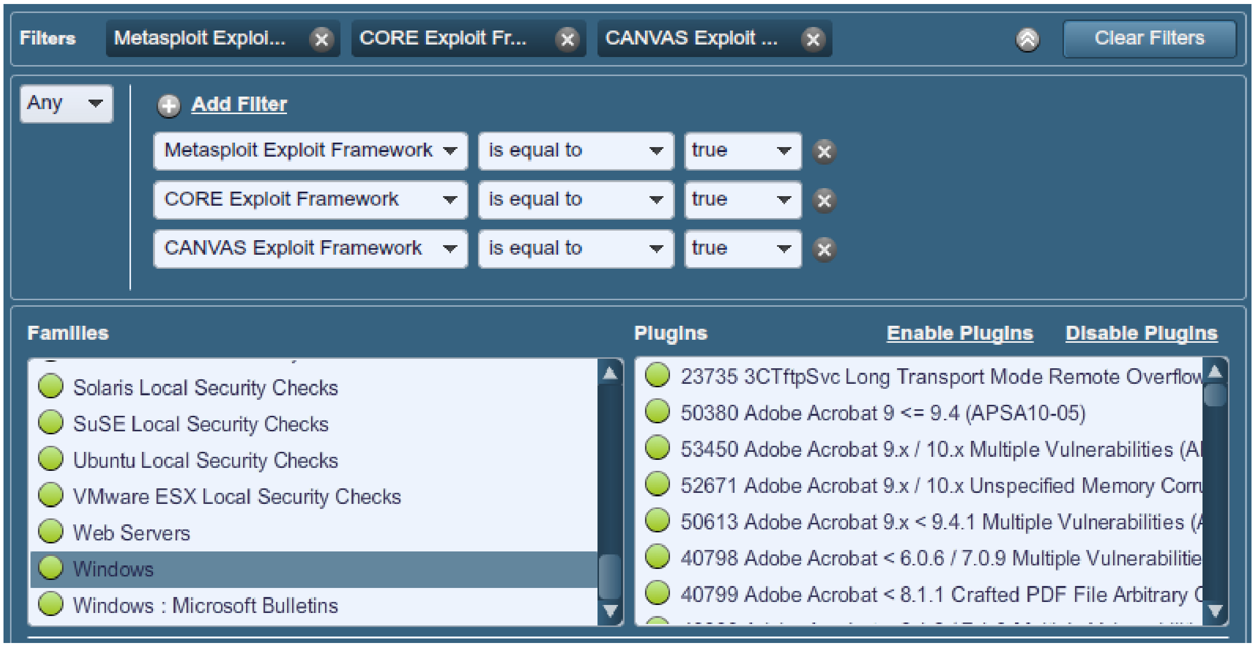
At the top of the plugin family tab, you can create filters to build a list of plugins to include in the policy. Filters allow granular control over plugin selection. Multiple filters can be set in a single policy. To create a filter, click on the "**Add Filter**" link:



Families:
- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS

Enabled Families: 42 Enabled Plugins: 46690

Each filter created gives you several options for refining a search. The filter criteria can be based on “Any”, where any one criteria will return matches, or “All”, where every filter criteria must be present. For example, if we want a policy that only includes plugins that have an associated exploit in a commercial exploit framework, we create three filters and select “Any” for the criteria:



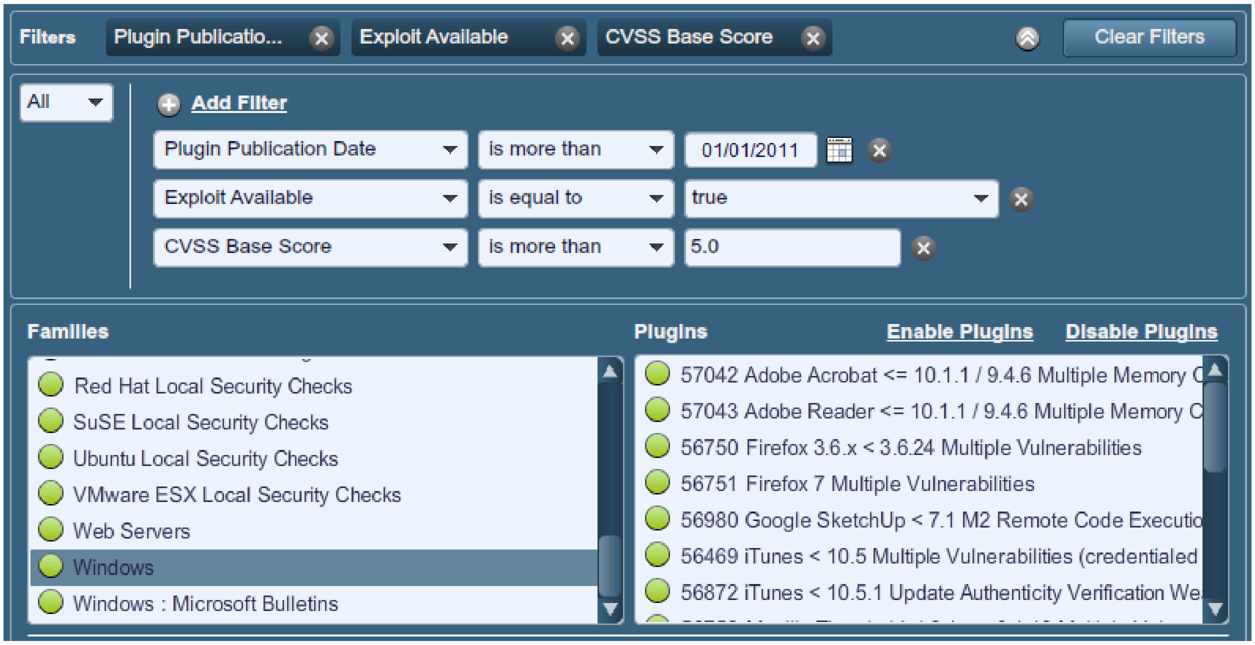
Any

Metasploit Exploit Framework | is equal to | true
CORE Exploit Framework | is equal to | true
CANVAS Exploit Framework | is equal to | true

Families:
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows
- Windows : Microsoft Bulletins

Plugins:
- 23735 3CTftpSvc Long Transport Mode Remote Overflow
- 50380 Adobe Acrobat 9 <= 9.4 (APSA10-05)
- 53450 Adobe Acrobat 9.x / 10.x Multiple Vulnerabilities (A
- 52671 Adobe Acrobat 9.x / 10.x Unspecified Memory Corr
- 50613 Adobe Acrobat 9.x < 9.4.1 Multiple Vulnerabilities (
- 40798 Adobe Acrobat < 6.0.6 / 7.0.9 Multiple Vulnerabilitie
- 40799 Adobe Acrobat < 8.1.1 Crafted PDF File Arbitrary C

If we want to create a policy that contains plugins that match several criteria, we select “All” and add the desired filters. For example, the policy below would include any plugin published after January 1, 2011 that has a public exploit and CVSS Base Score higher than 5.0:



All

Plugin Publication Date | is more than | 01/01/2011
Exploit Available | is equal to | true
CVSS Base Score | is more than | 5.0

Families:
- Red Hat Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows
- Windows : Microsoft Bulletins

Plugins:
- 57042 Adobe Acrobat <= 10.1.1 / 9.4.6 Multiple Memory C
- 57043 Adobe Reader <= 10.1.1 / 9.4.6 Multiple Memory C
- 56750 Firefox 3.6.x < 3.6.24 Multiple Vulnerabilities
- 56751 Firefox 7 Multiple Vulnerabilities
- 56980 Google SketchUp < 7.1 M2 Remote Code Executio
- 56469 iTunes < 10.5 Multiple Vulnerabilities (credentialed
- 56872 iTunes < 10.5.1 Update Authenticity Verification We

For a full list of filter criteria and details, check the Report Filters section of this document.

To use filters to create a policy, it is recommended you start by disabling all plugins. Using plugin filters, narrow down the plugins you want to be in your policy. Once completed, select each plugin family and click "Enable Plugins".

When a policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin feed update, they will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family will automatically be disabled as well.

The "Denial of Service" family contains some plugins that could cause outages on a network if the "Safe Checks" option is not enabled, but does contain some useful checks that will not cause any harm. The "Denial of Service" family can be used in conjunction with "Safe Checks" to ensure that any potentially dangerous plugins are not run. However, it is recommended that the "Denial of Service" family not be used on a production network.

Below the window showing the plugins you will find three options that will assist you in selecting and displaying plugins.

Option	Description
Show Only Enabled Plugins	Selecting this will cause Nessus to only display plugins that have been selected, either manually or via filter.
Enable all	Checks and enables all plugins and their families. This is an easy way to re-enable all plugins after creating a policy with some families or plugins disabled. Note that some plugins may require further configuration options.
Disable all	Un-checks and disables all plugins and their families. Running a scan with all plugins disabled will not produce any results.

Preferences

The "**Preferences**" tab includes means for granular control over scan policy settings. Selecting an item from the drop-down menu will display further configuration items for that category. Note that this is a dynamic list of configuration options that is dependent on the plugin feed, audit policies, and additional functionality that the connected Nessus scanner has access to. A scanner with a ProfessionalFeed may have more advanced configuration options available than a scanner configured with the HomeFeed. This list will change as plugins are added or modified.

The following table provides an overview of all preferences. For more detailed information regarding each preference item, check the Scanning Preferences in Detail section of this document.

Preference Drop-down	Description
ADSI settings	Active Directory Service Interfaces pulls information from the mobile device management (MDM) server regarding Android and iOS-based devices.
Apple Profile Manager API Settings	A ProfessionalFeed feature that enables enumeration and vulnerability scanning of Apple iOS devices (e.g., iPhone, iPad).
Cisco IOS Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test Cisco IOS based devices against compliance standards.
Database Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test databases such as DB2, SQL Server, MySQL, and Oracle against compliance standards.
Database Settings	Options used to specify the type of database to be tested as well as which credentials to use.
Do not scan fragile devices	A set of options that directs Nessus **not** to scan specific devices, due to increased risk of crashing the target.
Global variable settings	A wide variety of configuration options for Nessus.
HTTP cookies import	For web application testing, this preference specifies an external file to import HTTP cookies to allow authentication to the application.
HTTP login page	Settings related to the login page for web application testing.
IBM iSeries Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test IBM iSeries systems against compliance standards.
IBM iSeries Credentials	Where credentials are specified for IBM iSeries systems.
ICCP/COTP TSAP Addressing Weakness	A ProfessionalFeed option related to Supervisory Control And Data Acquisition (SCADA) tests.
Login configurations	Where credentials are specified for basic HTTP, NNTP, FTP, POP, and IMAP service testing.
Modbus/TCP Coil Access	A ProfessionalFeed option related to Supervisory Control And Data Acquisition (SCADA) tests.
Nessus SYN scanner	Options related to the built-in SYN scanner.
Nessus TCP scanner	Options related to the built-in TCP scanner.
News Server (NNTP) Information Disclosure	A set of options for testing NNTP servers for information disclosure vulnerabilities.

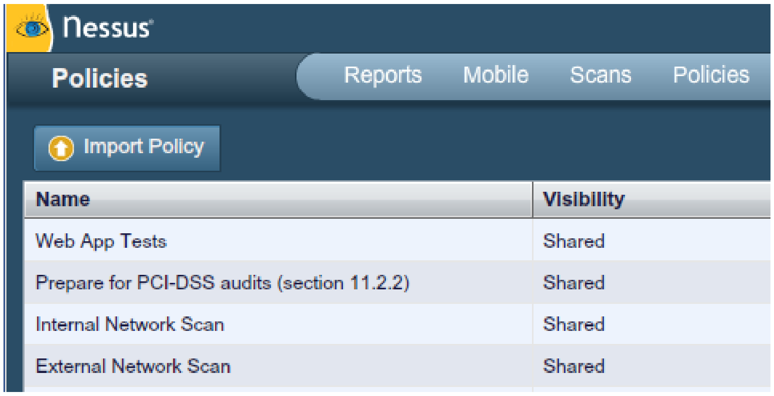
Oracle Settings	Options related to testing Oracle Database installations.
PCI DSS compliance	A ProfessionalFeed option that directs Nessus to compare scan results against PCI DSS standards.
Patch Management: Red Hat Satellite Server Settings	Options for integrating Nessus with the Red Hat Satellite patch management server. Consult the Patch Management Integration document for more information.
Patch Management: SCCM Server Settings	Options for integrating Nessus with the System Center Configuration Manager (SCCM) patch management server. Consult the Patch Management Integration document for more information.
Patch Management: VMware Go Server Settings	Options for integrating Nessus with the VMware Go Server (formerly Shavlik) patch management server. Consult the Patch Management Integration document for more information.
Patch Management: WSUS Server Settings	Options for integrating Nessus with the Windows Server Update Service (WSUS) patch management server. Consult the Patch Management Integration document for more information.
Ping the remote host	Settings that control Nessus' ping-based network discovery.
Port scanner settings	Two options that offer more control over port scanning activity.
SMB Registry : Start the Registry Service during the scan	Direct Nessus to start the SMB registry service on hosts that do not have it enabled.
SMB Scope	Direct Nessus to query domain users instead of local users.
SMB Use Domain SID to Enumerate Users	An option that allows you to specify the SID range for SMB lookups of domain users.
SMB Use Host SID to Enumerate Local Users	An option that allows you to specify the SID range for SMB lookups of local users.
SMTP Settings	Options for testing the Simple Mail Transport Protocol (SMTP).
SNMP Settings	Configuration and authentication information for the Simple Network Management Protocol (SNMP).
Service Detection	Options that direct Nessus how to test SSL-based services.
Unix Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test Unix systems against compliance standards.
VMware SOAP API Settings	Configuration and authentication information for VMware's SOAP API.

Wake-on-LAN	Direct Nessus to send Wake-on-LAN (WOL) packets before performing a scan.
Web Application Test Settings	Options related to testing web applications.
Web mirroring	Configuration details that control how many web pages Nessus will mirror, in order to analyze the contents for vulnerabilities.
Windows Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test Windows systems against compliance standards.
Windows File Contents Compliance Checks	A ProfessionalFeed option that allows a policy file to be specified to test files on Windows system against compliance standards.

⚠ Due to the XML meta-data upgrades in Nessus 5, compliance data that was generated with Nessus 4 will not be available in the compliance checks chapter of exported reports. However, compliance data will be available within the Nessus Web GUI.

Importing, Exporting, and Copying Policies

The "**Import**" button on the upper left will allow you to upload previously created policies to the scanner. Using the "**Browse...**" dialog box, select the policy from your local system and click on "**Submit**".



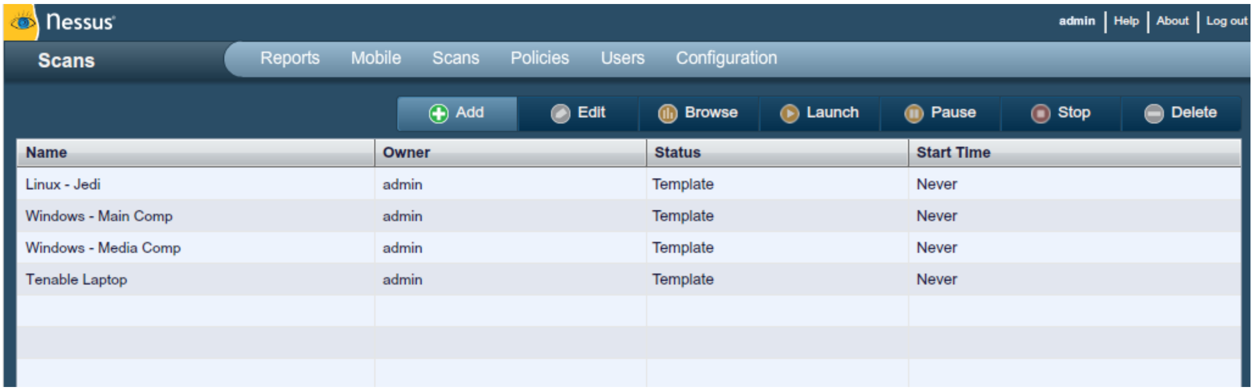
Name	Visibility
Web App Tests	Shared
Prepare for PCI-DSS audits (section 11.2.2)	Shared
Internal Network Scan	Shared
External Network Scan	Shared

The "**Export**" button on the menu bar will allow you to download an existing policy from the scanner to the local file system. The browser's download dialog box will allow you to open the policy in an external program (e.g., text editor) or save the policy to the directory of your choice.

⚠ Passwords and `.audit` files contained in a policy will **not** be exported.

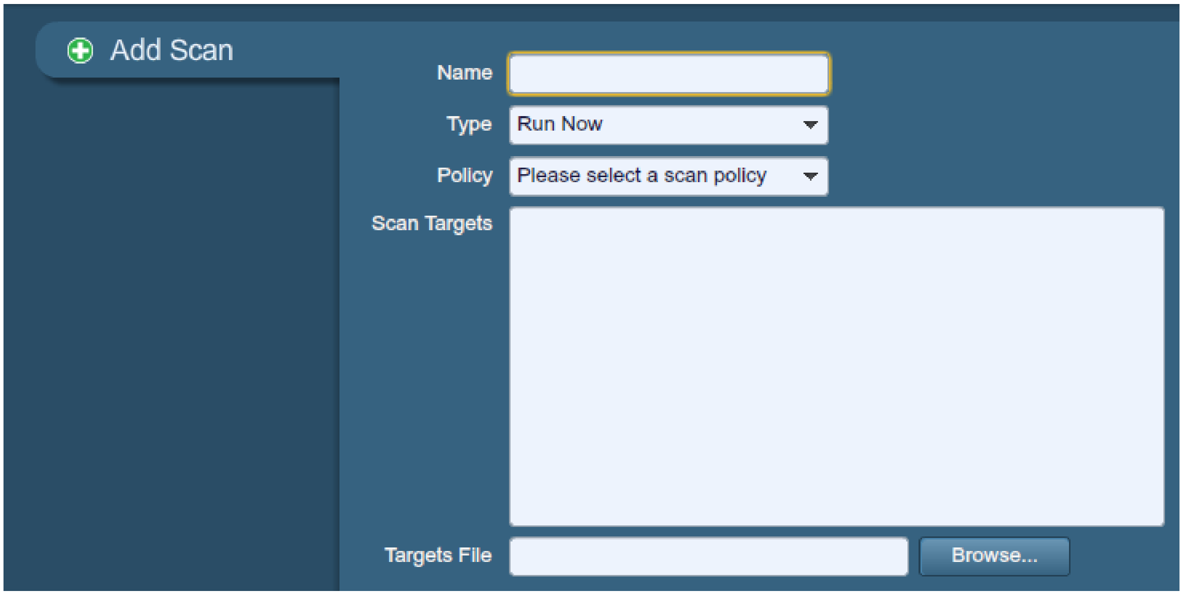
If you want to create a policy similar to an existing policy with minor modifications, you can select the base policy in the list and click on "**Copy**" on the upper right menu bar. This will create a copy of the original policy that can be edited to make any required modifications. This is useful for creating standard policies with minor changes as required for a given environment.

CREATING, LAUNCHING, AND SCHEDULING A SCAN



Name	Owner	Status	Start Time
Linux - Jedi	admin	Template	Never
Windows - Main Comp	admin	Template	Never
Windows - Media Comp	admin	Template	Never
Tenable Laptop	admin	Template	Never

After creating a policy, you can create a new scan by clicking on the "**Scans**" option on the menu bar at the top and then click on the "**+ Add**" button on the right. The "**Add Scan**" screen will be displayed as follows:



Name:

Type: Run Now

Policy: Please select a scan policy

Scan Targets:

Targets File:

There are five fields to enter the scan target:

- **Name** – Sets the name that will be displayed in the Nessus UI to identify the scan.
- **Type** – Choose between "Run Now" (immediately execute the scan after submitting), "Scheduled" (choose the time the scan should begin), or "Template" (save as a template for repeat scanning).
- **Policy** – Select a previously created policy that the scan will use to set parameters controlling Nessus server scanning behavior.
- **Scan Targets** – Targets can be entered by single IP address (e.g., 192.168.0.1), IP range (e.g., 192.168.0.1-192.168.0.255), subnet with CIDR notation (e.g., 192.168.0.0/24), or resolvable host (e.g., www.nessus.org).
- **Targets File** – A text file with a list of hosts can be imported by clicking on "**Browse...**" and selecting a file from the local machine.

⚠ The host file must be formatted as ASCII text with one host per line and no extra spaces or lines. Unicode/UTF-8 encoding is not supported.

Example host file formats:

Individual hosts:

```
192.168.0.100
192.168.0.101
192.168.0.102
```

Host range:

```
192.168.0.100-192.168.0.102
```

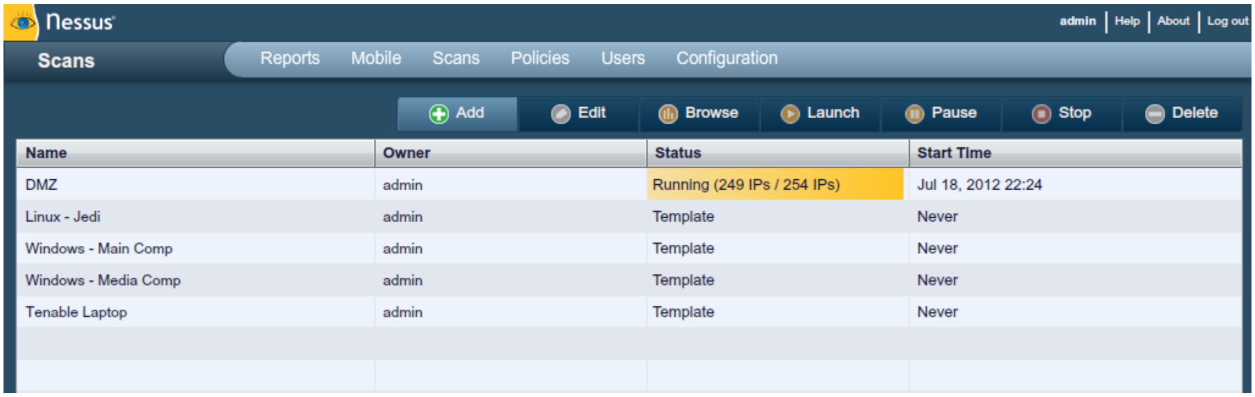
Host CIDR block:

```
192.168.0.1/24
```

Virtual servers:

```
www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]
```

After you have entered the scan information, click "**Submit**". After submitting, the scan will begin immediately (if "Run Now" was selected) before the display is returned to the general "**Scans**" page.

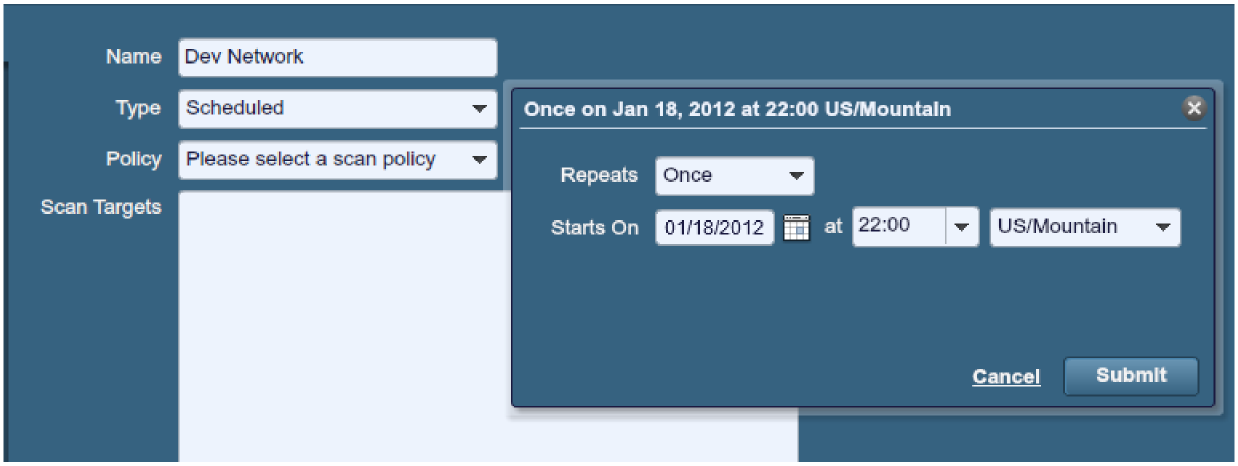


Name	Owner	Status	Start Time
DMZ	admin	Running (249 IPs / 254 IPs)	Jul 18, 2012 22:24
Linux - Jedi	admin	Template	Never
Windows - Main Comp	admin	Template	Never
Windows - Media Comp	admin	Template	Never
Tenable Laptop	admin	Template	Never

Once a scan has launched, the Scans list will display a list of all scans currently running, paused, or templated, along with basic information about the scan. After selecting a particular scan on the list, the action buttons on the top right allow you to "**Browse**" the results of the scan in progress, "**Pause**" and "**Resume**" the scan or "**Stop**" and "**Delete**" the scan completely. Users can also "**Edit**" template scans.

When a scan has completed (for any reason), it will be removed from the "**Scans**" list and be available for review on the "**Reports**" tab.

If a scan is designated as "Scheduled", an option will appear to set the desired start time and frequency:



Name: Dev Network

Type: Scheduled

Policy: Please select a scan policy

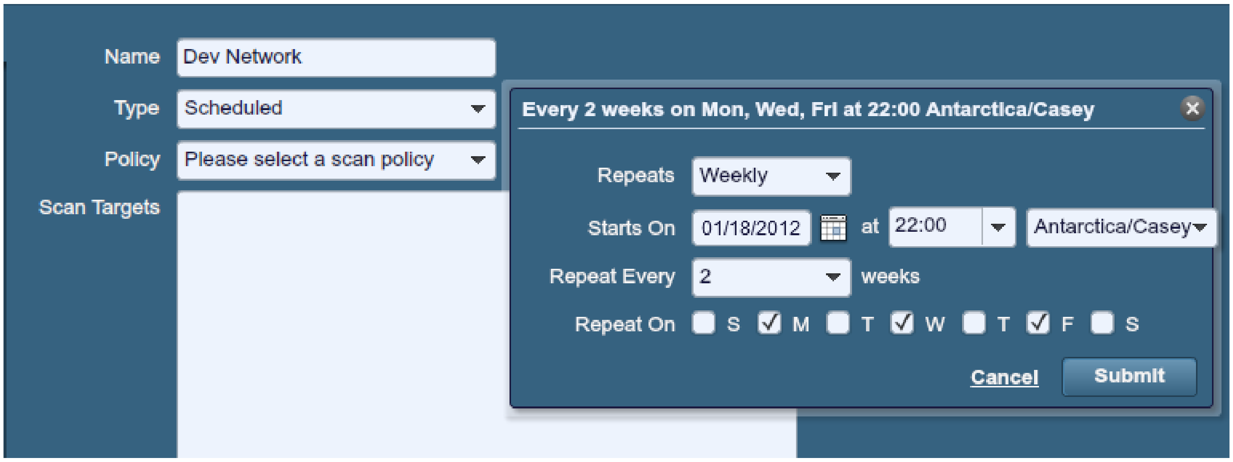
Scan Targets

Once on Jan 18, 2012 at 22:00 US/Mountain

Repeats: Once

Starts On: 01/18/2012 at 22:00 US/Mountain

Using the "Repeats" drop-down menu, a scan can be scheduled to run once, daily, weekly, monthly, or yearly. This choice can be further be specified to begin on a specific day and time. Once the scan is saved, Nessus will launch the scan at the time specified.



Name: Dev Network

Type: Scheduled

Policy: Please select a scan policy

Scan Targets

Every 2 weeks on Mon, Wed, Fri at 22:00 Antarctica/Casey

Repeats: Weekly

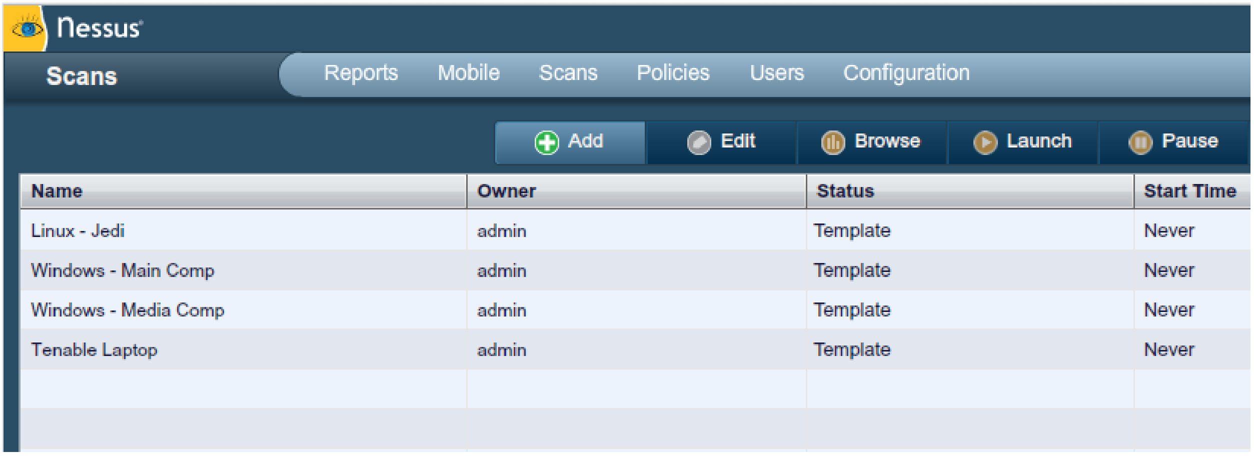
Starts On: 01/18/2012 at 22:00 Antarctica/Casey

Repeat Every: 2 weeks

Repeat On: □ S ☑ M □ T ☑ W □ T ☑ F □ S

Scheduled scans are only available to ProfessionalFeed customers.

If a scan is saved as a template, it will appear in the scan list as such and wait to be launched.

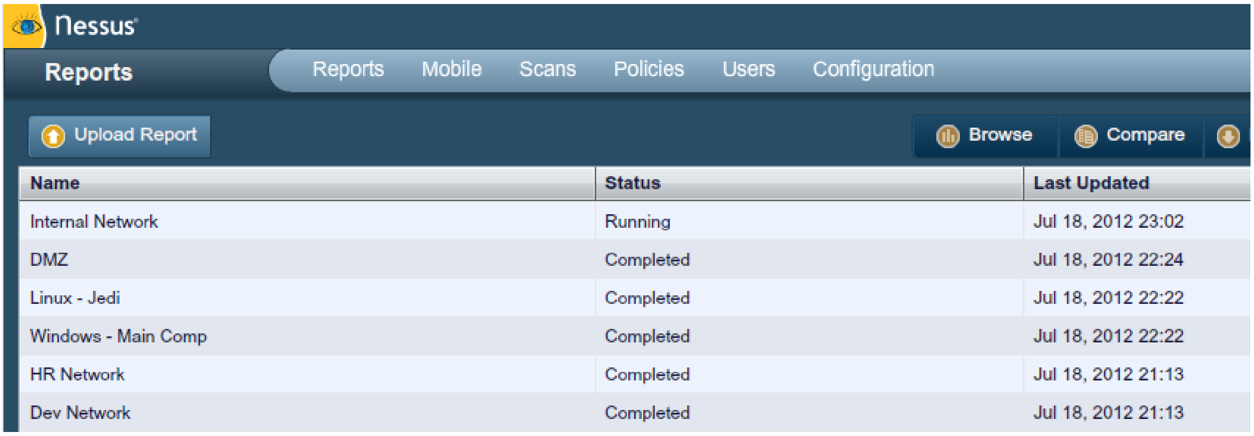


Name	Owner	Status	Start Time
Linux - Jedi	admin	Template	Never
Windows - Main Comp	admin	Template	Never
Windows - Media Comp	admin	Template	Never
Tenable Laptop	admin	Template	Never

Reports

With the release of Nessus 5, users can create their own report by chapters: Vulnerability Centric, Host Centric, Compliance, or Compliance Executive. The HTML format is still supported by default; however if Java is installed on the scanner host, it is also possible to export reports in PDF. By using the report filters and export features, users can create dynamic reports of their own choosing instead of selecting from a specific list.

Clicking on the "**Reports**" tab on the menu bar at the top of the interface will bring up the list of running and completed scans:

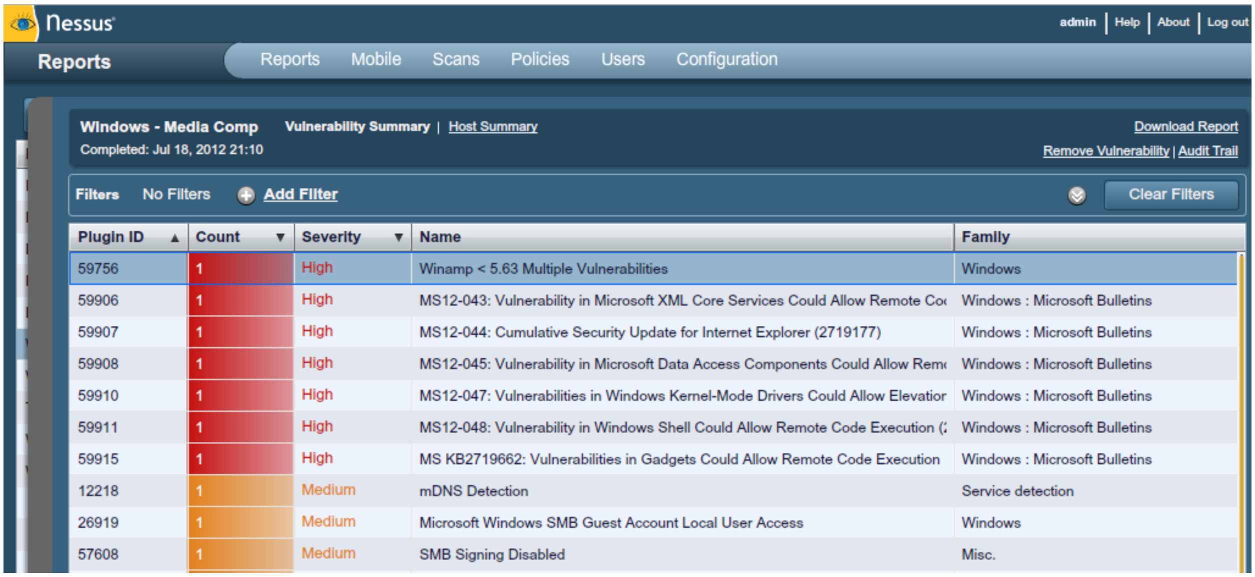


Name	Status	Last Updated
Internal Network	Running	Jul 18, 2012 23:02
DMZ	Completed	Jul 18, 2012 22:24
Linux - Jedi	Completed	Jul 18, 2012 22:22
Windows - Main Comp	Completed	Jul 18, 2012 22:22
HR Network	Completed	Jul 18, 2012 21:13
Dev Network	Completed	Jul 18, 2012 21:13

The "**Reports**" screen acts as a central point for viewing, comparing, uploading, and downloading scan results. Use the "Shift" or "Ctrl" key, to select multiple reports at one time.

Browse

To browse the results of a scan, select a name from the "**Reports**" list and click on "**Browse**". This allows you to view results by navigating through vulnerabilities or hosts, displaying ports and specific vulnerability information. The default view is by vulnerability summary, which shows each vulnerability found sorted by severity:



Nessus
admin | Help | About | Log out
Reports
Reports Mobile Scans Policies Users Configuration

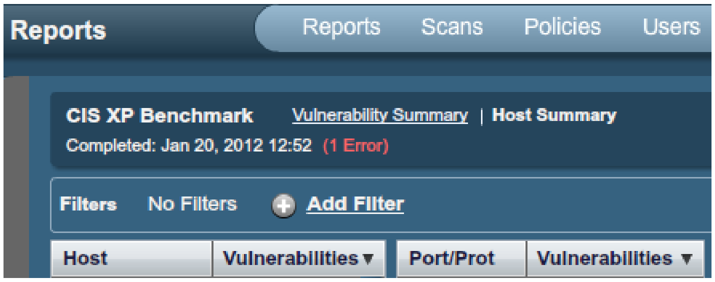
Windows - Media Comp Vulnerability Summary | Host Summary

Completed: Jul 18, 2012 21:10

Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter Clear Filters

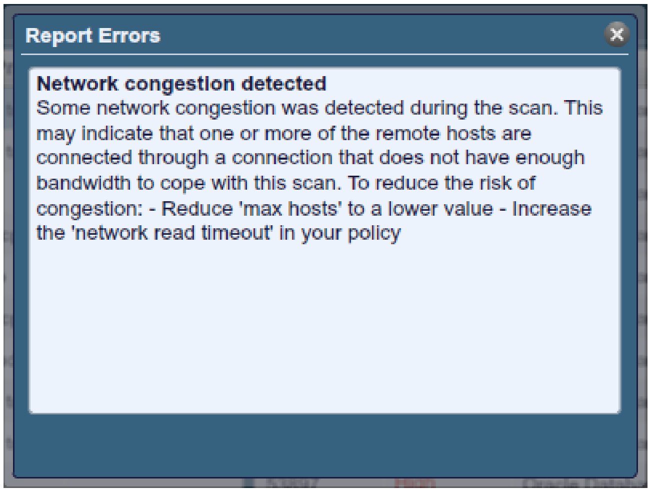
Plugin ID ▲	Count ▼	Severity ▼	Name	Family
59756	1	High	Winamp < 5.63 Multiple Vulnerabilities	Windows
59906	1	High	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Coc	Windows : Microsoft Bulletins
59907	1	High	MS12-044: Cumulative Security Update for Internet Explorer (2719177)	Windows : Microsoft Bulletins
59908	1	High	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Rem	Windows : Microsoft Bulletins
59910	1	High	MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevatior	Windows : Microsoft Bulletins
59911	1	High	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (:	Windows : Microsoft Bulletins
59915	1	High	MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution	Windows : Microsoft Bulletins
12218	1	Medium	mDNS Detection	Service detection
26919	1	Medium	Microsoft Windows SMB Guest Account Local User Access	Windows
57608	1	Medium	SMB Signing Disabled	Misc.

If any errors occurred during the scan, there will be a notation next to the "Completed" date. Clicking on the error will provide more information:



CIS XP Benchmark Vulnerability Summary | Host Summary

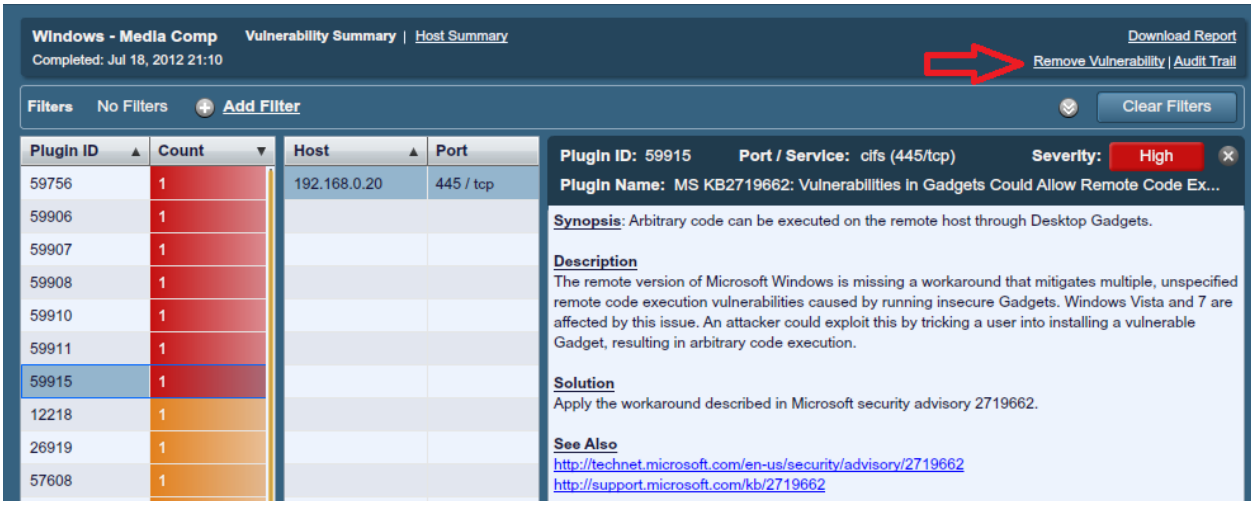
Completed: Jan 20, 2012 12:52 (1 Error)



Report Errors

Network congestion detected
Some network congestion was detected during the scan. This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to cope with this scan. To reduce the risk of congestion: - Reduce 'max hosts' to a lower value - Increase the 'network read timeout' in your policy

From the "**Vulnerability Summary**" view, the user can selectively remove vulnerabilities from the report. By selecting a vulnerability, additional information such as the affected host(s) and port(s) will display, along with technical details of the vulnerability. In the upper right corner, "**Remove Vulnerability**" can be used to delete the selected vulnerability:


Windows - Media Comp
Vulnerability Summary | Host Summary
Completed: Jul 18, 2012 21:10
Download Report
Remove Vulnerability | Audit Trail
Filters
No Filters
Add Filter
Clear Filters

Plugin ID	Count
59756	1
59906	1
59907	1
59908	1
59910	1
59911	1
59915	1
12218	1
26919	1
57608	1

Host	Port
192.168.0.20	445 / tcp

Plugin ID: 59915 **Port / Service:** cifs (445/tcp) **Severity:** High

Plugin Name: MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Ex...

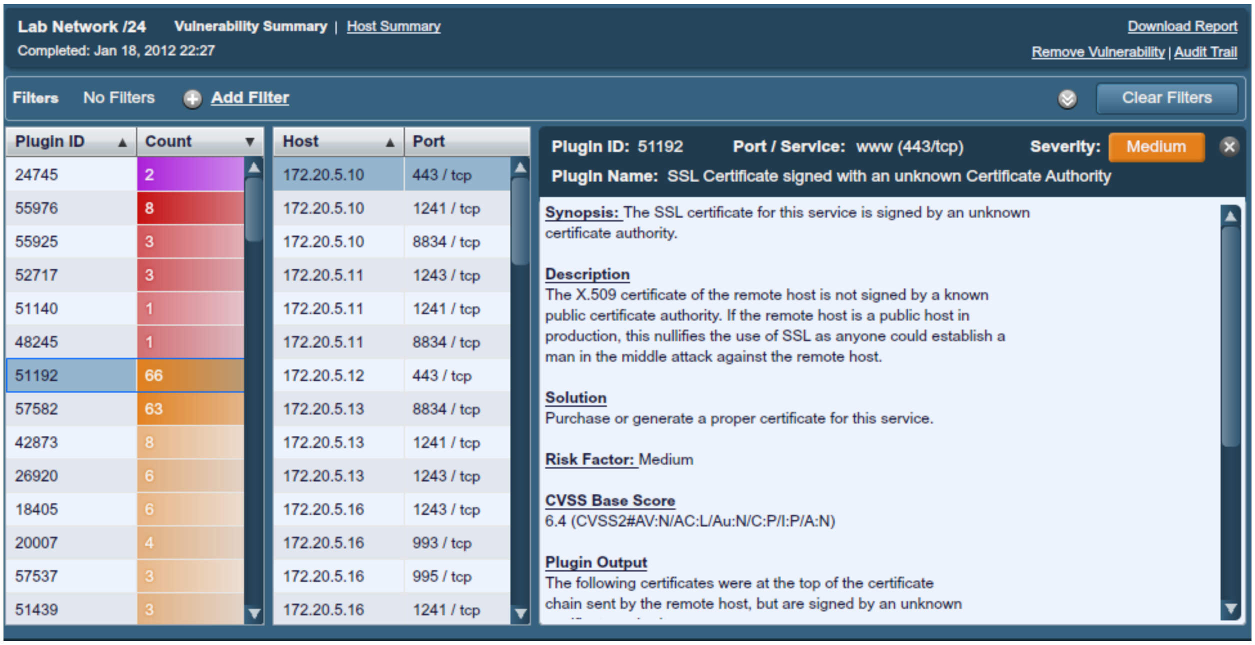
Synopsis: Arbitrary code can be executed on the remote host through Desktop Gadgets.

Description
The remote version of Microsoft Windows is missing a workaround that mitigates multiple, unspecified remote code execution vulnerabilities caused by running insecure Gadgets. Windows Vista and 7 are affected by this issue. An attacker could exploit this by tricking a user into installing a vulnerable Gadget, resulting in arbitrary code execution.

Solution
Apply the workaround described in Microsoft security advisory 2719662.

See Also
http://technet.microsoft.com/en-us/security/advisory/2719662
http://support.microsoft.com/kb/2719662

As you navigate through the scan results, the user interface will display a list of affected hosts and ports as well as additional information about the vulnerability:


Lab Network /24
Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27
Download Report
Remove Vulnerability | Audit Trail
Filters
No Filters
Add Filter
Clear Filters

Plugin ID	Count
24745	2
55976	8
55925	3
52717	3
51140	1
48245	1
51192	66
57582	63
42873	8
26920	6
18405	6
20007	4
57537	3
51439	3

Host	Port
172.20.5.10	443 / tcp
172.20.5.10	1241 / tcp
172.20.5.10	8834 / tcp
172.20.5.11	1243 / tcp
172.20.5.11	1241 / tcp
172.20.5.11	8834 / tcp
172.20.5.12	443 / tcp
172.20.5.13	8834 / tcp
172.20.5.13	1241 / tcp
172.20.5.13	1243 / tcp
172.20.5.16	1243 / tcp
172.20.5.16	993 / tcp
172.20.5.16	995 / tcp
172.20.5.16	1241 / tcp

Plugin ID: 51192 **Port / Service:** www (443/tcp) **Severity:** Medium

Plugin Name: SSL Certificate signed with an unknown Certificate Authority

Synopsis: The SSL certificate for this service is signed by an unknown certificate authority.

Description
The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

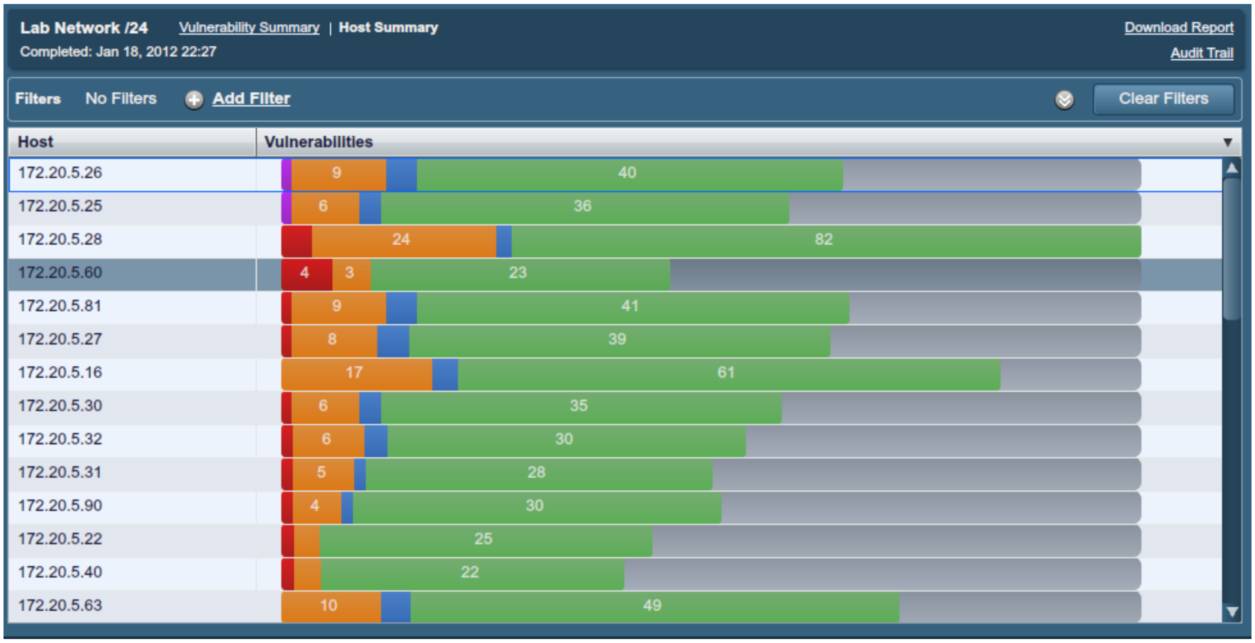
Solution
Purchase or generate a proper certificate for this service.

Risk Factor: Medium

CVSS Base Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Output
The following certificates were at the top of the certificate chain sent by the remote host, but are signed by an unknown

To switch views between vulnerability summary and host summary, select which view you want at the top of the screen next to the scan name:



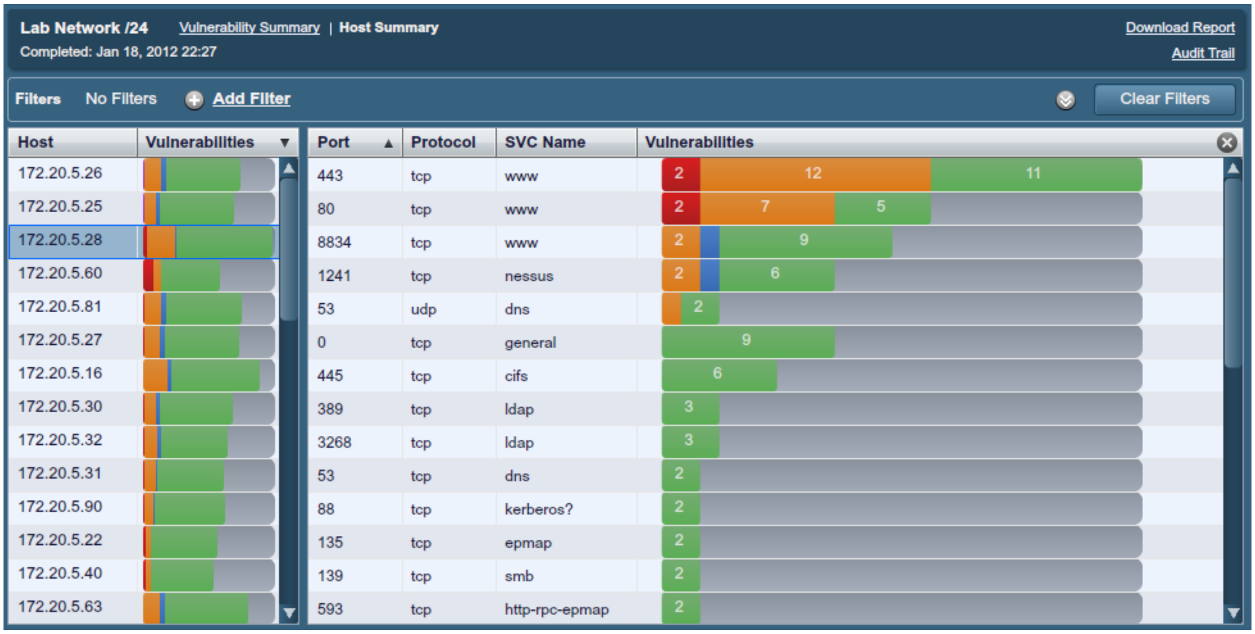
Lab Network /24 Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27

Download Report
Audit Trail

Filters No Filters Add Filter Clear Filters

Host	Vulnerabilities
172.20.5.26	9 40
172.20.5.25	6 36
172.20.5.28	24 82
172.20.5.60	4 3 23
172.20.5.81	9 41
172.20.5.27	8 39
172.20.5.16	17 61
172.20.5.30	6 35
172.20.5.32	6 30
172.20.5.31	5 28
172.20.5.90	4 30
172.20.5.22	25
172.20.5.40	22
172.20.5.63	10 49

Selecting a host will display all of the vulnerability findings associated with that host by port:



Lab Network /24 Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27

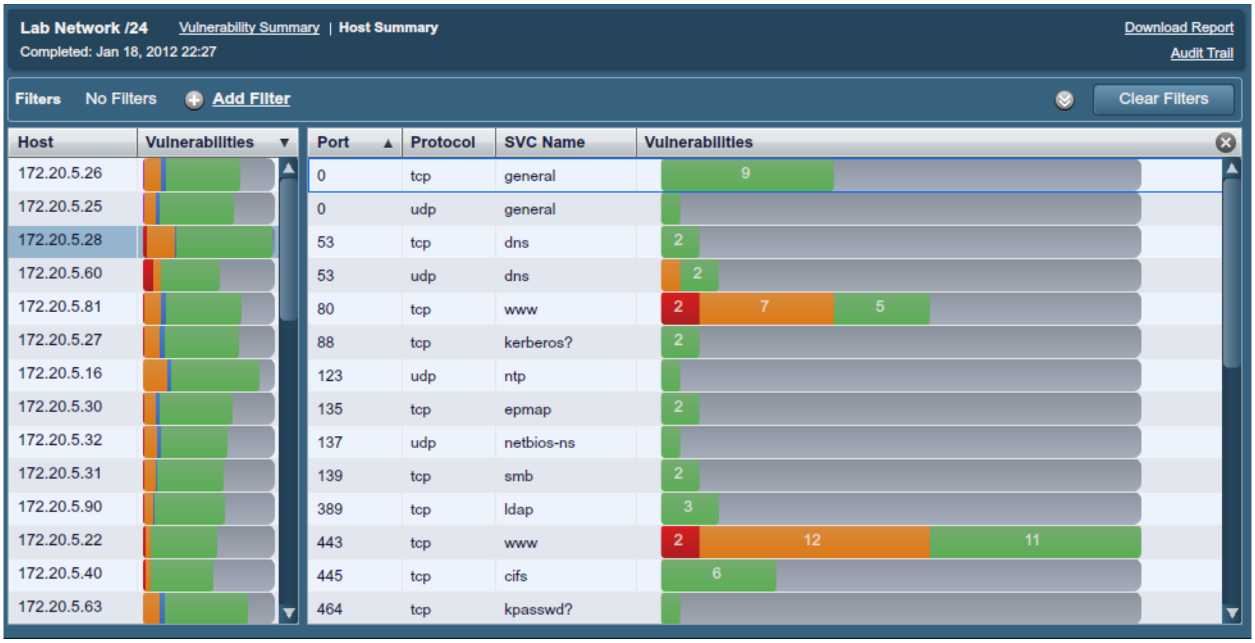
Download Report
Audit Trail

Filters No Filters Add Filter Clear Filters

Host	Vulnerabilities
172.20.5.26	
172.20.5.25	
172.20.5.28	
172.20.5.60	
172.20.5.81	
172.20.5.27	
172.20.5.16	
172.20.5.30	
172.20.5.32	
172.20.5.31	
172.20.5.90	
172.20.5.22	
172.20.5.40	
172.20.5.63	

Port	Protocol	SVC Name	Vulnerabilities
443	tcp	www	2 12 11
80	tcp	www	2 7 5
8834	tcp	www	2 9
1241	tcp	nessus	2 6
53	udp	dns	2
0	tcp	general	9
445	tcp	cifs	6
389	tcp	ldap	3
3268	tcp	ldap	3
53	tcp	dns	2
88	tcp	kerberos?	2
135	tcp	epmap	2
139	tcp	smb	2
593	tcp	http-rpc-epmap	2

In the example above, we see that host 172.20.5.60 has 30 vulnerabilities and 82 informative plugins associated with it. For each port, the protocol, service name, and a colored representation of vulnerabilities associated with the port is displayed. By clicking once on any column heading, the results can be sorted by the column's content. Clicking a second time will reverse sort the results:

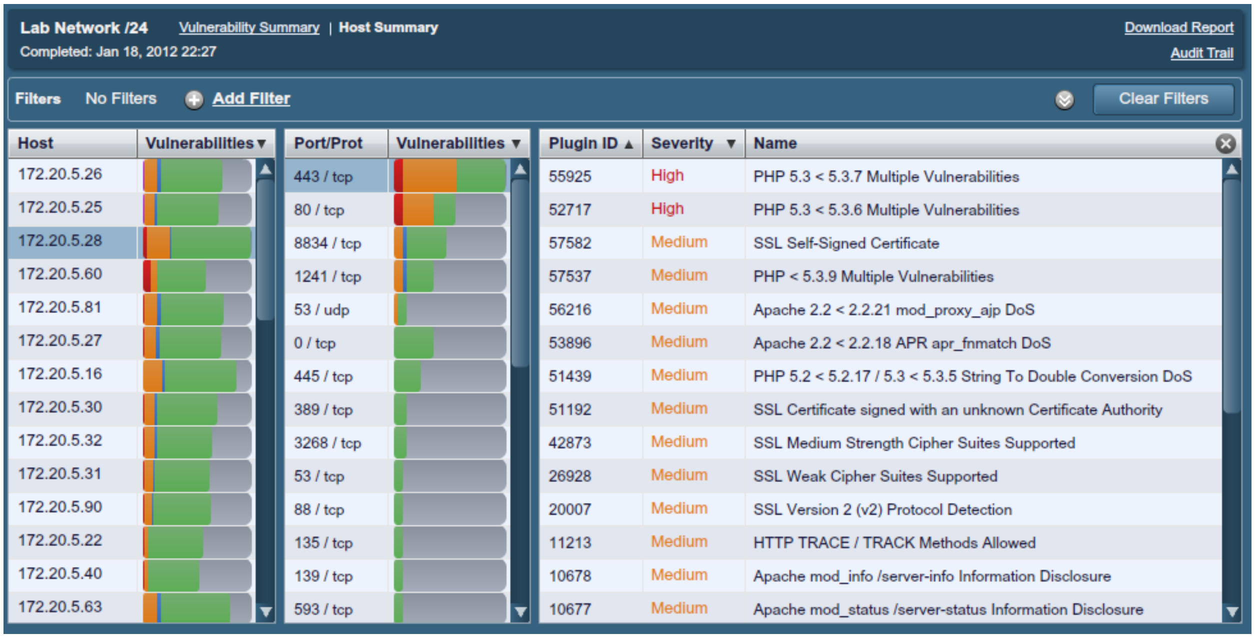


Lab Network /24 Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27

Host	Vulnerabilities ▼
172.20.5.26	
172.20.5.25	
172.20.5.28	
172.20.5.60	
172.20.5.81	
172.20.5.27	
172.20.5.16	
172.20.5.30	
172.20.5.32	
172.20.5.31	
172.20.5.90	
172.20.5.22	
172.20.5.40	
172.20.5.63	

Port ▲	Protocol	SVC Name	Vulnerabilities
0	tcp	general	9
0	udp	general	
53	tcp	dns	2
53	udp	dns	2
80	tcp	www	2 7 5
88	tcp	kerberos?	2
123	udp	ntp	
135	tcp	epmap	2
137	udp	netbios-ns	
139	tcp	smb	2
389	tcp	ldap	3
443	tcp	www	2 12 11
445	tcp	cifs	6
464	tcp	kpasswd?	

Selecting a port from the list will display the list of vulnerabilities associated with it, along with the plugin ID and severity:



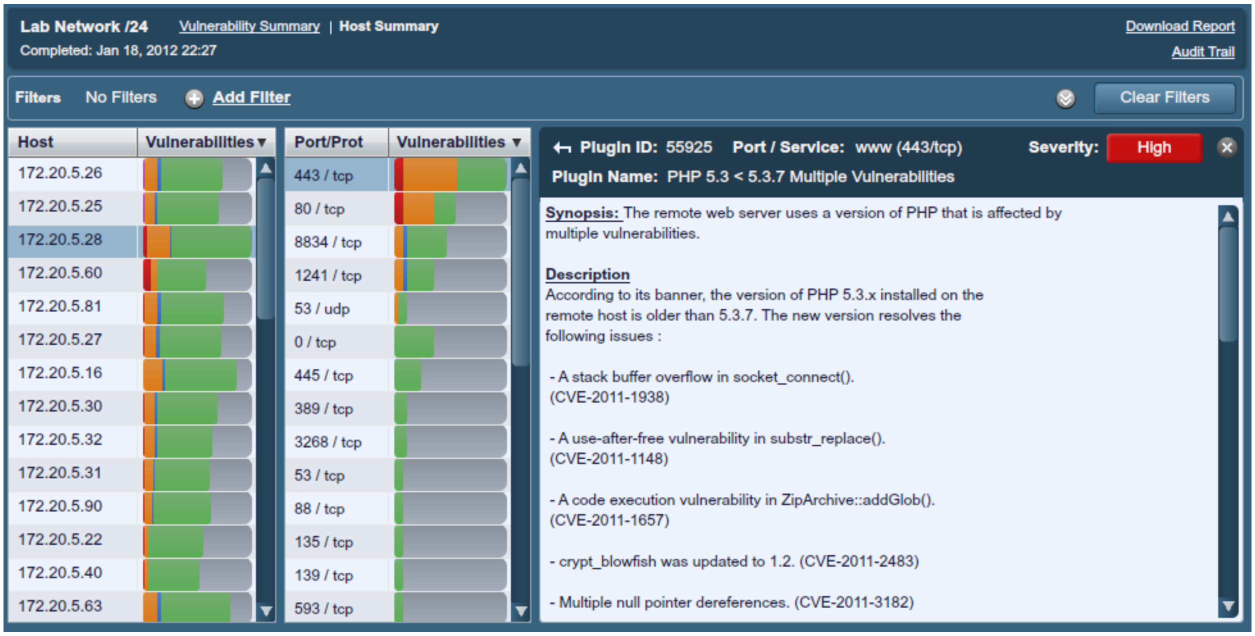
Lab Network /24 Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27

Host	Vulnerabilities ▼
172.20.5.26	
172.20.5.25	
172.20.5.28	
172.20.5.60	
172.20.5.81	
172.20.5.27	
172.20.5.16	
172.20.5.30	
172.20.5.32	
172.20.5.31	
172.20.5.90	
172.20.5.22	
172.20.5.40	
172.20.5.63	

Port/Prot	Vulnerabilities ▼
443 / tcp	
80 / tcp	
8834 / tcp	
1241 / tcp	
53 / udp	
0 / tcp	
445 / tcp	
389 / tcp	
3268 / tcp	
53 / tcp	
88 / tcp	
135 / tcp	
139 / tcp	
593 / tcp	

Plugin ID ▲	Severity ▼	Name
55925	High	PHP 5.3 < 5.3.7 Multiple Vulnerabilities
52717	High	PHP 5.3 < 5.3.6 Multiple Vulnerabilities
57582	Medium	SSL Self-Signed Certificate
57537	Medium	PHP < 5.3.9 Multiple Vulnerabilities
56216	Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS
53896	Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS
51439	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
51192	Medium	SSL Certificate signed with an unknown Certificate Authority
42873	Medium	SSL Medium Strength Cipher Suites Supported
26928	Medium	SSL Weak Cipher Suites Supported
20007	Medium	SSL Version 2 (v2) Protocol Detection
11213	Medium	HTTP TRACE / TRACK Methods Allowed
10678	Medium	Apache mod_info /server-info Information Disclosure
10677	Medium	Apache mod_status /server-status Information Disclosure

Clicking on a vulnerability will display details about it including a synopsis, description, solution, third-party references, risk factor, CVSS scores, plugin output (if applicable), a set of dates related to the plugin and vulnerability, and if a public exploit is available in some capacity (e.g., public or exploit framework):



Lab Network /24 Vulnerability Summary | Host Summary

Completed: Jan 18, 2012 22:27

Download Report

Audit Trail

Filters No Filters Add Filter Clear Filters

Host	Vulnerabilities ▾
172.20.5.26	
172.20.5.25	
172.20.5.28	
172.20.5.60	
172.20.5.81	
172.20.5.27	
172.20.5.16	
172.20.5.30	
172.20.5.32	
172.20.5.31	
172.20.5.90	
172.20.5.22	
172.20.5.40	
172.20.5.63	

Port/Prot	Vulnerabilities ▾
443 / tcp	
80 / tcp	
8834 / tcp	
1241 / tcp	
53 / udp	
0 / tcp	
445 / tcp	
389 / tcp	
3268 / tcp	
53 / tcp	
88 / tcp	
135 / tcp	
139 / tcp	
593 / tcp	

Plugin ID: 55925 Port / Service: www (443/tcp) Severity: High

Plugin Name: PHP 5.3 < 5.3.7 Multiple Vulnerabilities

Synopsis: The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is older than 5.3.7. The new version resolves the following issues :

- A stack buffer overflow in socket_connect(). (CVE-2011-1938)

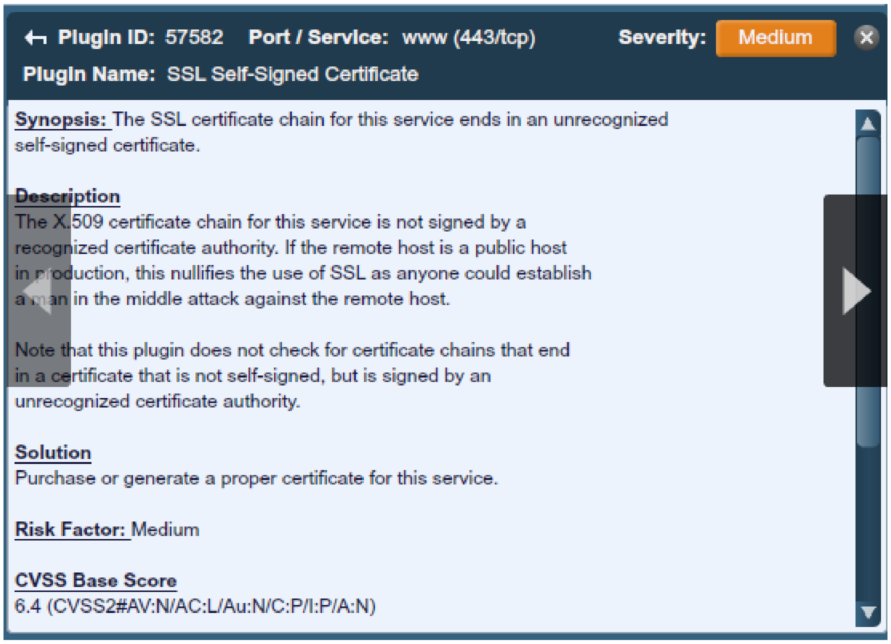
- A use-after-free vulnerability in substr_replace(). (CVE-2011-1148)

- A code execution vulnerability in ZipArchive::addGlob(). (CVE-2011-1657)

- crypt_blowfish was updated to 1.2. (CVE-2011-2483)

- Multiple null pointer dereferences. (CVE-2011-3182)

The vulnerability detail screen provides a navigation arrow on each side to quickly cycle through each vulnerability:



Plugin ID: 57582 Port / Service: www (443/tcp) Severity: Medium

Plugin Name: SSL Self-Signed Certificate

Synopsis: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor: Medium

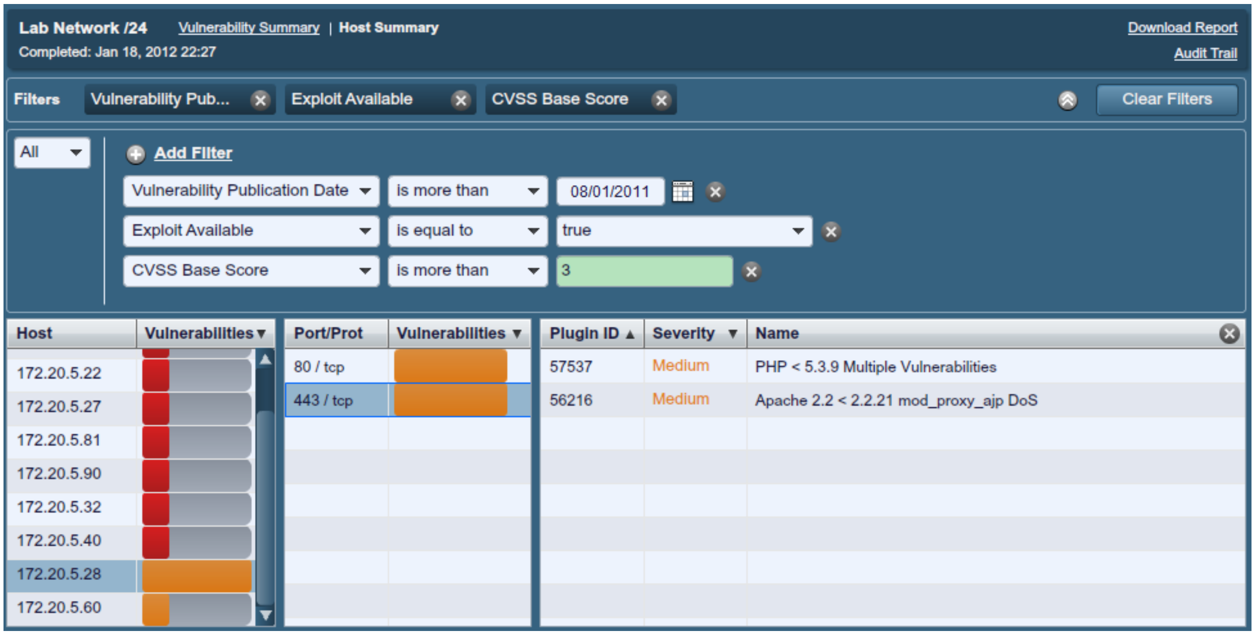
CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Report Filters

Nessus offers a flexible system of filters to assist in displaying specific report results. Filters can be used to display results based on any aspect of the vulnerability findings. When multiple filters are used, more detailed and customized report views can be created.

To create a filter, begin by clicking on "**Add Filter**" above the report results. Filters can be created from the report summary, host, or port level breakdown screens. Multiple filters can be created with logic that allows for complex filtering. A filter is created by selecting the plugin attribute, a filter argument, and a value to filter on. When selecting multiple filters, they keyword “Any” or “All” should be specified accordingly. If “All” is selected, then only results that match **all** filters will be displayed:



Lab Network /24 | Vulnerability Summary | Host Summary | Download Report
Completed: Jan 18, 2012 22:27 | Audit Trail

Filters: Vulnerability Pub... | Exploit Available | CVSS Base Score | Clear Filters

All | Add Filter

Vulnerability Publication Date	is more than	08/01/2011
Exploit Available	is equal to	true
CVSS Base Score	is more than	3

Host
172.20.5.22
172.20.5.27
172.20.5.81
172.20.5.90
172.20.5.32
172.20.5.40
172.20.5.28
172.20.5.60

Port/Prot
80 / tcp
443 / tcp

Plugin ID	Severity	Name
57537	Medium	PHP < 5.3.9 Multiple Vulnerabilities
56216	Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS

Once a filter has been set, it can be removed individually by clicking on the ☒ to the right or on the filter button above. Additionally, all filters can be removed at the same time by selecting “Clear Filters”. The report filters allow for a wide variety of criteria for granular control of results:

Option	Description
Plugin ID	Filter results if Plugin ID “*is equal to*”, “*is not equal to*”, “*contains*”, or “*does not contain*” a given string (e.g., 42111).
Plugin Description	Filter results if Plugin Description “*contains*”, or “*does not contain*” a given string (e.g., “remote”).
Plugin Name	Filter results if Plugin Name “*is equal to*”, “*is not equal to*”, “*contains*”, or “*does not contain*” a given string (e.g., “windows”).
Plugin Family	Filter results if Plugin Name “*is equal to*” or “*is not equal to*” one of the designated Nessus plugin families. The possible matches are provided via a drop-down menu.
Plugin Output	Filter results if Plugin Description “*is equal to*”, “*is not equal to*”, “*contains*”, or “*does not contain*” a given string (e.g., “PHP”)
Plugin Type	Filter results if Plugin Type “*is equal to*” or “*is not equal to*” one of the two types of plugins: local or remote.
Solution	Filter results if the plugin Solution “*contains*” or “*does not contain*” a given string (e.g., “upgrade”).

Synopsis	Filter results if the plugin Solution "*contains*" or "*does not contain*" a given string (e.g., "PHP").
Hostname	Filter results if the host "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "192.168" or "lab").
Port	Filter results based on if a port "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "80").
Protocol	Filter results if a protocol "*is equal to*" or "*is not equal to*" a given string (e.g., "http").
CPE	Filter results based on if the Common Platform Enumeration (CPE) "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "solaris").
CVSS Base Score	Filter results based on if a CVSS base score "*is less than*", "*is more than*", "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a string (e.g., "5"). ⚠ This filter can be used to select by risk level. The severity ratings are derived from the associated CVSS score, where 0 is "Info", less than 4 is "Low", less than 7 is "Medium", less than 10 is "High", and a CVSS score of 10 will be flagged "Critical".
CVSS Temporal Score	Filter results based on if a CVSS temporal score "*is less than*", "*is more than*", "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a string (e.g., "3.3").
CVSS Temporal Vector	Filter results based on if a CVSS temporal vector "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "E:F").
CVSS Vector	Filter results based on if a CVSS vector "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "AV:N").
Vulnerability Publication Date	Filter results based on if a vulnerability publication date "*earlier than*", "*later than*", "*on*", "*not on*", "*contains*", or "*does not contain*" a string (e.g., "01/01/2012"). Note: Pressing the 📅 button next to the date will bring up a calendar interface for easier date selection.

Patch Publication Date	Filter results based on if a vulnerability patch publication date "*is less than*", "*is more than*", "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a string (e.g., "12/01/2011").
Plugin Publication Date	Filter results based on if a Nessus plugin publication date "*is less than*", "*is more than*", "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a string (e.g., "06/03/2011").
Plugin Modification Date	Filter results based on if a Nessus plugin modification date "*is less than*", "*is more than*", "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a string (e.g., "02/14/2010").
CVE	Filter results based on if a CVE reference "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "2011-0123").
Bugtraq ID	Filter results based on if a Bugtraq ID "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "51300").
CERT Advisory ID	Filter results based on if a CERT Advisory ID (now called Technical Cyber Security Alert) "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "TA12-010A").
OSVDB ID	Filter results based on if an Open Source Vulnerability Database (OSVDB) ID "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "78300").
Secunia ID	Filter results based on if a Secunia ID "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "47650").
Exploit Database ID	Filter results based on if an Exploit Database ID (EBD-ID) reference "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "18380").
Metasploit Name	Filter results based on if a Metasploit name "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., "xslt_password_reset").
Exploit Hub	Filter results based on if an ExploitHub exploit is "*true*" or "*false*".
IAVA	Filter results based on if an IAVA reference "*is equal to*", "*is not equal to*", "*contains*", or "*does not contain*" a given string (e.g., 2012-A-0008).
See Also	Filter results based on if a Nessus plugin "see also" reference "*is equal to*", "*is not equal to*", "*contains*", or "*does not*

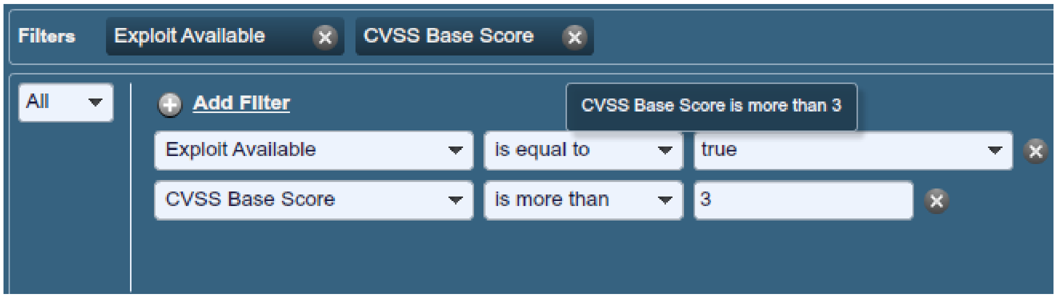
	contain" a given string (e.g., "seclists.org").
Exploits Available	Filter results based on the vulnerability having a known public exploit.
Exploitability Ease	Filter results based on if the exploitability ease "*is equal to*" or "*is not equal to*" to the following values: "*Exploits are available*", "*No exploit is required*", or "*No known exploits are available*".
Metasploit Exploit Framework	Filter results based on if the presence of a vulnerability in the Metasploit Exploit Framework "*is equal to*" true or false.

When using a filter, the string or numeric value can be comma delimited to filter based on multiple strings. For example, to filter results to show only web servers, you could create a "Ports" filter, select "is equal to" and input "80,443,8000,8080". This will show you results associated with those four ports.

Filter criteria are **not** case sensitive.

If a filter option is not available, it means that the report contains nothing that meets the criteria. For example, if "Microsoft Bulletin" is not on the filter dropdown list, then no vulnerabilities were found that reference a Microsoft Bulletin.

As filters are created, they will be listed above the filter input area. To see active filter details, mouse over the filter name:

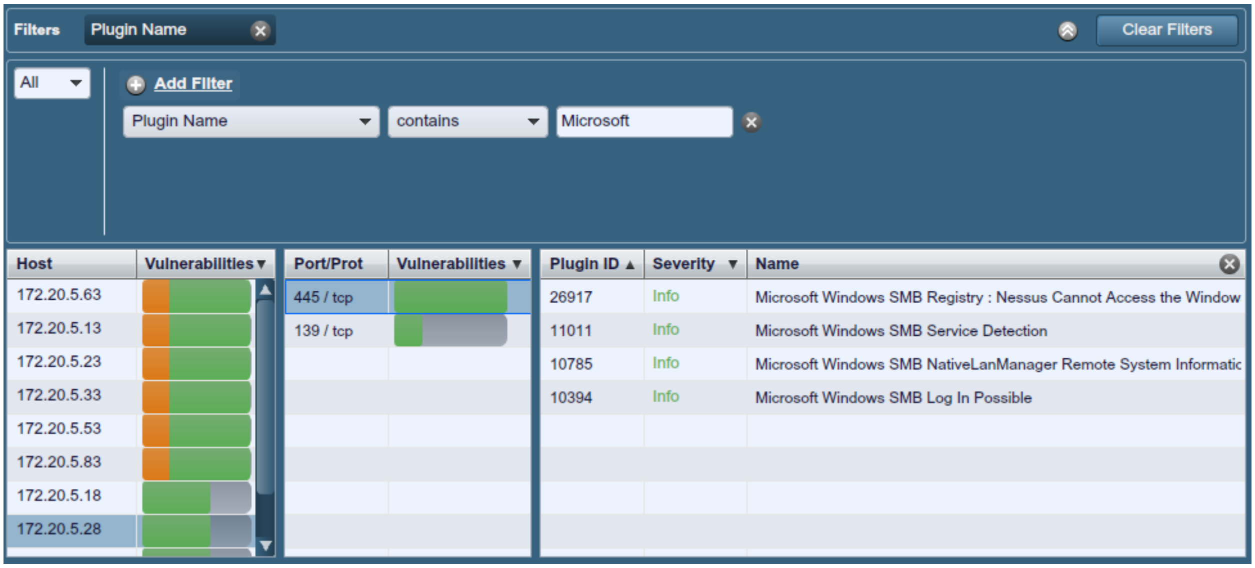


CVSS Base Score is more than 3

Exploit Available | is equal to | true

CVSS Base Score | is more than | 3

As soon as a filter is created, the scan results will be updated to reflect the new filter criteria. In the example below, creating a filter to only display results with "Microsoft" in the plugin name removes most findings:



Plugin Name | contains | Microsoft

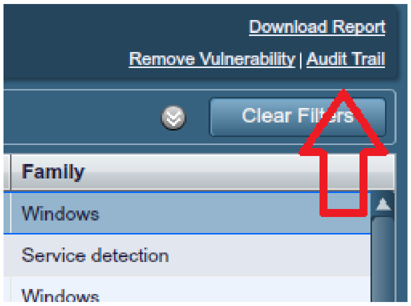
Host	Vulnerabilities ▾
172.20.5.63	
172.20.5.13	
172.20.5.23	
172.20.5.33	
172.20.5.53	
172.20.5.83	
172.20.5.18	
172.20.5.28	

Port/Prot	Vulnerabilities ▾
445 / tcp	
139 / tcp	

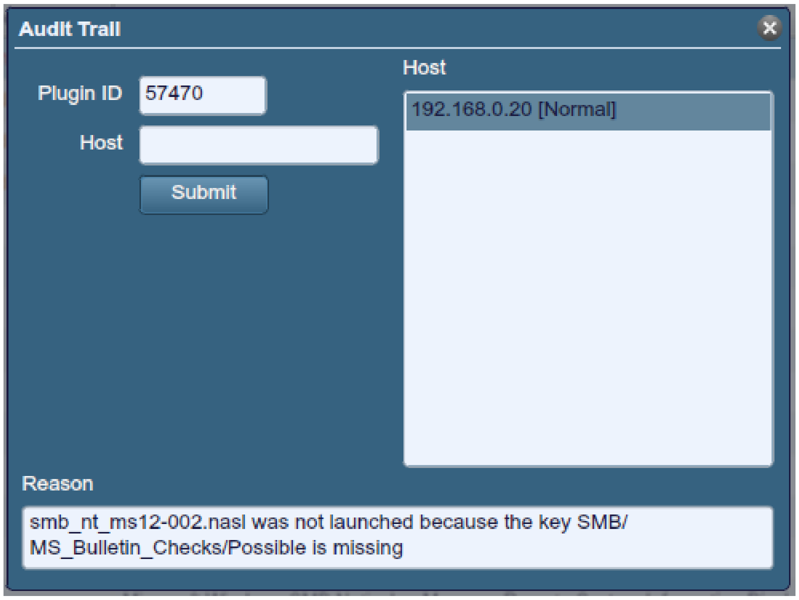
Plugin ID ▴	Severity ▾	Name
26917	Info	Microsoft Windows SMB Registry : Nessus Cannot Access the Window
11011	Info	Microsoft Windows SMB Service Detection
10785	Info	Microsoft Windows SMB NativeLanManager Remote System Informatic
10394	Info	Microsoft Windows SMB Log In Possible

Once the results have been filtered to provide the data set you want, click "**Download Report**" to export just the filtered results. To receive a report with all of the results, use the download button from the main "**Reports**" screen.

Nessus scan results give a concise list of plugins that detected issues on the host. However, there are times where you may want to know why a plugin did not return results. The "Audit Trail" functionality will provide this information. Begin by clicking "Audit Trail" in the upper right corner:



This will bring up the Audit Trail dialogue. Begin by entering the plugin ID you want to know more about. Click "Submit" and a host or list of hosts will be displayed that relates to your query. Optionally, you can supply a host IP for the initial query to limit the results to a target of interest. Once the host(s) are displayed, click on one to display information about why the plugin did not fire:



Audit Trail

Plugin ID: 57470

Host:

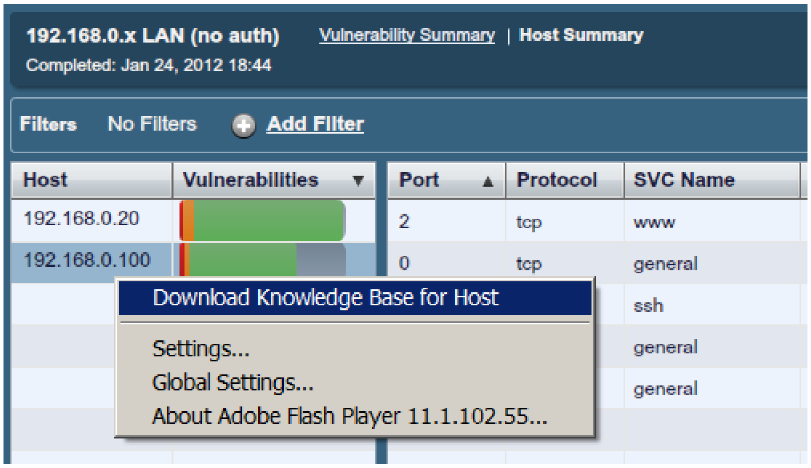
Host: 192.168.0.20 [Normal]

Reason: smb_nt_ms12-002.nasl was not launched because the key SMB/MS_Bulletin_Checks/Possible is missing

Due to the resources required for the audit trail, there are cases where only a partial audit trail will be provided. For a single scanned host, the full audit trail is available. If between 2 and 512 hosts are scanned, a full audit trail is only available if the Nessus server has more than 1 CPU and 2G of RAM. Scanning over 512 hosts will always result in a partial audit trail.

With Nessus 5, a Knowledge Base (KB) is saved with every scan performed. This is an ASCII text file containing a log of information relevant to the scan performed and results found. A KB is often useful during cases where you need support from Tenable, as it allows Support staff to understand exactly what Nessus did, and what information was found.

To download a KB, right click on a host name and select "Download Knowledge Base for Host":



192.168.0.x LAN (no auth)

Completed: Jan 24, 2012 18:44

Filters: No Filters

Host	Vulnerabilities
192.168.0.20	
192.168.0.100	

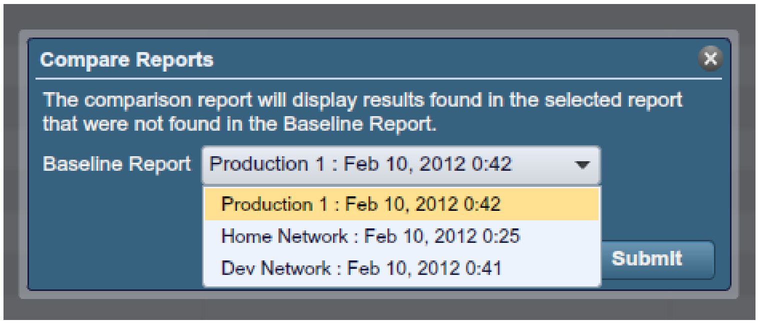
Port	Protocol	SVC Name
2	tcp	www
0	tcp	general
		ssh
		general
		general

Vulnerability Summary | Host Summary
Add Filter
Download Knowledge Base for Host
Settings...
Global Settings...
About Adobe Flash Player 11.1.102.55...

Compare

With Nessus, you can compare two scan reports against each other to display any differences. The ability to show scan differentials helps to point out how a given system or network has changed over time. This helps in analysis of compliance by showing how vulnerabilities are being remediated, if systems are patched as new vulnerabilities are found, or how two scans may not be targeting the same hosts.

To compare reports, begin by selecting a scan from the "**Reports**" list and click on "**Compare**" from the menu bar on the right. The resulting dialog menu will give you a drop-down list of other reports to compare. Select one and click on "**Submit**":



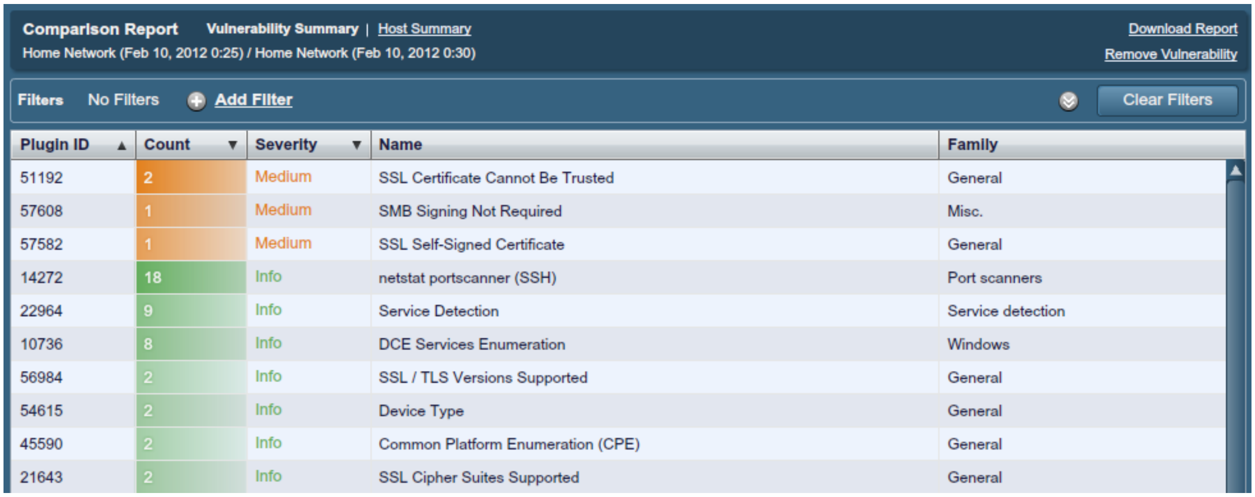
Compare Reports

The comparison report will display results found in the selected report that were not found in the Baseline Report.

Baseline Report: Production 1 : Feb 10, 2012 0:42

- Production 1 : Feb 10, 2012 0:42
- Home Network : Feb 10, 2012 0:25
- Dev Network : Feb 10, 2012 0:41

Nessus will compare the first report selected with the second, and produce a list of results that are different since the first. The compare feature shows what is new since the baseline (i.e., the first report selected), not produce a differential of any two reports. This comparison highlights which vulnerabilities have been found or remediated between the two scans. In the example above, "LAN Scan One" is a scan of the entire 192.168.0.0/24 subnet and "LAN Scan Two" is a scan of three select hosts on the 192.168.0.0/24 subnet. The "Compare" feature displays the differences, highlighting hosts that were not scanned in "LAN Scan Two":



Comparison Report — Vulnerability Summary | Host Summary

Home Network (Feb 10, 2012 0:25) / Home Network (Feb 10, 2012 0:30)

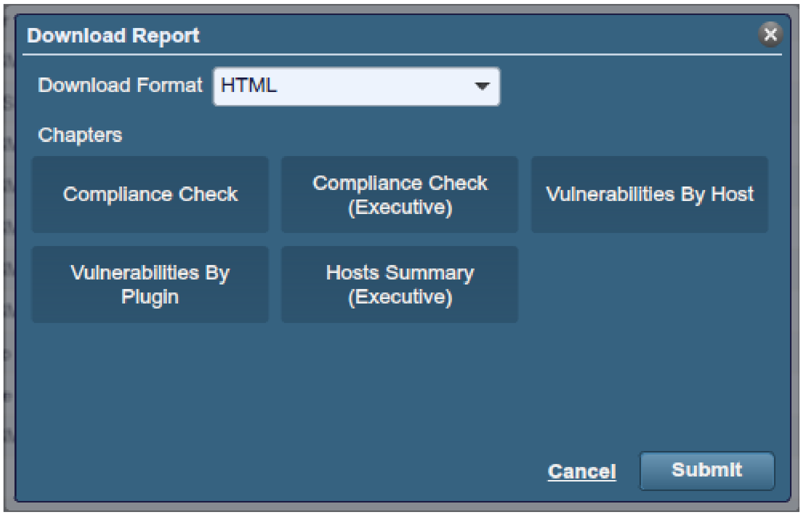
Plugin ID ▲	Count ▼	Severity ▼	Name	Family
51192	2	Medium	SSL Certificate Cannot Be Trusted	General
57608	1	Medium	SMB Signing Not Required	Misc.
57582	1	Medium	SSL Self-Signed Certificate	General
14272	18	Info	netstat portscanner (SSH)	Port scanners
22964	9	Info	Service Detection	Service detection
10736	8	Info	DCE Services Enumeration	Windows
56984	2	Info	SSL / TLS Versions Supported	General
54615	2	Info	Device Type	General
45590	2	Info	Common Platform Enumeration (CPE)	General
21643	2	Info	SSL Cipher Suites Supported	General

The "Compare" function is only available for ProfessionalFeed users.

Upload & Download

Scan results can be exported from one Nessus scanner and imported to a different Nessus scanner. The "**Upload**" and "**Download**" features facilitate better scan management, report comparison, report backup, and communication between groups or organizations within a company.

To export a scan, begin by selecting it from the "**Reports**" screen and clicking on "**Download**". This will display the report download dialog box asking which format you want, as well as specific information (broken into "chapters") that should be included. Clicking on the desired chapter will display a check mark to indicate it will be included in the report:



Download Report

Download Format: HTML

Chapters
Compliance Check
Compliance Check (Executive)
Vulnerabilities By Host
Vulnerabilities By Plugin
Hosts Summary (Executive)
Cancel
Submit

⚠ Only compliance scans performed with Nessus 5 can be exported to PDF or HTML formats with compliance chapters. Imported scans from previous versions of Nessus will not export in that manner.

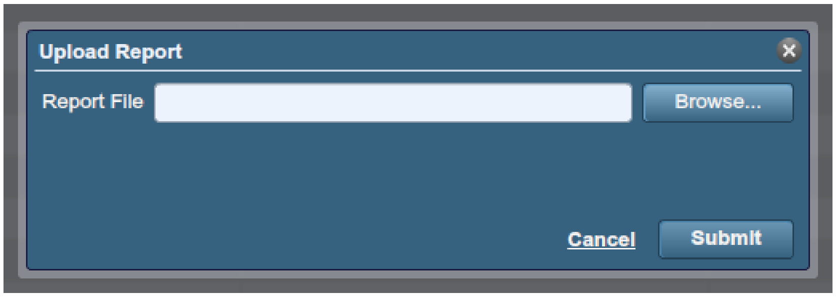
Reports can be downloaded in several formats. Note that some formats will not allow chapter selection, and include all information.

Option	Description
`.nessus`	An XML-based format and the de-facto standard in Nessus 4.2 and later. This format uses an expanded set of XML tags to make extracting and parsing information more granular. This report does not allow chapter selection.
`.nessus` **(v1)**	An XML-based format used in Nessus 3.2 through 4.0.2, compatible with Nessus 4.x and Security Center 3. This report does not allow chapter selection.
HTML	A report generated using standard HTML that allows chapter selection. This report will open in a new tab in your browser.
PDF	A report generated in PDF format that allows chapter selection. Depending on the size of the report, PDF generation may take several minutes. ⚠ Oracle Java (formerly Sun Microsystems' Java) is required for PDF report functionality.

CSV	A comma-separated values (CSV) export that can be used to import into many external programs such as databases, spreadsheets, and more. This report does not allow chapter selection.
NBE export	A pipe-delimited export that can be used to import into many external programs. This report does not allow chapter selection.

After selecting either **`.nessus`**, NBE format, or PDF, your standard web browser "Save File" dialog will be displayed, allowing you to save the scan results to the location of your choice. HTML reports will display in your browser and can be saved through the browser "File -> Save" function.

To import a report, click on the "**Upload Report**" button on the upper left side of the "**Reports**" screen:



Using the "**Browse...**" button, select the **`.nessus`** scan file you want to import and click on "**Submit**". Nessus will parse the information and make it available in the "**Reports**" interface.

.nessus File Format

Nessus uses a specific file format (**`.nessus`**) for scan export and import. This format has the following advantages:

- XML based, for easy forward and backward compatibility, and easy implementation.
- Self-sufficient: a single **`.nessus`** file contains the list of targets, the policies defined by the user, as well as the scan results themselves.
- Secure: Passwords are not saved in the file. Instead, a reference to a password stored in a secure location on the local host is used.

The process to create a **`.nessus`** file that contains the targets, policies, and scan results is to first generate the policy and save it. Next, generate the list of target addresses and finally, run a scan. Once the scan is complete, all the information can be saved in a **`.nessus`** file by using the "**Download**" option from the "**Reports**" tab. Please see the "Nessus v2 File Format" document for more details on **`.nessus`** files.

Delete

Once you are finished with scan results, you can select a scan from the "Reports" list and click on the "**Delete**" button. This will delete the scan from the user interface. **This action**

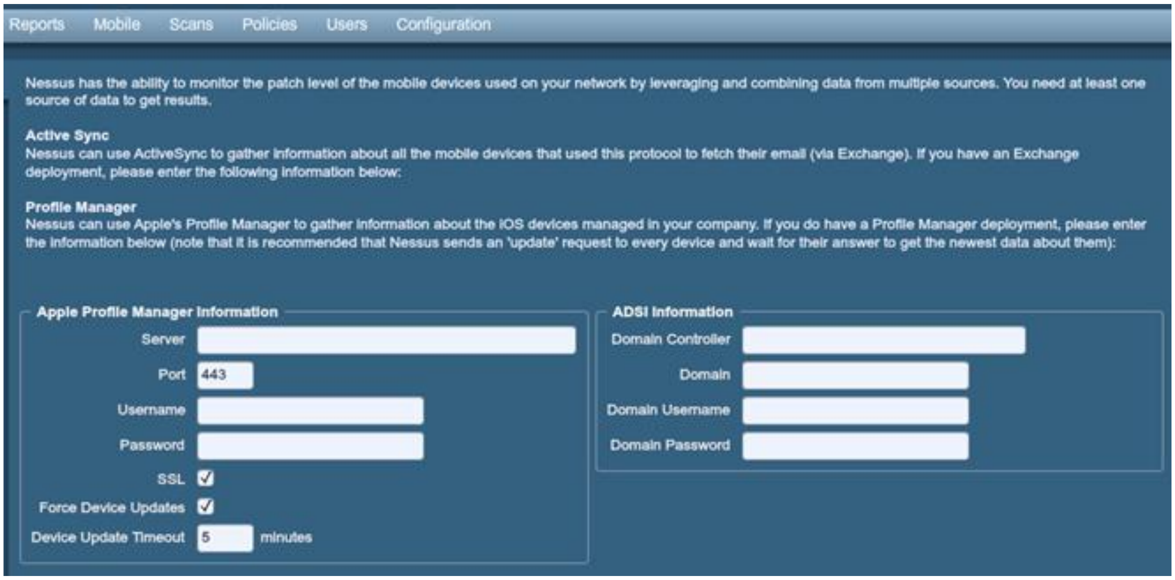
cannot be undone! Use the "**Download**" feature to export your scan results before deleting.

Mobile

Nessus 5 has the ability to scan Active Directory Service Interfaces and Apple Profile Manager, allowing for the inventory and vulnerability scanning of both Apple iOS-based and Android devices. Nessus can be configured to authenticate to these servers, query for mobile device information, and report on any issues. This can be done via a traditional scan policy, or via the "**Mobile**" tab.

To scan for mobile devices, Nessus must be configured with authentication information for the management server and/or the mobile plugins of interest. Since Nessus authenticates directly to the management servers, a scan policy does not need to be configured to scan specific hosts.

The "Mobile" tab offers one place to configure the Apple Profile Manager and ADSI information. Once the details have been added and submitted, Nessus will immediately scan these servers to retrieve mobile device information. Clicking on this tab again will re-launch a scan to poll for current information.



Nessus has the ability to monitor the patch level of the mobile devices used on your network by leveraging and combining data from multiple sources. You need at least one source of data to get results.

Active Sync
Nessus can use ActiveSync to gather information about all the mobile devices that used this protocol to fetch their email (via Exchange). If you have an Exchange deployment, please enter the following information below:

Profile Manager
Nessus can use Apple's Profile Manager to gather information about the iOS devices managed in your company. If you do have a Profile Manager deployment, please enter the information below (note that it is recommended that Nessus sends an 'update' request to every device and wait for their answer to get the newest data about them):

Apple Profile Manager Information

Server
Port 443
Username
Password
SSL ☑
Force Device Updates ☑
Device Update Timeout 5 minutes

ADSI Information

Domain Controller
Domain
Domain Username
Domain Password

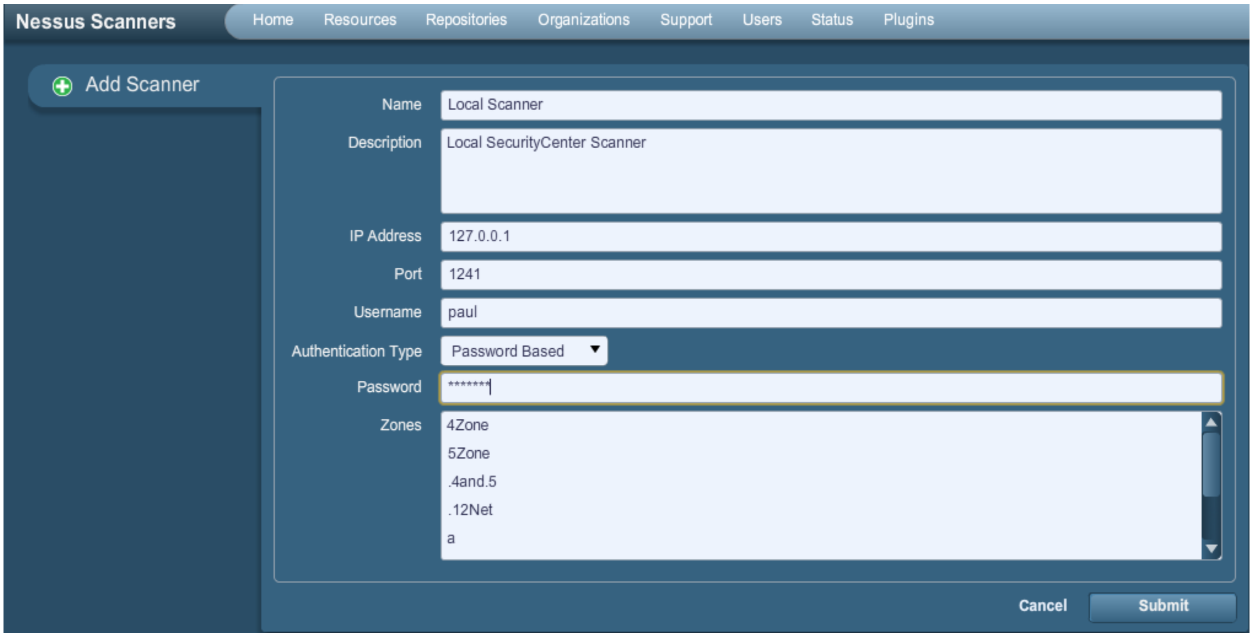
The only information required to launch a basic mobile device scan is the Active Directory or MDM server information. Upon completing this information, a scan will launch, and results can be viewed in the "**Reports**" tab.

SecurityCenter

Configuring SecurityCenter 4.0-4.2 to Work with Nessus

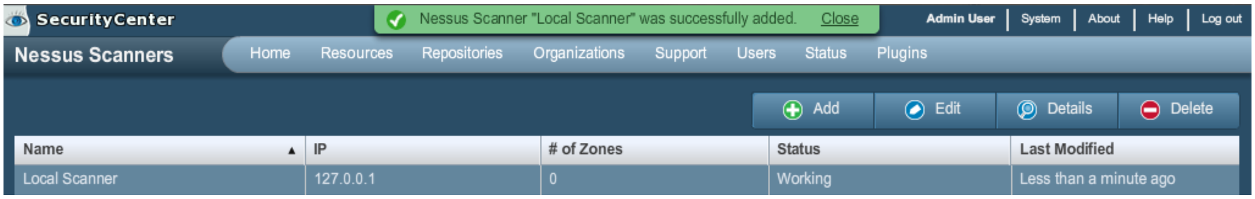
A "Nessus Server" can be added through the SecurityCenter administration interface. Using this interface, SecurityCenter can be configured to access and control virtually any Nessus scanner. Click the "Resources" tab and then click "**Nessus Scanners**". Click "**Add**" to open the "Add Scanner" dialog. The Nessus scanner's IP address, Nessus port (default: 1241), administrative login ID, authentication type, and password (created while configuring Nessus) are required. The password fields are not available if "SSL Certificate" authentication is selected. In addition, Zones that the Nessus scanner will be assigned to are selectable.

An example screen capture of SecurityCenter's "Add Scanner" page is shown below:



Name: Local Scanner
Description: Local SecurityCenter Scanner
IP Address: 127.0.0.1
Port: 1241
Username: paul
Authentication Type: Password Based
Password: *******
Zones: 4Zone, 5Zone, .4and.5, .12Net, a

After successfully adding the scanner, the following page is displayed after the scanner is selected:



Nessus Scanner "Local Scanner" was successfully added. Close

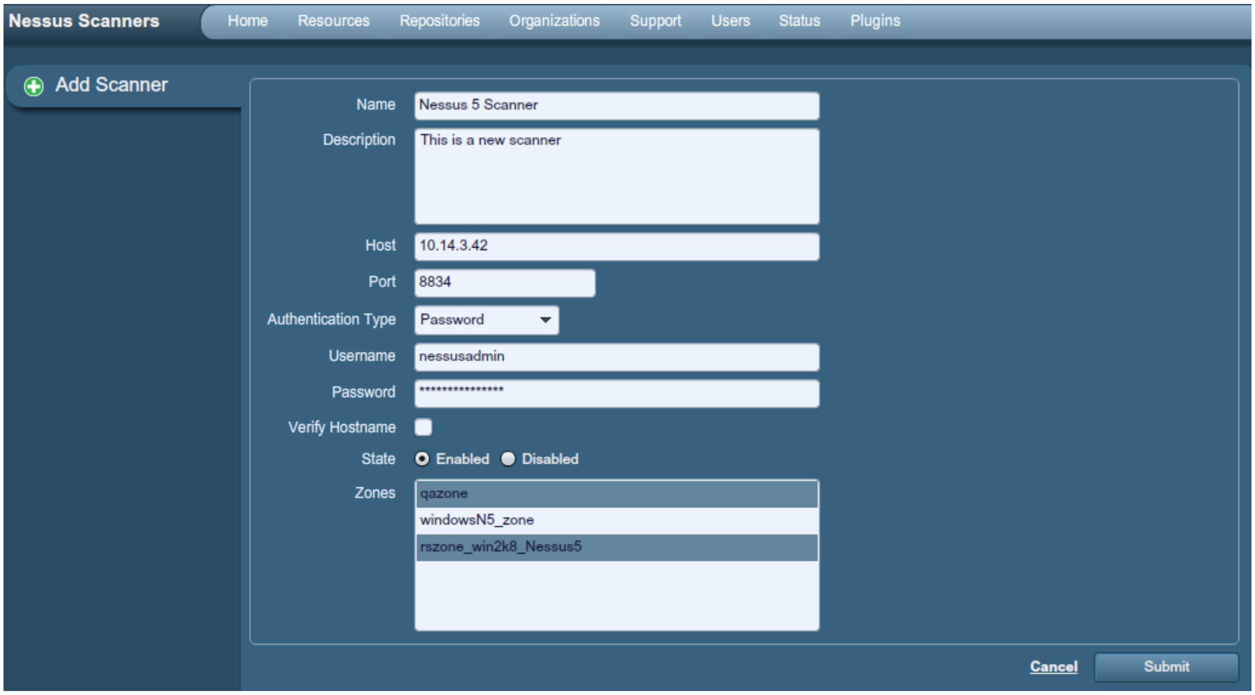
Name	IP	# of Zones	Status	Last Modified
Local Scanner	127.0.0.1	0	Working	Less than a minute ago

For more information please refer to the "SecurityCenter Administration Guide".

Configuring SecurityCenter 4.4 to Work with Nessus

The SecurityCenter administration interface is used to configure access and control of any Nessus scanner that is version 4.2.x or higher. Click the "**Resources**" tab and then click "**Nessus Scanners**". Click "**Add**" to open the "**Add Scanner**" dialog. The Nessus scanner's IP address or hostname, Nessus port (default: 8834), authentication type (created while configuring Nessus), and administrative login ID and password or certificate information are required. The password fields are not available if "SSL Certificate" authentication is selected. The ability to Verify Hostname is provided to check the CommonName (CN) of the SSL certificate presented by the Nessus server. The state of the Nessus scanner may be set to Enabled or Disabled as needed, with a default of Enabled. Zones the Nessus scanner may be assigned to can be selected.

An example screen capture of the SecurityCenter 4.4 "**Add Scanner**" page is shown below:



Name: Nessus 5 Scanner

Description: This is a new scanner

Host: 10.14.3.42

Port: 8834

Authentication Type: Password

Username: nessusadmin

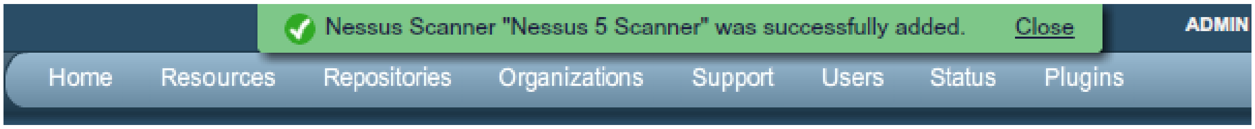
Password: ***************

Verify Hostname: □

State: ● Enabled ○ Disabled

Zones: qazone, windowsN5_zone, rszone_win2k8_Nessus5

After successfully adding the scanner, the following banner is displayed:



✓ Nessus Scanner "Nessus 5 Scanner" was successfully added.

For more information on integrating Nessus and SecurityCenter, please refer to the "SecurityCenter Administration Guide".

Host-Based Firewalls

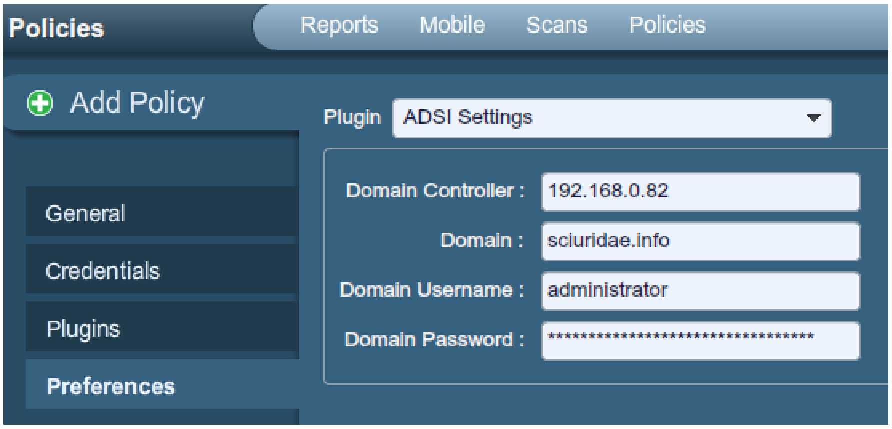
If your Nessus server is configured with a local firewall such as ZoneAlarm, Sygate, BlackICE, the Windows XP firewall, or any other firewall software, it is required that connections be opened from SecurityCenter's IP address.

By default, port 8834 is used. On Microsoft XP Service Pack 2 systems and later, clicking on the "**Security Center**" icon available in the "**Control Panel**" presents the user with the opportunity to manage the "Windows Firewall" settings. To open up port 8834 choose the "**Exceptions**" tab and then add port "8834" to the list.

⚠ If SecurityCenter is using the deprecated NTP protocol over port 1241, the above commands would use 1241 in place of 8834.

SCANNING PREFERENCES IN DETAIL

The "**Preferences**" tab includes almost 40 drop-down menus that provide fine granular control over scan settings. Spending time to explore and configure each menu can provide great flexibility and considerably more accurate scan results over using a default policy. The following section provides extensive detail on each "**Preferences**" option. Note that this is a dynamic list of configuration options that is dependent on the plugin feed, audit policies, and additional functionality that the connected Nessus scanner has access to. A scanner with a ProfessionalFeed may have more advanced configuration options available than a scanner configured with the HomeFeed. This list may also change as plugins are added or modified.

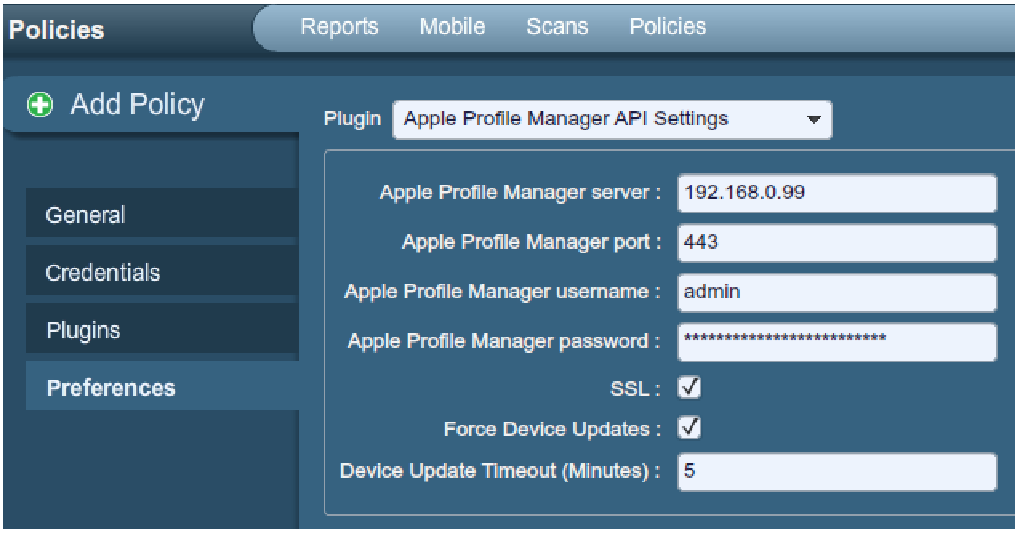


Plugin: ADSI Settings

Domain Controller : 192.168.0.82
Domain : sciuridae.info
Domain Username : administrator
Domain Password : *********************************

"**ADSI Settings**" allow Nessus to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Nessus authenticates to the domain controller (not Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan policy. These settings are required for mobile device scanning.

Note: For "ADSI Settings" and "Apple Profile Manager API Settings", host devices do not need to be scanned directly to obtain information about them. The Nessus scanner must be able to reach the mobile device management (MDM) server to query it for information. When either of these options are configured, the scan policy does not require a target host to scan; you can target "localhost" and the policy will still reach out to the MDM server for information.

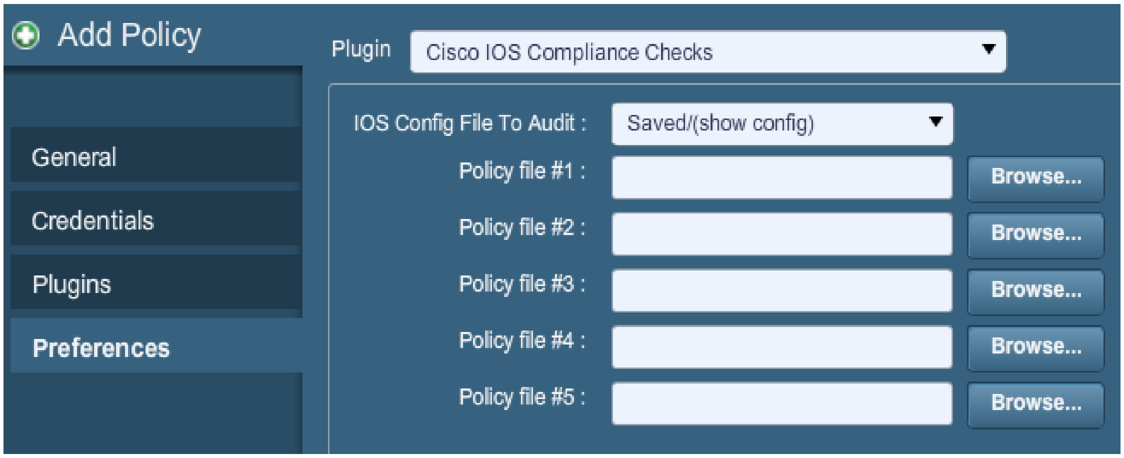


Plugin: Apple Profile Manager API Settings

Apple Profile Manager server : 192.168.0.99
Apple Profile Manager port : 443
Apple Profile Manager username : admin
Apple Profile Manager password : *************************
SSL : ☑
Force Device Updates : ☑
Device Update Timeout (Minutes) : 5

"**Apple Profile Manager API Settings**" allow Nessus to query an Apple Profile Manager server to enumerate Apple iOS-based devices (e.g., iPhone, iPad) on the network. Using the credentials and server information, Nessus authenticates to the Profile Manager to directly query it for device information. Optionally, communications over SSL can be specified as well as directing the server to force a device information update (i.e., each device will update its information with the Profile Manager server).

This feature does not require any ports be specified in the scan policy. These settings are required for mobile device scanning.



Plugin: Cisco IOS Compliance Checks

IOS Config File To Audit : Saved/(show config)

Policy file #1 :

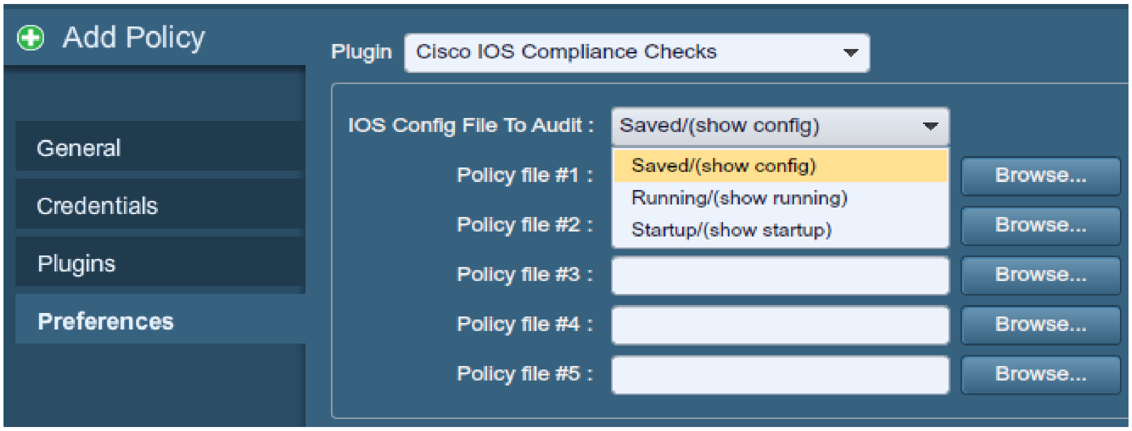
Policy file #2 :

Policy file #3 :

Policy file #4 :

Policy file #5 :

"**Cisco IOS Compliance Checks**" allow ProfessionalFeed customers to upload policy files that will be used to determine if a tested Cisco IOS based device meets the specified compliance standards. Up to five policies may be selected at one time. The policies may be run against Saved (**`show config`**), Running (**`show running`**), or Startup (**`show startup`**) configurations.



Plugin: Cisco IOS Compliance Checks

IOS Config File To Audit : Saved/(show config)

Policy file #1 :

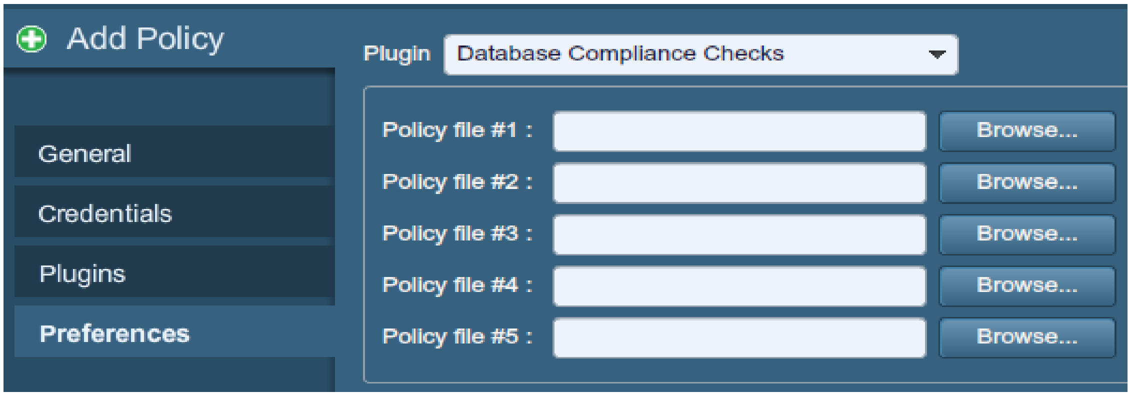
Policy file #2 :

Policy file #3 :

Policy file #4 :

Policy file #5 :

"**Database Compliance Checks**" allow ProfessionalFeed customers to upload policy files that will be used to determine if a tested database meets the specified compliance standards. Up to five policies may be selected at one time.



Add Policy

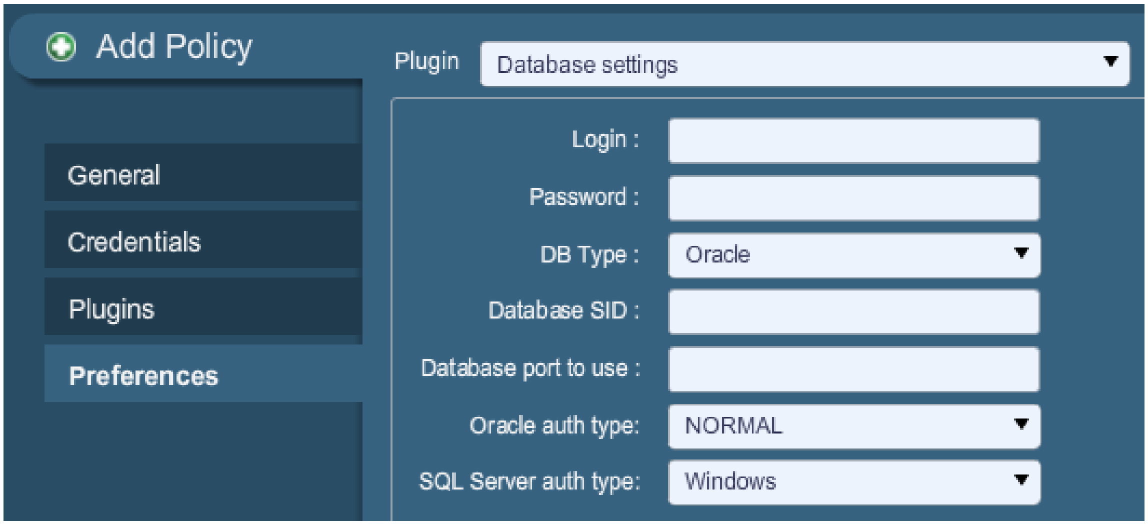
General
Credentials
Plugins
Preferences

Plugin: Database Compliance Checks

Policy file #1 : Browse...
Policy file #2 : Browse...
Policy file #3 : Browse...
Policy file #4 : Browse...
Policy file #5 : Browse...

The “**Database settings**” options are used to specify the type of database to be tested, relevant settings, and credentials:

Option	Description
Login	The username for the database.
Password	The password for the supplied username.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL are supported.
Database SID	ID of the database to audit.
Database port to use	Port the database listens on.
Oracle auth type	NORMAL, SYSOPER, and SYSDBA are supported.
SQL Server auth type	Windows or SQL are supported.



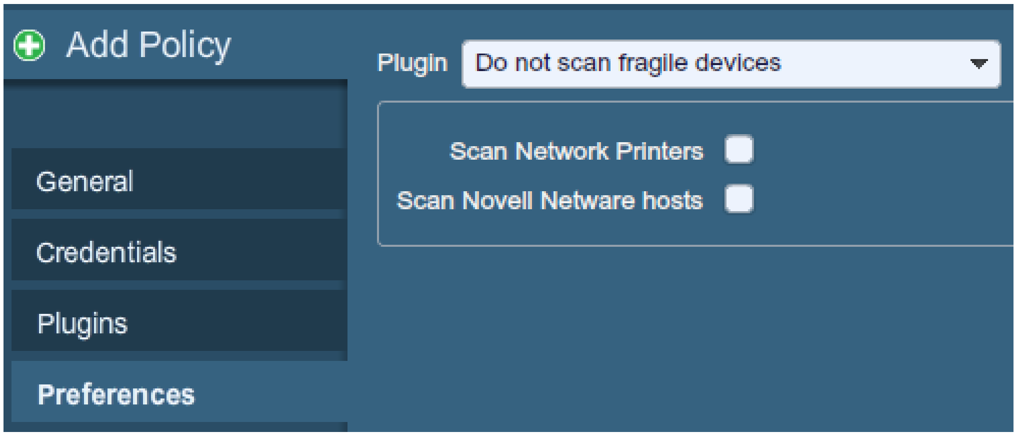
Add Policy

General
Credentials
Plugins
Preferences

Plugin: Database settings

Login :
Password :
DB Type : Oracle
Database SID :
Database port to use :
Oracle auth type: NORMAL
SQL Server auth type: Windows

“**Do not scan fragile devices**” offers two options that instruct the Nessus scanner not to scan hosts that have a history of being “fragile”, or prone to crashing when receiving unexpected input. Users can select either “Scan Network Printers” or “Scan Novell Netware hosts” to instruct Nessus to scan those particular devices. Only if these options are checked will Nessus scan them. It is recommended that scanning of these devices be performed in a manner that allows IT staff to monitor the systems for issues.

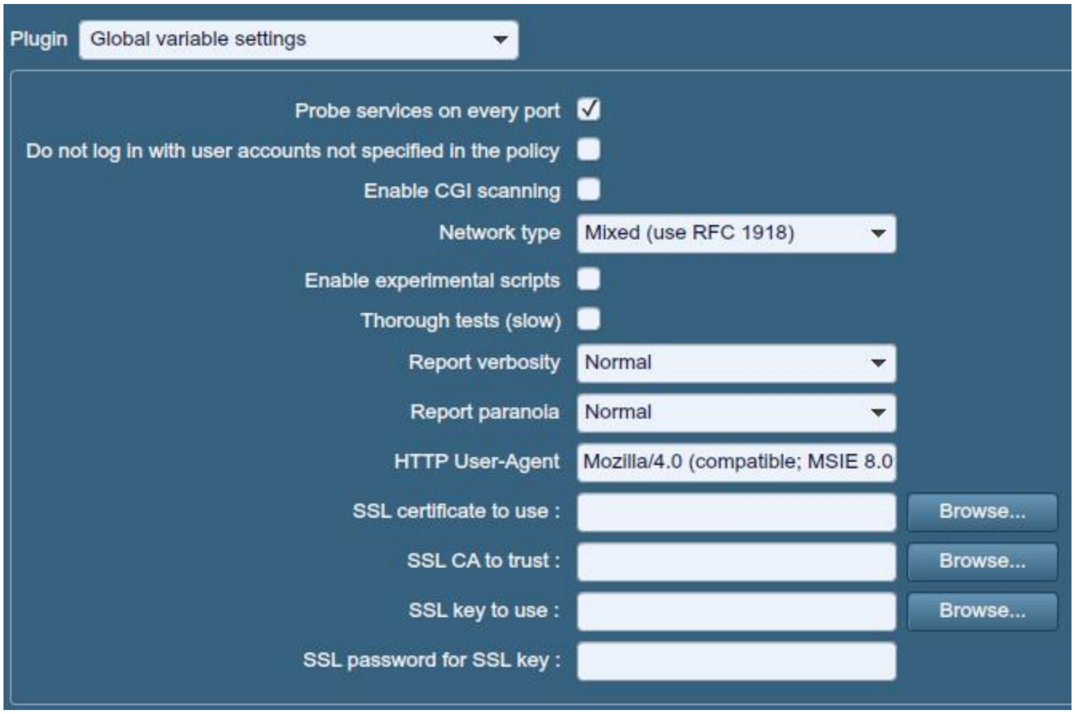


Plugin: Do not scan fragile devices

Scan Network Printers □

Scan Novell Netware hosts □

“**Global variable settings**” contains a wide variety of configuration options for the Nessus server.



Plugin: Global variable settings

Probe services on every port ☑

Do not log in with user accounts not specified in the policy □

Enable CGI scanning □

Network type: Mixed (use RFC 1918)

Enable experimental scripts □

Thorough tests (slow) □

Report verbosity: Normal

Report paranoia: Normal

HTTP User-Agent: Mozilla/4.0 (compatible; MSIE 8.0

SSL certificate to use :

SSL CA to trust :

SSL key to use :

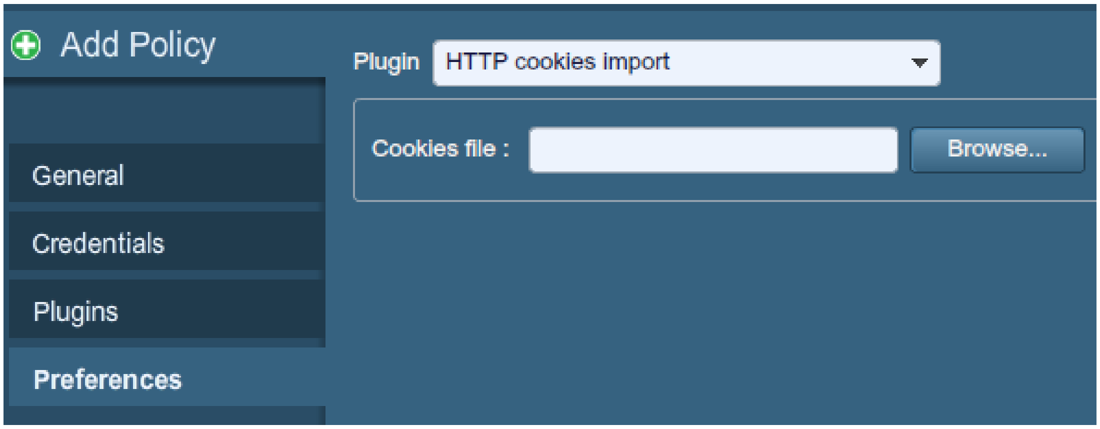
SSL password for SSL key :

The following table provides more detailed information about each option available:

Option	Description

Probe services on every port	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.
Do not log in with user accounts not specified in the policy	Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.
Enable CGI scanning	Activates CGI checking. Disabling this option will tremendously speed up the audit of a local network.
Network type	Allows you to specify if you are using public routable IPs, private non-internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.
Enable experimental scripts	Causes plugins that are considered experimental to be used in the scan. Do not enable this setting while scanning a production network.
Thorough tests (slow)	Causes various plugins to "work harder". For example, when looking through SMB file shares, a plugin can analyze 3 levels deep instead of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially having better audit results.
Report verbosity	A higher setting will provide more or less information about plugin activity in the report.
Report paranoia	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If the report paranoia is set to "**Paranoid**" then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of "**Avoid false alarm**" will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. The default option ("**Normal**") will be a middle ground between these two settings.
HTTP User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.
SSL certificate to use	Allows Nessus to use a client side SSL certificate for communicating with a remote host.
SSL CA to trust	Specifies a Certificate Authority (CA) that Nessus will trust.
SSL key to use	Specifies a local SSL key to use for communicating with the remote host.
SSL password for SSL key	The password for managing the SSL key specified.

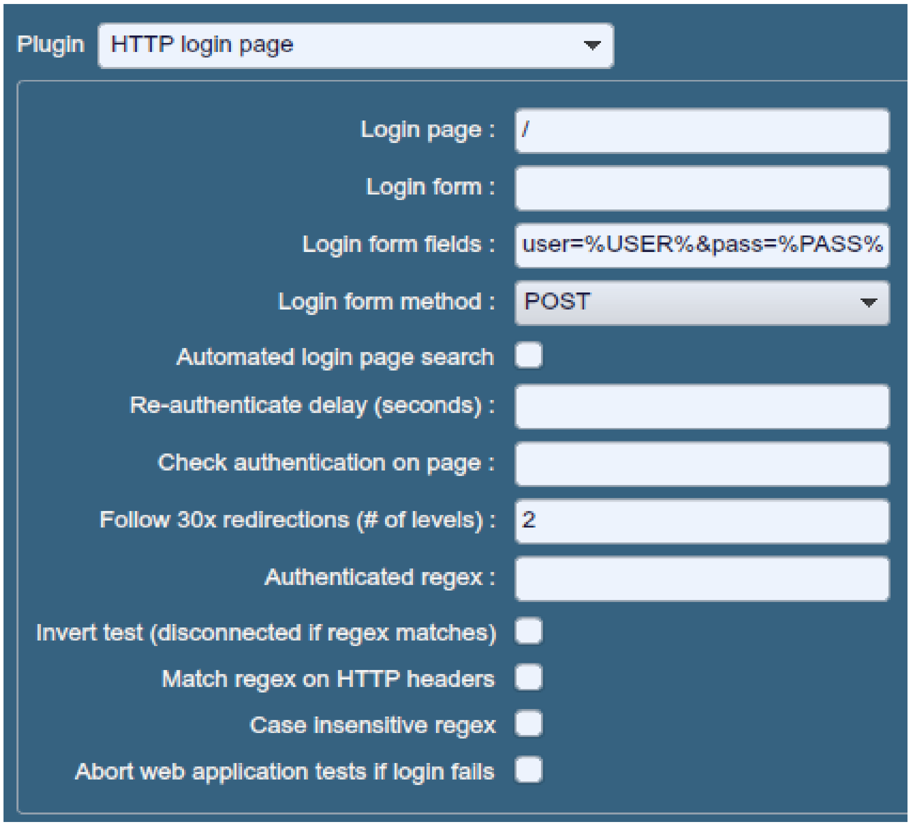
To facilitate web application testing, Nessus can import HTTP cookies from another piece of software (e.g., web browser, web proxy, etc.) with the "**HTTP cookies import**" settings. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.



The "**HTTP login page**" settings provide control over where authenticated testing of a custom web-based application begins.

Option	Description
Login page	The base URL to the login page of the application.
Login form	The "action" parameter for the form method. For example, the login form for `<form method="POST" name="auth_form" action="/login.php">` would be "`/login.php`".
Login form fields	Specify the authentication parameters (e.g., `login=%USER%&password=%PASS%`). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the "Login configurations" drop-down menu. This field can be used to provide more than two parameters if required (e.g., a "group" name or some other piece of information is required for the authentication process).
Login form method	Specify if the login action is performed via a GET or POST request.
Automated login page search	Direct Nessus to search for a login page.
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Check authentication on page	The URL of a protected web page that requires authentication, to better assist Nessus in determining authentication status.

Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Authenticated regex	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as "Authentication successful!"
Invert test (disconnected if regex matches)	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., "Authentication failed!")
Match regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.
Case insensitive regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.
Abort web application tests if login fails	If the credentials supplied do not work, Nessus will abort the custom web application tests (but not the CGI plugin families).



Plugin: HTTP login page

Login page : /

Login form :

Login form fields : user=%USER%&pass=%PASS%

Login form method : POST

Automated login page search □

Re-authenticate delay (seconds) :

Check authentication on page :

Follow 30x redirections (# of levels) : 2

Authenticated regex :

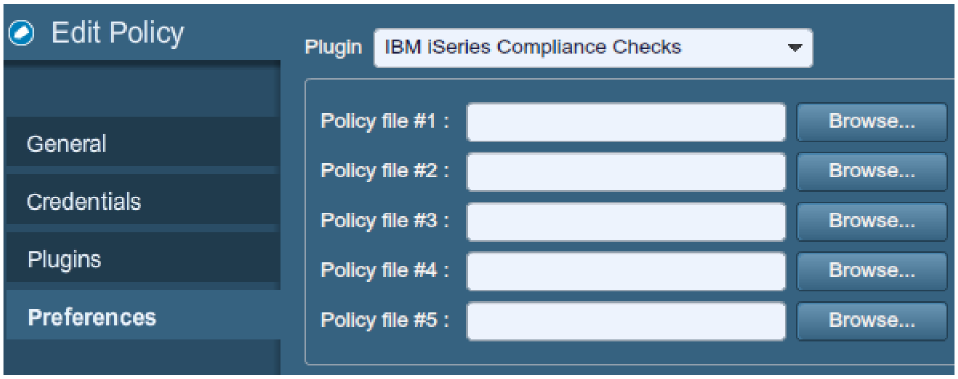
Invert test (disconnected if regex matches) □

Match regex on HTTP headers □

Case insensitive regex □

Abort web application tests if login fails □

"**IBM iSeries Compliance Checks**" allow ProfessionalFeed customers to upload policy files that will be used to determine if a tested IBM iSeries system meets the specified compliance standards. Up to five policies may be selected at one time.



Plugin: IBM iSeries Compliance Checks

Policy file #1 :

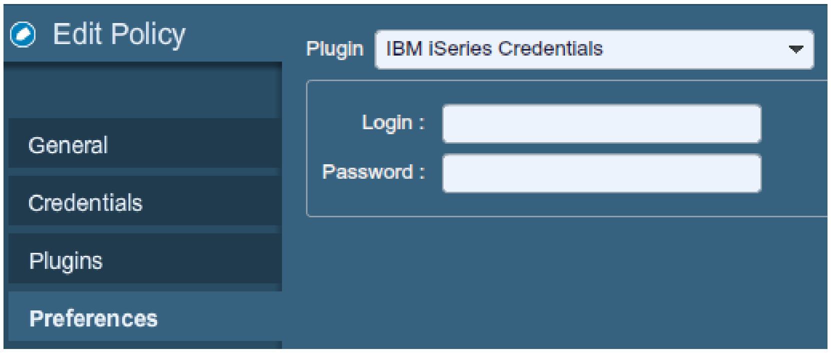
Policy file #2 :

Policy file #3 :

Policy file #4 :

Policy file #5 :

The "**IBM iSeries Credentials**" preferences provides a place to give Nessus credentials to authenticate to an IBM iSeries system. This is required for compliance auditing for example.

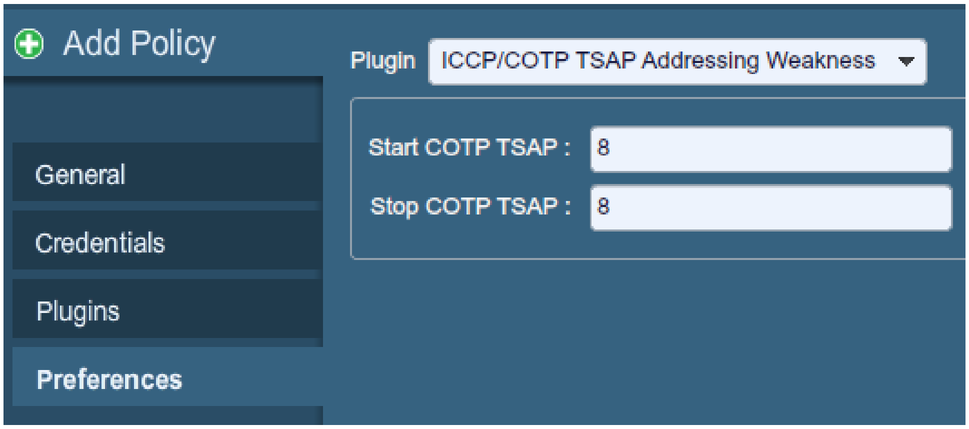


Plugin: IBM iSeries Credentials

Login :

Password :

The "**ICCP/COTP TSAP Addressing"** menu deals specifically with SCADA checks. It determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to "8" by default.

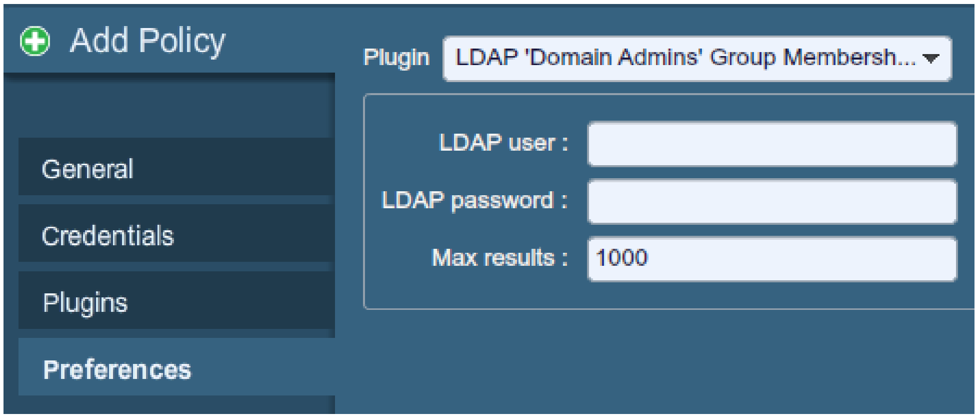


Plugin: ICCP/COTP TSAP Addressing Weakness

Start COTP TSAP : 8

Stop COTP TSAP : 8

The "LDAP 'Domain Admins' Group Membership Enumeration" menu allows you to enter a set of LDAP credentials that can be used to enumerate a list of members of the "Domain Admins" group in the remote LDAP directory.



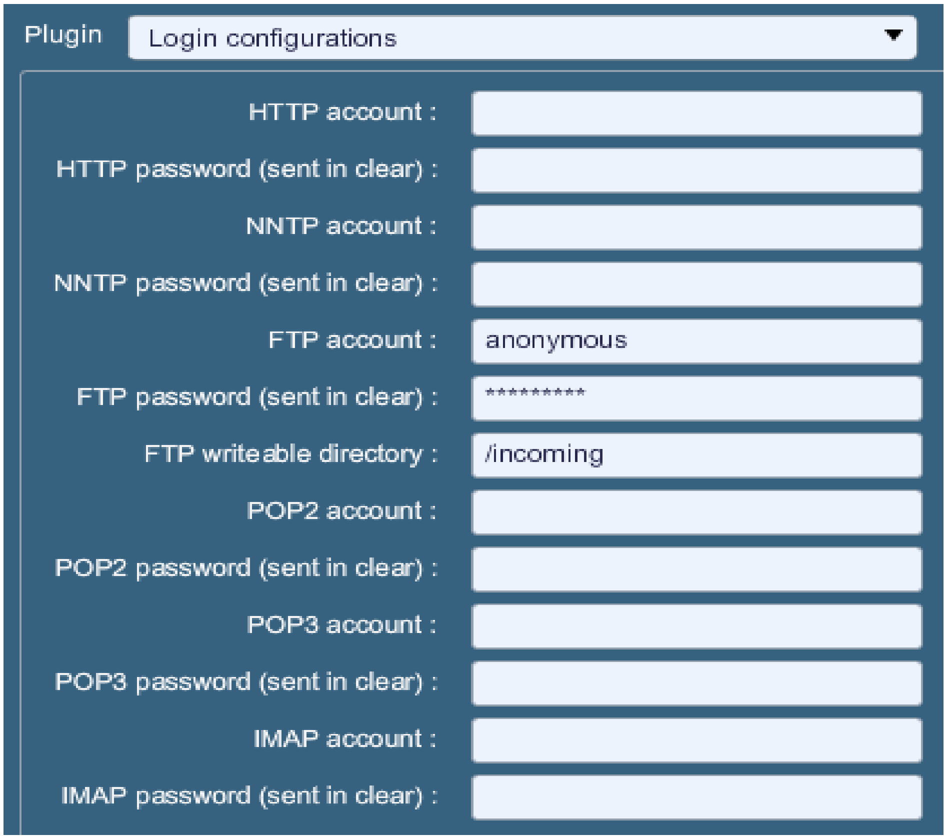
Plugin: LDAP 'Domain Admins' Group Membersh...

LDAP user :

LDAP password :

Max results : 1000

"**Login configurations**" allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3, or IMAP. By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied here will be used for Basic and Digest authentication only. For configuring credentials for a custom web application, use the "HTTP login page" pull-down menu.



Plugin: Login configurations

HTTP account :

HTTP password (sent in clear) :

NNTP account :

NNTP password (sent in clear) :

FTP account : anonymous

FTP password (sent in clear) : *********

FTP writeable directory : /incoming

POP2 account :

POP2 password (sent in clear) :

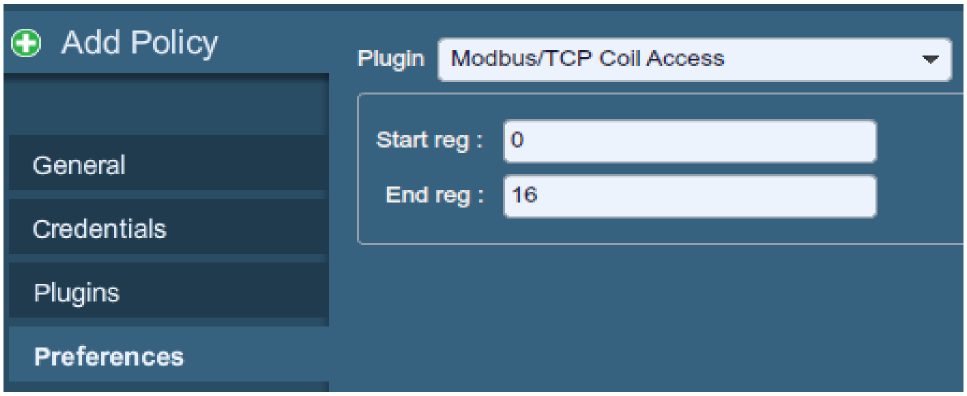
POP3 account :

POP3 password (sent in clear) :

IMAP account :

IMAP password (sent in clear) :

The "**Modbus/TCP Coil Access**" options are available for ProfessionalFeed users. This drop-down menu item is dynamically generated by the SCADA plugins available with the ProfessionalFeed. Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message. The defaults for this are "0" for the Start reg and "16" for the End reg.



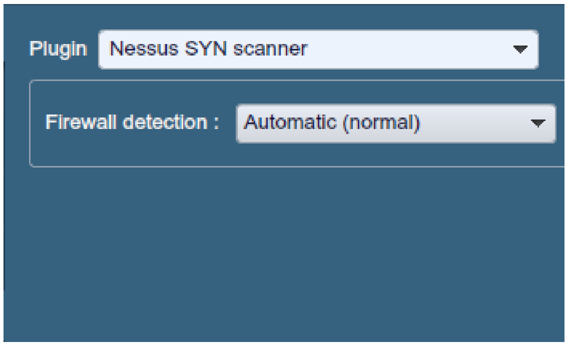
Plugin: Modbus/TCP Coil Access

Start reg : 0

End reg : 16

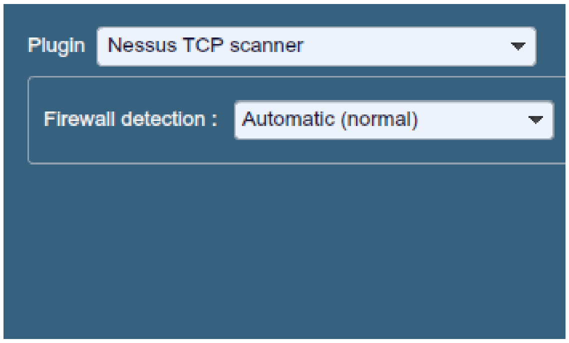
"**Nessus SYN scanner**" and "**Nessus TCP scanner**" options allow you to better tune the native SYN and TCP scanners to detect the presence of a firewall.

Value	Description
Automatic (normal)	This option can help identify if a firewall is located between the scanner and the target (**default**).
Disabled (softer)	Disables the **Firewall detection** feature.
Do not detect RST rate limitation (soft)	Disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.
Ignore closed ports (aggressive)	Will attempt to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.



Plugin: Nessus SYN scanner

Firewall detection : Automatic (normal)



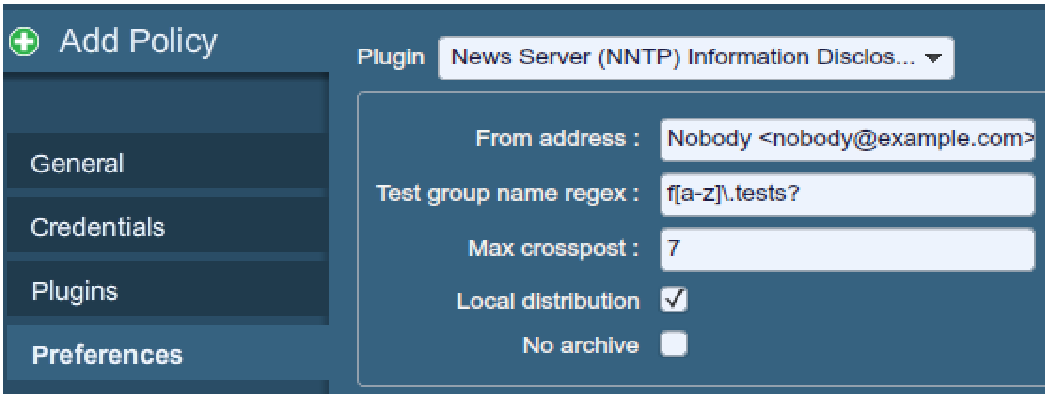
Plugin: Nessus TCP scanner

Firewall detection : Automatic (normal)

"**News Server (NNTP) Information Disclosure**" can be used to determine if there are news servers that are able to relay spam. Nessus will attempt to post a news message to a NNTP (Network News Transport Protocol) server(s), and can test if it is possible to post a message to upstream news servers as well.

Option	Description

From address	The address that Nessus will use as it attempts to post a message to the news server(s). This message will delete itself automatically after a short period of time.
Test group name regex	The name of the news group(s) that will receive a test message from the specified address. The name can be specified as a regular expression (regex) so that the message can be posted to multiple news groups simultaneously. For example, the default value "**f[a-z]\.tests?**" will broadcast a mail message to all news groups with names that begin with any letter (from "a" to "z") and end with ".tests" (or some variation that matched the string). The question mark acts as an optional wildcard.
Max crosspost	The maximum number of news servers that will receive the test posting, regardless of the number of name matches. For example, if the Max crosspost is "**7**", the test message will only be sent to seven news servers, even if there are 2000 news servers that match the regex in this field.
Local distribution	If this option is selected, Nessus will only attempt to post a message to the local news server(s). Otherwise, an attempt will be made to forward the message upstream.
No archive	If this option is selected, Nessus will request to not archive the test message being sent to the news server(s). Otherwise, the message will be archived like any other posting.



Plugin: News Server (NNTP) Information Disclos...

From address : Nobody <nobody@example.com>

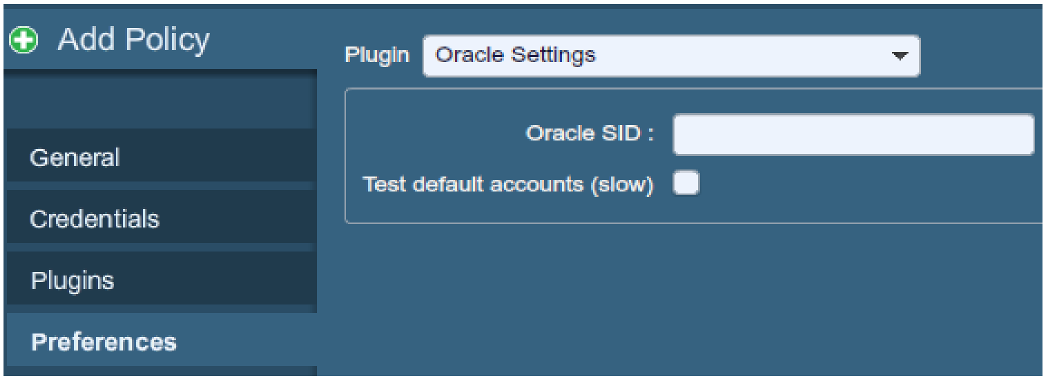
Test group name regex : f[a-z]\.tests?

Max crosspost : 7

Local distribution ☑

No archive □

"**Oracle Settings**" configures Nessus with the Oracle Database SID and includes an option to test for known default accounts in Oracle software.

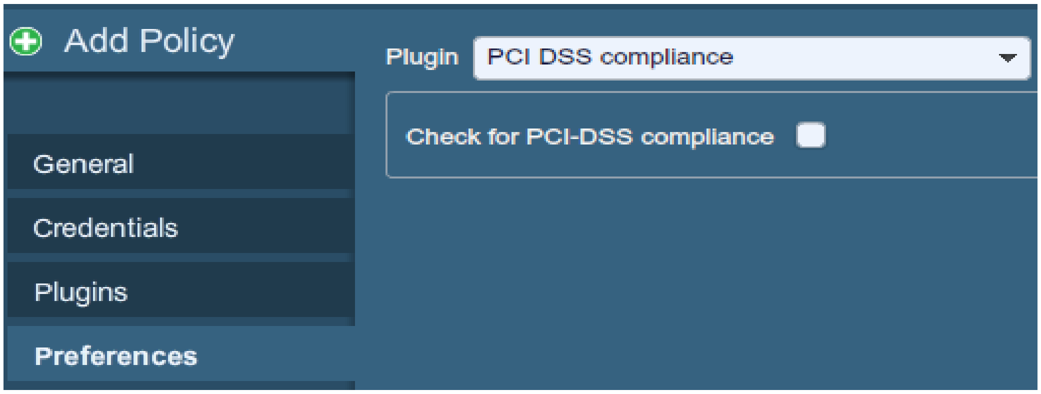


Plugin: Oracle Settings

Oracle SID :

Test default accounts (slow) □

"**PCI DSS Compliance**" will have Nessus compare the scan results to current PCI DSS compliance standards. This feature is only available to ProfessionalFeed customers.



Plugin: PCI DSS compliance

Check for PCI-DSS compliance □

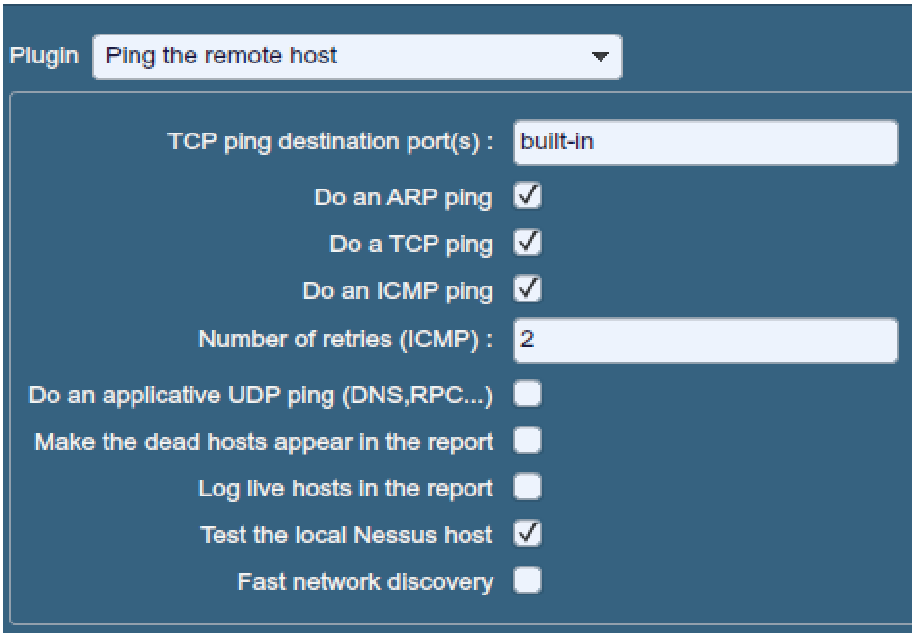
Nessus can leverage credentials for the Red Hat Satellite Server, WSUS, SCCM, and VMware Go (formerly Shavlik) patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner. Options for these patch management systems can be found under "Preferences" in their respective drop-down menus: "**Patch Management: Red Hat Satellite Server Settings**", "**Patch Management: SCCM Server Settings**", "**Patch Management: VMware Go Server Settings**", and "**Patch Management: WSUS Server Settings**". More information on using Nessus to scan hosts via these patch management systems is available in the "Patch Management Integration" document.

"**Ping the remote host**" options allow for granular control over Nessus' ability to ping hosts during discovery scanning. This can be done via ARP ping, TCP ping, ICMP ping, or applicative UDP ping.

Option	Description
TCP ping destination port(s)	Specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting to the default of "built-in".
Number of Retries (ICMP)"	Allows you to specify the number of attempts to try to ping the remote host. The default is set to 6.

Do an applicative UDP ping (DNS, RPC…)	Perform a UDP ping against specific UDP-based applications including DNS (port 53), RPC (port 111), NTP (port 123), and RIP (port 520).
Make the dead hosts appear in the report	If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts.
Log live hosts in the report	Select this option to specifically report on the ability to successfully ping a remote host.
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.
Fast network discovery	By default, when Nessus "pings" a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1-65535 but there is no service behind). Such checks can take some time, especially if the remote host is firewalled. If the "fast network discovery" option is enabled, Nessus will not perform these checks.

To scan VMware guest systems, "ping" must disabled. In the scan policy under "Advanced" -> "Ping the remote host", uncheck TCP, ICMP, and ARP ping.



Plugin: Ping the remote host

TCP ping destination port(s) : built-in

Do an ARP ping ☑

Do a TCP ping ☑

Do an ICMP ping ☑

Number of retries (ICMP) : 2

Do an applicative UDP ping (DNS,RPC…) □

Make the dead hosts appear in the report □

Log live hosts in the report □

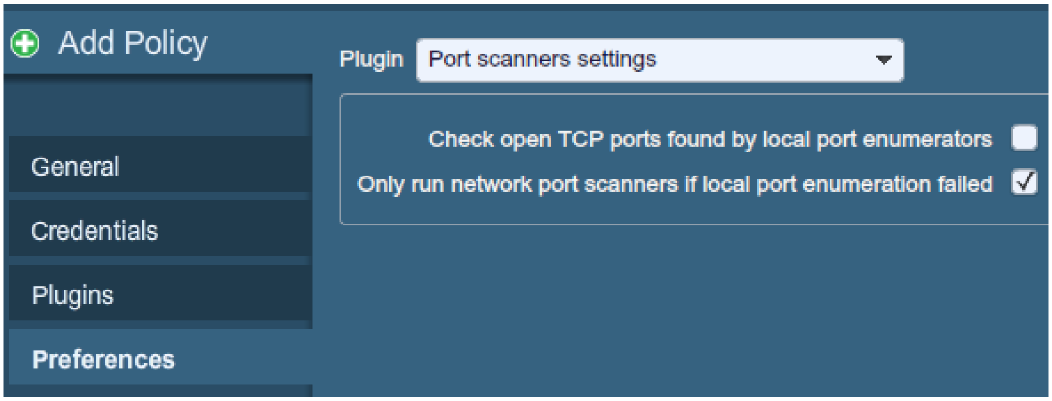
Test the local Nessus host ☑

Fast network discovery □

"**Port scanner settings**" provide two options for further controlling port scanning activity:

Option	Description

Check open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Otherwise, rely on local port enumeration first.



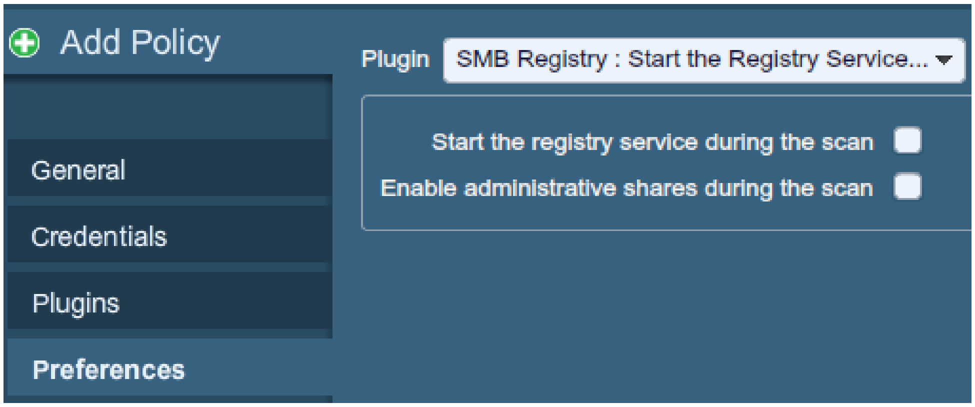
Plugin: Port scanners settings

Check open TCP ports found by local port enumerators □

Only run network port scanners if local port enumeration failed ☑

“**SMB Registry: Start the Registry Service during the scan**” enables the service to facilitate some of the scanning requirements for machines that may not have the SMB Registry running all the time.

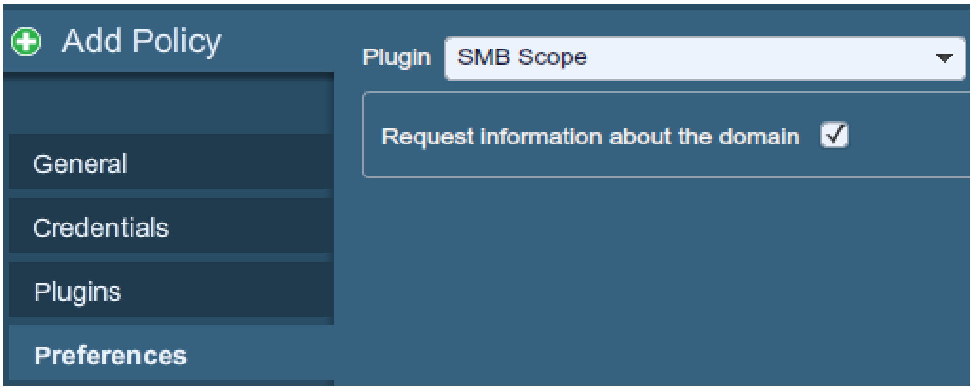
Under the “**SMB Scope**” menu, if the option “**Request information about the domain**” is set, then domain users will be queried instead of local users.



Plugin: SMB Registry : Start the Registry Service...

Start the registry service during the scan □

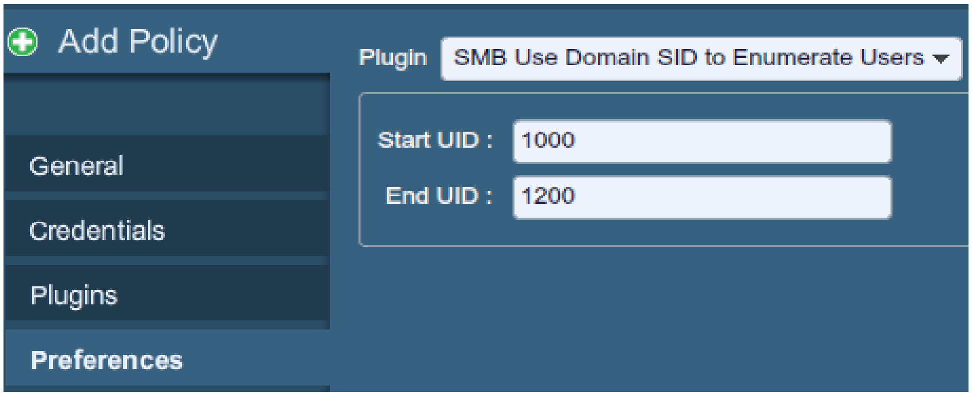
Enable administrative shares during the scan □



Plugin: SMB Scope

Request information about the domain ☑

"**SMB Use Domain SID to Enumerate Users**" specifies the SID range to use to perform a reverse lookup on usernames on the domain. The default setting is recommended for most scans.

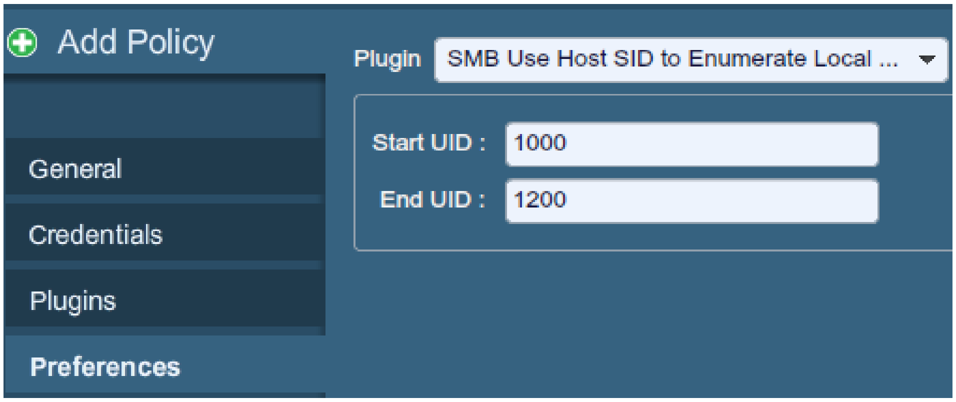


Plugin: SMB Use Domain SID to Enumerate Users

Start UID : 1000

End UID : 1200

"**SMB Use Host SID to Enumerate Local Users**" specifies the SID range to use to perform a reverse lookup on local usernames. The default setting is recommended.



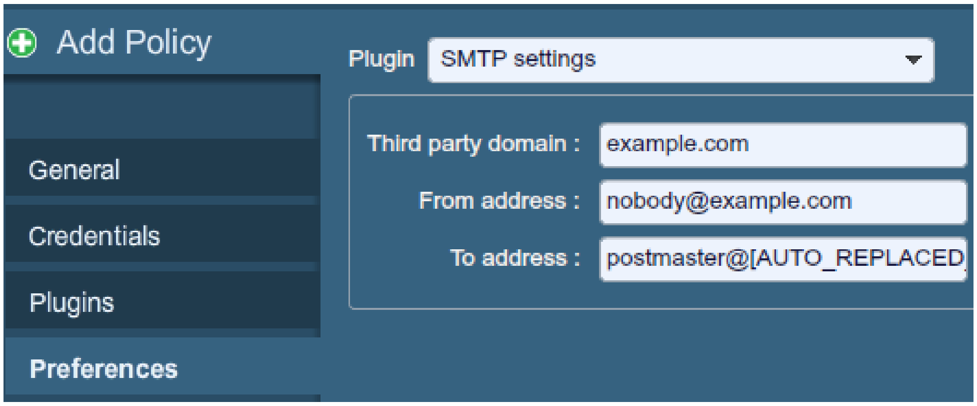
Plugin: SMB Use Host SID to Enumerate Local ...

Start UID : 1000

End UID : 1200

"**SMTP settings**" specify options for SMTP (Simple Mail Transport Protocol) tests that run on all devices within the scanned domain that are running SMTP services. Nessus will attempt to relay messages through the device to the specified "**Third party domain**". If the message sent to the "**Third party domain**" is rejected by the address specified in the "**To address**" field, the spam attempt failed. If the message is accepted, then the SMTP server was successfully used to relay spam.

Option	Description
Third party domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.
To address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The **postmaster** address is the default value since it is a valid address on most mail servers.



Plugin: SMTP settings

Third party domain : example.com

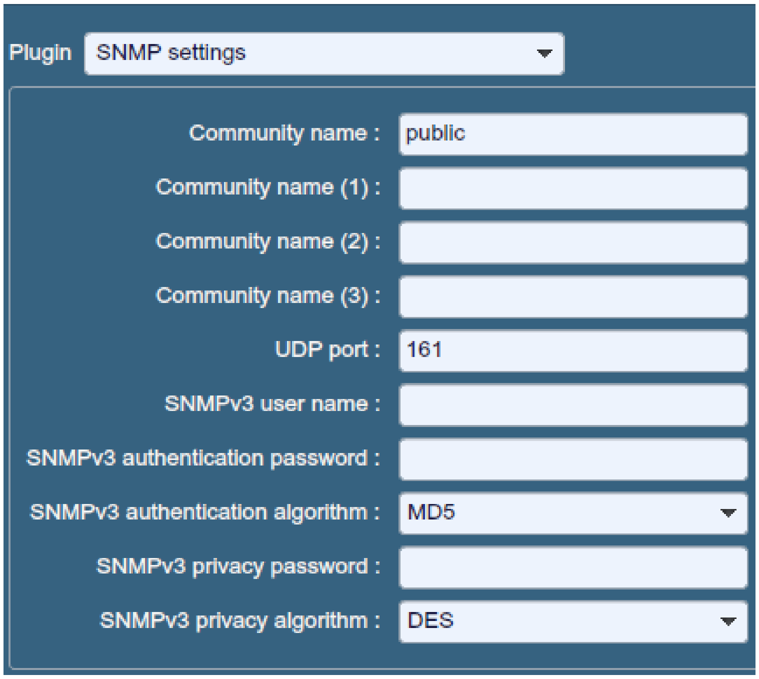
From address : nobody@example.com

To address : postmaster@[AUTO_REPLACED

"**SNMP settings**" allow you to configure Nessus to connect and authenticate to the SNMP service of the target. During the course of scanning, Nessus will make some attempts to guess the community string and use it for subsequent tests. Up to four separate community name strings are supported per scan policy. If Nessus is unable to guess the community string and/or password, it may not perform a full audit against the service.

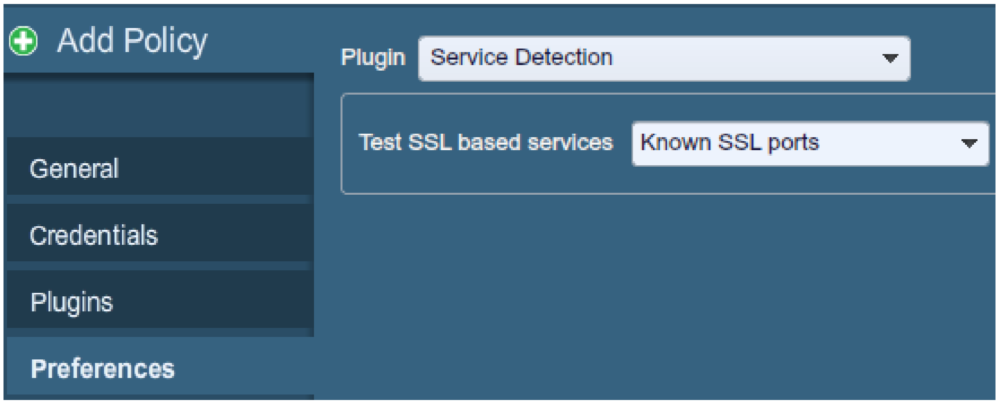
Option	Description
Community name (0-3)	The SNMP community name.
UDP port	Direct Nessus to scan a different port if SNMP is running on a port other than 161.
SNMPv3 user name	The username for a SNMPv3 based account.
SNMPv3 authentication password	The password for the username specified.
SNMPv3 authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
SNMPv3 privacy password	A password used to protect encrypted SNMP communication.

SNMPv3 privacy algorithm	The encryption algorithm to use for SNMP traffic.



Plugin	SNMP settings
Community name :	public
Community name (1) :	
Community name (2) :	
Community name (3) :	
UDP port :	161
SNMPv3 user name :	
SNMPv3 authentication password :	
SNMPv3 authentication algorithm :	MD5
SNMPv3 privacy password :	
SNMPv3 privacy algorithm :	DES

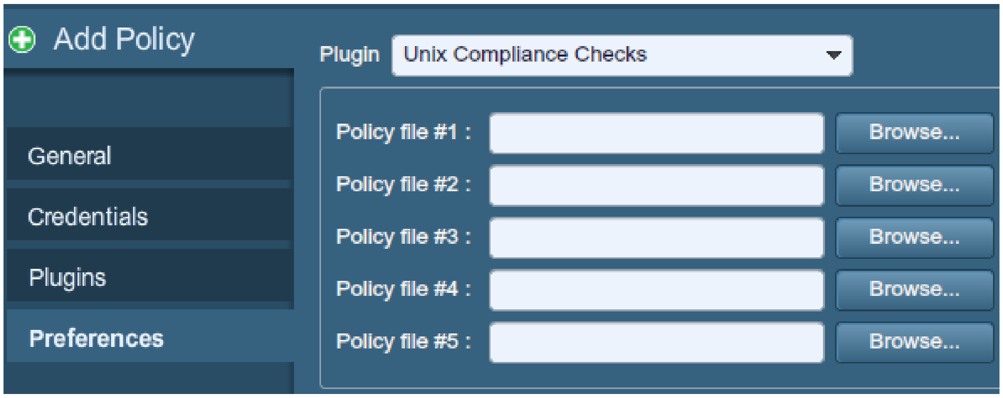
"**Service Detection**" controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.



Plugin: Service Detection

Test SSL based services: Known SSL ports

"**Unix Compliance Checks**" allow ProfessionalFeed customers to upload Unix audit files that will be used to determine if a tested system meets the specified compliance standards. Up to five policies may be selected at one time.



Add Policy

General

Credentials

Plugins

Preferences

Plugin: Unix Compliance Checks

Policy file #1 :

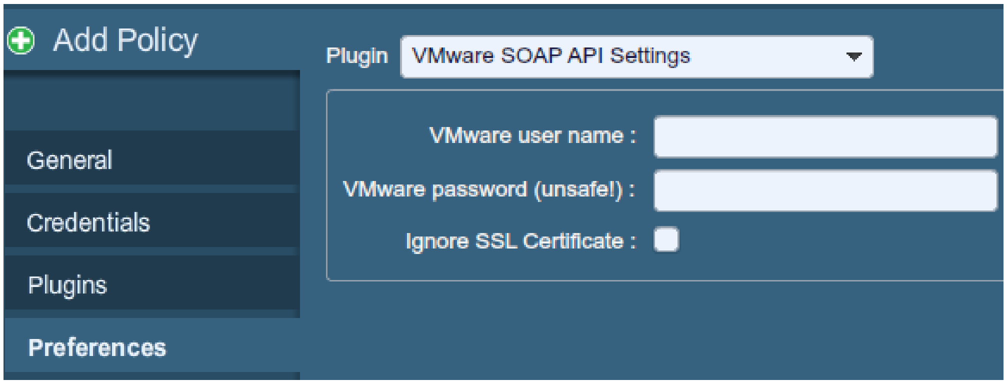
Policy file #2 :

Policy file #3 :

Policy file #4 :

Policy file #5 :

"**VMware SOAP API Settings**" provides Nessus with the credentials required to authenticate to VMware ESX, ESXi, and vSphere Hypervisor management systems via their own SOAP API, as SSH access has been deprecated. The API is intended for the auditing of vSphere 4.x / 5.x, ESXi, and ESX hosts, not the virtual machines running on the hosts. This authentication method can be used to perform credentialed scans or perform compliance audits.



Add Policy

General

Credentials

Plugins

Preferences

Plugin: VMware SOAP API Settings

VMware user name :

VMware password (unsafe!) :

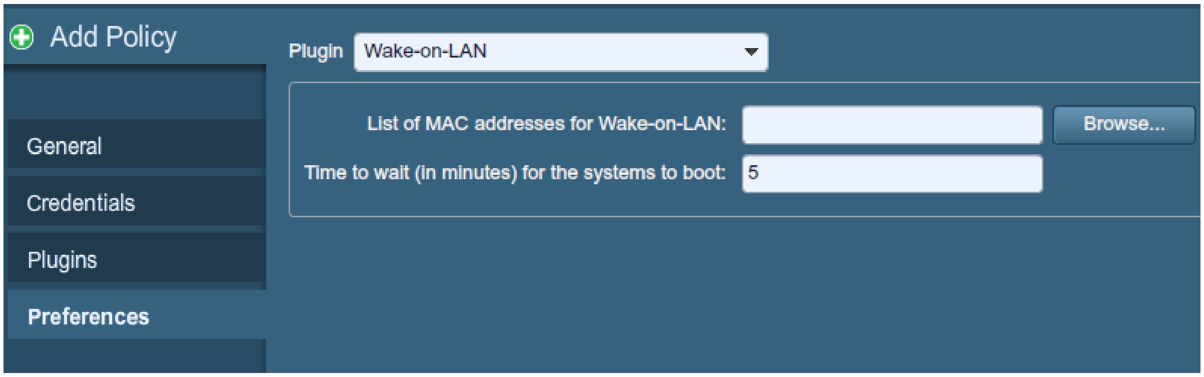
Ignore SSL Certificate : □

Option	Description
VMware user name	The user name to authenticate with. The credentials can be Active Directory (AD) accounts for integrated hosts or local accounts, and the account must be in the `root` local group. Domain credentials are user@domain, locally created accounts are user and password.
VMware password (unsafe!)	This password is sent insecurely and may be intercepted by sniffing the network.
Ignore SSL Certificate	If an SSL certificate is present on the server, ignore it.

"**Wake-on-LAN**" (WOL) controls which hosts to send WOL magic packets to before performing a scan and how long to wait (in minutes) for the systems to boot. The list of MAC addresses for WOL is entered using an uploaded text file with one host MAC address per line. For example:

```
00:11:22:33:44:55
```

```
aa:bb:cc:dd:ee:ff
[…]
```



Plugin: Wake-on-LAN

List of MAC addresses for Wake-on-LAN:

Time to wait (in minutes) for the systems to boot: 5

"**Web Application Tests Settings**" tests the arguments of the remote CGIs (Common Gateway Interface) discovered in the web mirroring process by attempting to pass common CGI programming errors such as cross-site scripting, remote file inclusion, command execution, traversal attacks, and SQL injection. Enable this option by selecting the "Enable web applications tests" checkbox. These tests are dependent on the following NASL plugins:

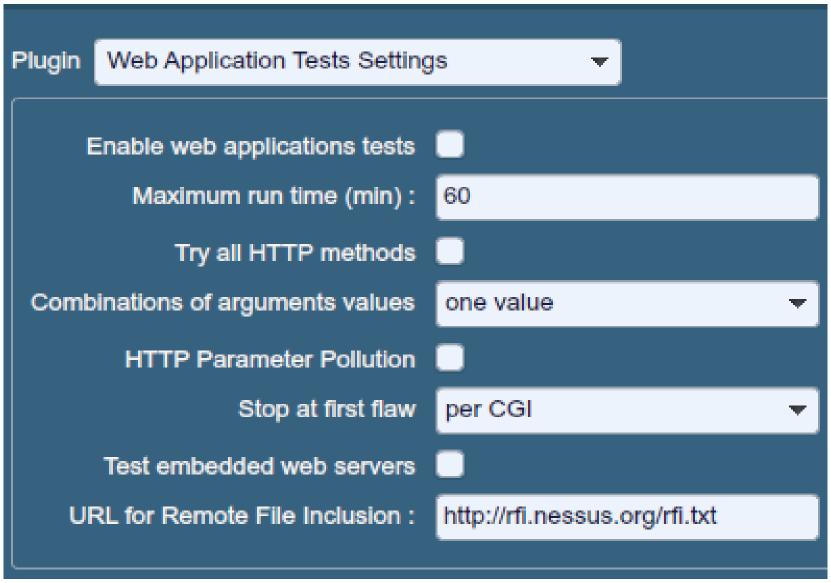
- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI abuses)
- 39465, 44967 – Command Execution (CGI abuses)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI abuses: XSS)
- 39467, 46195, 46194 – Directory Traversal (CGI abuses)
- 39468 – HTTP Header Injection (CGI abuses: XSS)
- 39469, 42056, 42872 –File Inclusion (CGI abuses)
- 42055 - Format String (CGI abuses)
- 42423, 42054 - Server Side Includes (CGI abuses)
- 44136 - Cookie Manipulation (CGI abuses)
- 46196 - XML Injection (CGI abuses)
- 40406, 48926, 48927 - Error Messages
- 47830, 47832, 47834, 44134 - Additional attacks (CGI abuses)

Note: This list of web application related plugins is updated frequently and may not be complete. Additional plugins may be dependent on the settings in this preference option.

Option	Description
Maximum run time (min)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.
Try all HTTP methods	By default, Nessus will only test using GET requests. This option will instruct Nessus to also use "POST requests" for enhanced web form testing. By default, the web application

	tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests.
Combinations of arguments values	This option manages the combination of argument values used in the HTTP requests. This dropdown has three options: **one value** – This tests one parameter at a time with an attack string, without trying “non-attack” variations for additional parameters. For example, Nessus would attempt “`/test.php?arg1=XSS&b=1&c=1`” where “b” and “c” allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. **All pairs (slower but efficient)** – This form of testing is slightly slower but more efficient than the “one value” test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt “`/test.php?a=XSS&b=1&c=1&d=1`” and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for “`/test.php?a=XSS&b=3&c=3&d=3`” when the first value of each variable is “1”. **All combinations (extremely slow)** – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where “All-pairs” testing seeks to create a smaller data set as a tradeoff for speed, “all combinations” makes no compromise on time and uses a complete data set of tests. This testing method may take a **long** time to complete.
HTTP Parameter Pollution	When performing web application tests, attempt to bypass any filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like “`/target.cgi?a='&b=2`”. With HTTP Parameter Pollution (HPP) enabled, the request may look like “`/target.cgi?a='&a=1&b=2`”.
Stop at first flaw	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless “thorough tests” is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if

	they were caught by the same attack. The dropdown has four options: **per CGI** – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. **per port (quicker)** – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. **per parameter (slow)** – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. **look for all flaws (slower)** – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
Test Embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.
URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted on Tenable’s web server for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.



Plugin: Web Application Tests Settings

Enable web applications tests □

Maximum run time (min) : 60

Try all HTTP methods □

Combinations of arguments values: one value

HTTP Parameter Pollution □

Stop at first flaw: per CGI

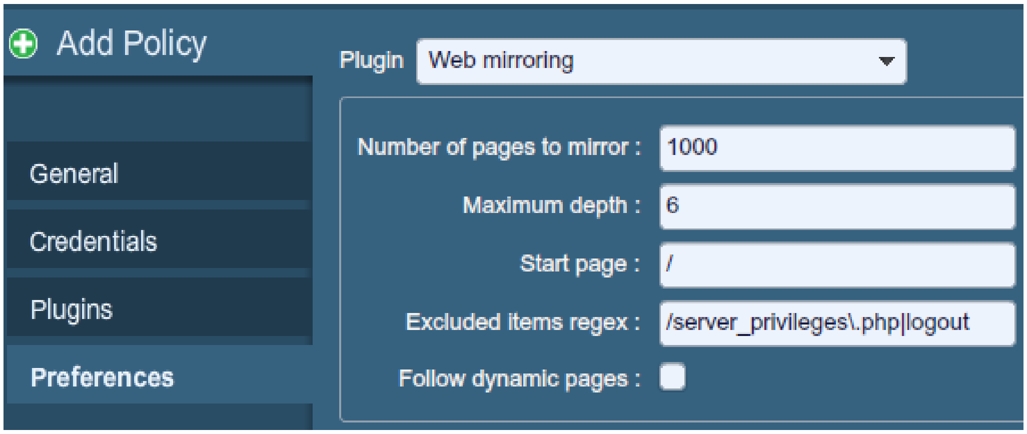
Test embedded web servers □

URL for Remote File Inclusion : http://rfi.nessus.org/rfi.txt

“**Web Mirroring**” sets configuration parameters for Nessus’ native web server content mirroring utility. Nessus will mirror web content to better analyze the contents for vulnerabilities and help minimize the impact on the server.

If the web mirroring parameters are set in such a way to mirror an entire web site, this may cause a significant amount of traffic to be generated during the scan. For example, if there is 1 gigabyte of material on a web server and Nessus is configured to mirror everything, then the scan will generate at least 1 gigabyte of traffic from the server to the Nessus scanner.

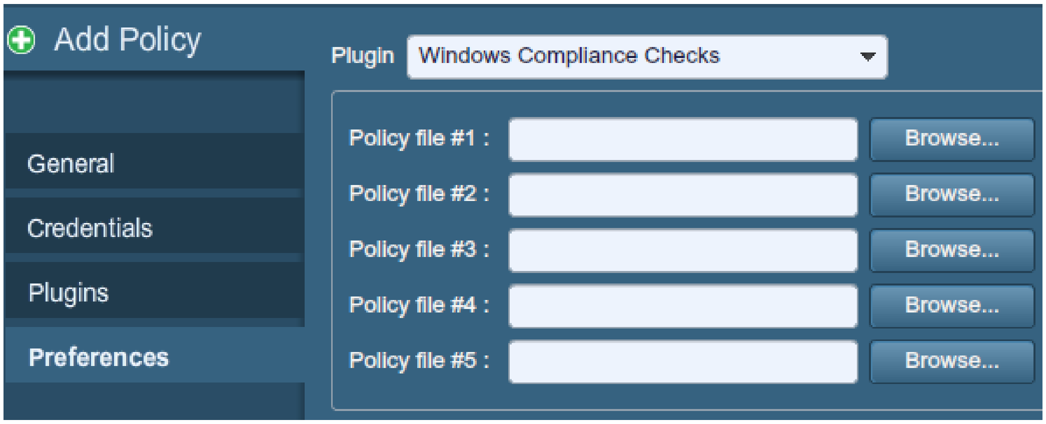
Option	Description
Number of pages to mirror	The maximum number of pages to mirror.
Maximum depth	Limit the number of links Nessus will follow for each start page.
Start page	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., “/:/php4:/base”).
Excluded items regex	Enable exclusion of portions of the web site from being crawled. For example, to exclude the “/manual” directory and all Perl CGI, set this field to: **(^/ manual) | (\ . pl (\ ?. *) ?$) .**
Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.



Plugin: Web mirroring

Number of pages to mirror : 1000
Maximum depth : 6
Start page : /
Excluded items regex : /server_privileges\.php|logout
Follow dynamic pages : □

“**Windows Compliance Checks**” allow ProfessionalFeed customers to upload Microsoft Windows configuration audit files that will be used to determine if a tested system meets the specified compliance standards. Up to five policies may be selected at one time.



Plugin: Windows Compliance Checks

Policy file #1 :

Policy file #2 :

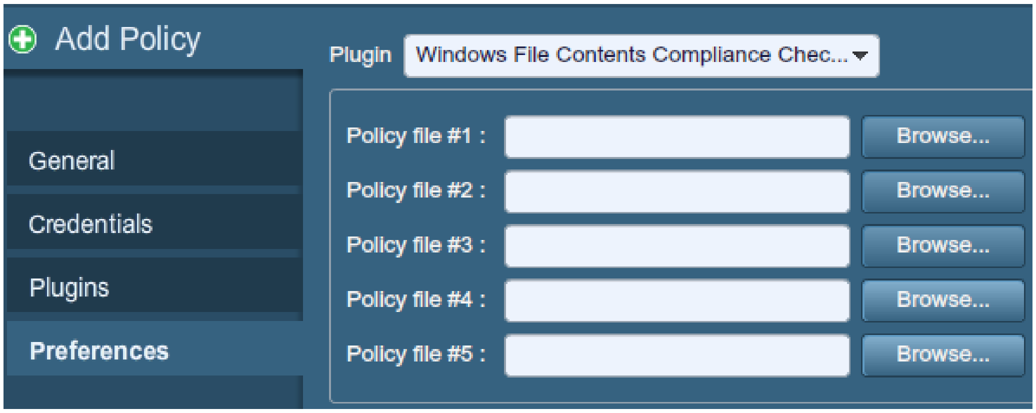
Policy file #3 :

Policy file #4 :

Policy file #5 :

“**Windows File Contents Compliance Checks**” allows ProfessionalFeed customers to upload Windows-based audit files that search a system for a specific type of content (e.g., credit cards, Social Security numbers) to help determine compliance with corporate regulations or third-party standards.

When all of the options have been configured as desired, click “**Submit**” to save the policy and return to the Policies tab. At any time, you can click on “**Edit**” to make changes to a policy you have already created or click on “**Delete**” to remove a policy completely.



Plugin: Windows File Contents Compliance Chec...

Policy file #1 :

Policy file #2 :

Policy file #3 :

Policy file #4 :

Policy file #5 :

FOR FURTHER INFORMATION

Tenable has produced a variety of other documents detailing Nessus’ installation, deployment, configuration, user operation and overall testing. These are listed here:

- **Nessus Installation Guide** – step by step walk through of installation
- **Nessus Credential Checks for Unix and Windows –** information on how to perform authenticated network scans with the Nessus vulnerability scanner
- **Nessus Compliance Checks** – high-level guide to understanding and running compliance checks using Nessus and SecurityCenter
- **Nessus Compliance Checks Reference** – comprehensive guide to Nessus Compliance Check syntax
- **Nessus v2 File Format** – describes the structure for the `.nessus` file format, which was introduced with Nessus 3.2 and NessusClient 3.2

- **Nessus XML-RPC Protocol Specification** – describes the XML-RPC protocol and interface in Nessus
- **Real-Time Compliance Monitoring** – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations
- **SecurityCenter Administration Guide**

Other online resources are listed below:

- Nessus Discussions Forum: https://discussions.nessus.org/
- Tenable Blog: http://blog.tenable.com/
- Tenable Podcast: http://blog.tenablesecurity.com/podcast/
- Example Use Videos: http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed: http://twitter.com/tenablesecurity

Please feel free to contact Tenable at support@tenable.com, sales@tenable.com, or visit our website at http://www.tenable.com/.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com