Руководство пользователя сервера Nessus 4.4

14 июня 2011 г.

(редакция 10)

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

Содержание

ВВЕДЕНИЕ

В этом документе описывается использование **интерфейса пользователя (ИП)** сервера **Nessus** компании Tenable Network Security. Мы будем рады получить ваши комментарии и предложения по адресу электронной почты support@tenable.com.

Интерфейс пользователя Nessus представляет собой веб-интерфейс сканера уязвимостей Nessus. Для использования клиента должен быть развернут действующий сканер безопасности Nessus, а также необходимо ознакомиться с порядком его использования.

СТАНДАРТЫ И УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Этот документ является переводом оригинальной версии на английском языке. Часть текста остается на английском языке, чтобы показать, как этот текст представлен в программном продукте.

В рамках всей документации имена файлов, демонов и исполняемых модулей выделены шрифтом **`courier bold`**, например **`gunzip`**, **`httpd`** и **`/etc/passwd`**.

Параметры и ключевые слова командной строки также выделены шрифтом **`courier bold`**. Параметры командной строки могут включать или не включать приглашение командной строки и выводимый в результате выполнения команды текст. Часто выполняемая команда приводится **жирным шрифтом**, чтобы выделить набираемый пользователем текст. Ниже приведен пример выполнения команды Unix **`pwd`**:

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

Этим символом и рамкой с серым фоном выделены важные примечания и соображения.

Этим символом и рамкой с синим фоном и белым текстом выделены советы, примеры и оптимальные методы.

ОБЗОР ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ NESSUS

ОПИСАНИЕ

Интерфейс пользователя (ИП) Nessus представляет собой веб-интерфейс сканера Nessus, который состоит из простого HTTP-сервера и веб-клиента, не требующего установки программного обеспечения, кроме установки сервера Nessus. Начиная с версии Nessus 4 все платформы являются производными из единой базы кода, что позволяет устранить большинство присущих определенным платформам программных ошибок и обеспечивает более быстрое развертывание новых функций. Основными функциями являются следующие.

- Генерирование файлов **`.nessus`**, которые продукты компании Tenable используют в качестве стандарта данных об уязвимостях и политики сканирования.

- Сеанс политики, список целей и результаты нескольких сканирований могут быть сохранены в едином файле `.nessus`, который легко экспортируется. Дополнительные сведения см. в руководстве по форматам файлов Nessus.
- Графический интерфейс пользователя отображает результаты сканирования в режиме реального времени, поэтому для просмотра результатов не требуется ждать завершения сканирования.
- Обеспечение унифицированного интерфейса сканера Nessus, независимо от базовой платформы. Одинаковые функции обеспечиваются на операционных системах Mac OS X, Windows и Linux.
- Выполнение сканирования будет продолжаться на сервере, даже если вы по какой-либо причине будете отключены.
- Отчеты о сканировании Nessus могут быть отправлены на сервер через интерфейс пользователя Nessus для сравнения с другими отчетами.

Поддерживаемые платформы

Поскольку интерфейс пользователя Nessus является веб-клиентом, он может выполняться на любой платформе с веб-браузером.

Веб-интерфейсом Nessus лучше всего пользоваться с помощью Microsoft Internet Explorer 7 и 8, Mozilla Firefox 3.5.x и 3.6.x или Apple Safari.

УСТАНОВКА

Начиная с версии Nessus 4.2 управление пользователями сервера Nessus выполняется через веб-интерфейс или консоль SecurityCenter, при этом использование отдельного клиента NessusClient больше не требуется. Отдельные клиенты NessusClients по-прежнему будут подключаться и управлять сканером, но не будут обновляться.

Инструкции по установке Nessus см. в руководстве по установке Nessus 4.4. Установка дополнительного программного обеспечения не требуется.

РАБОТА

Обзор

Nessus предоставляет простой, но мощный интерфейс для управления сканированием уязвимостей.

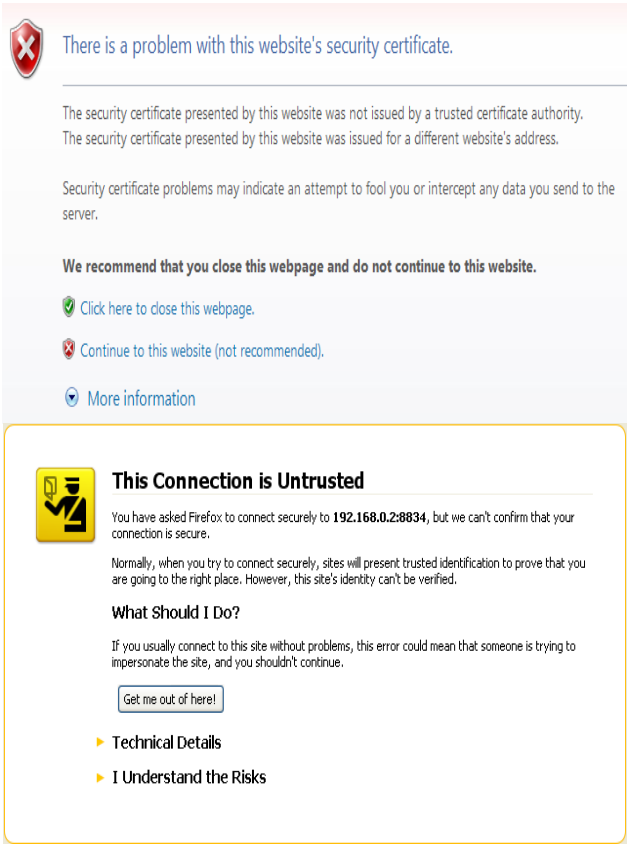
Подключение к графическому интерфейсу пользователя Nessus

Для запуска графического интерфейса пользователя Nessus выполните следующие действия.

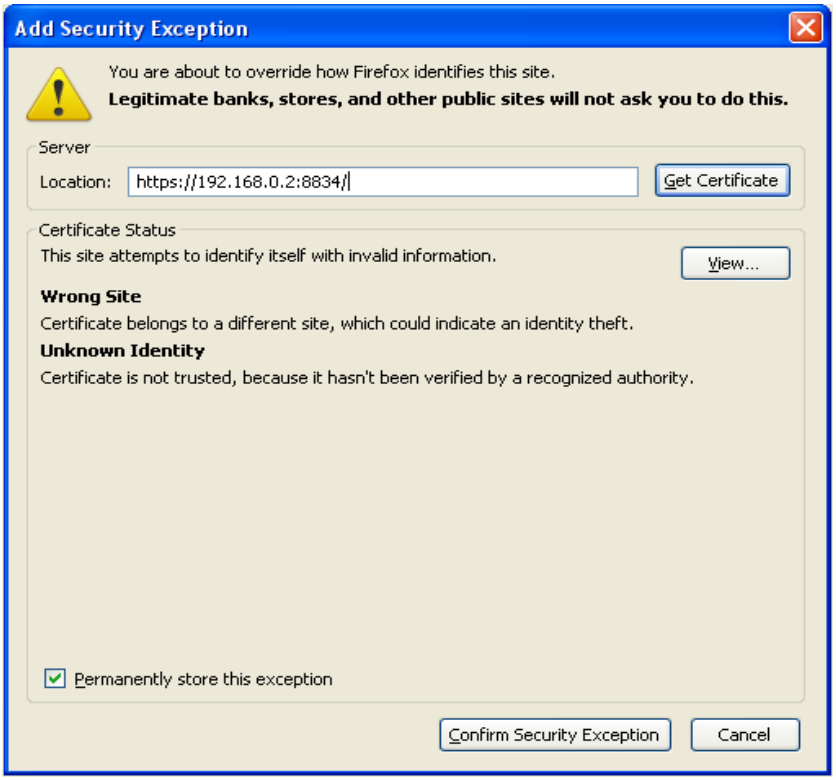
- Откройте предпочтительный веб-браузер.
- Введите на панели навигации адрес https://[server IP]:8834/.

Подключаться к интерфейсу пользователя необходимо по протоколу HTTPS, поскольку нешифрованные соединения HTTP не поддерживаются.

При первой попытке подключения к интерфейсу пользователя Nessus большинство веб-браузеров выдают сообщение об ошибке вследствие того, что сайт не является надежным, так как на нем используется сертификат SSL с самозаверением:

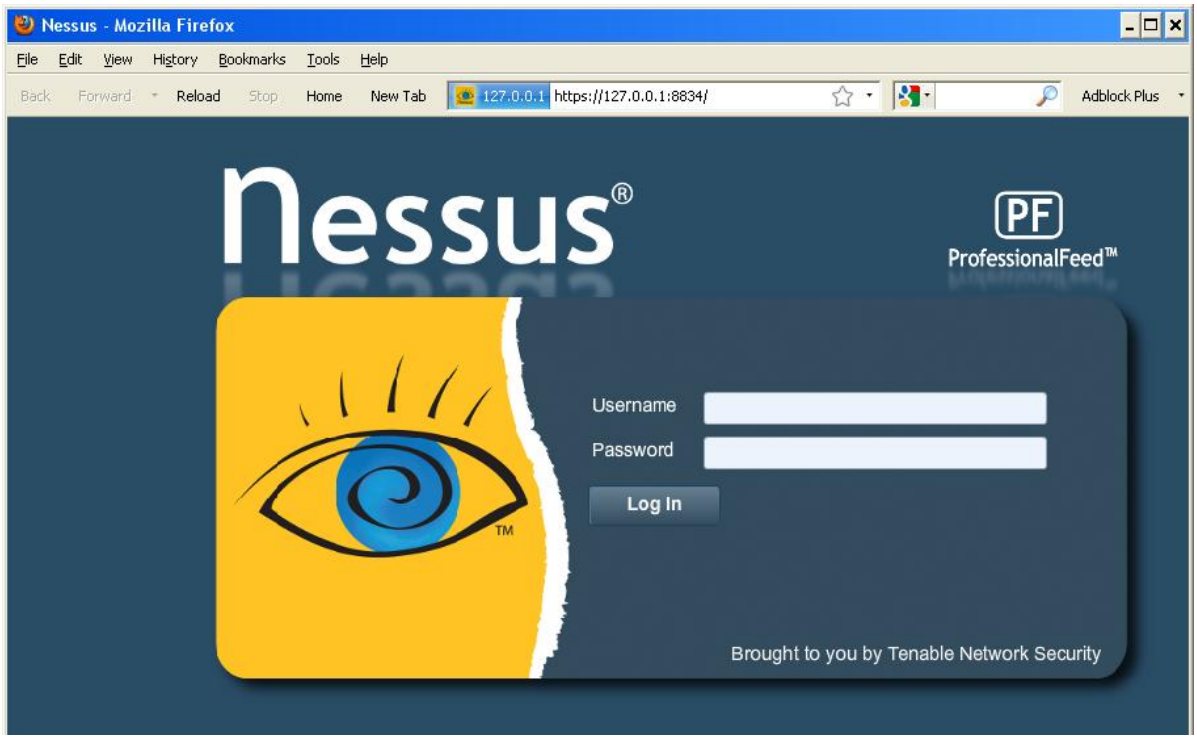


Пользователи браузера Microsoft Internet Explorer могут выбрать вариант «Continue to this website (not recommended)» (Продолжить открытие этого веб-узла (не рекомендуется)), чтобы загрузить интерфейс пользователя Nessus. Пользователи браузера Firefox 3.x могут нажать кнопку «I Understand the Risks» (Я понимаю риски), а затем «Add Exception…» (Добавить исключение…), чтобы вызвать диалоговое окно исключения узлов:

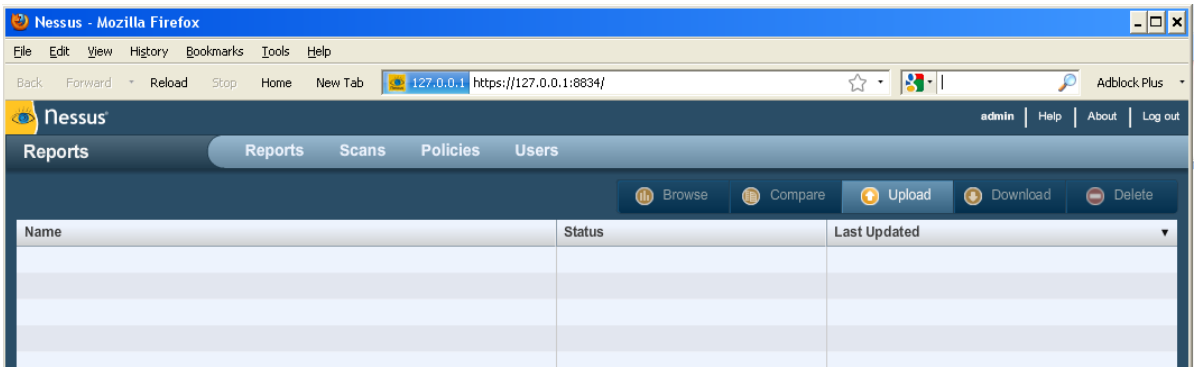


Проверьте, чтобы в поле «Location:» (адрес:) был указан URL-адрес сервера Nessus, и нажмите кнопку **Confirm Security Exception** (подтвердить исключение безопасности). Информацию по установке пользовательского сертификата SSL см. в руководстве по установке Nessus.

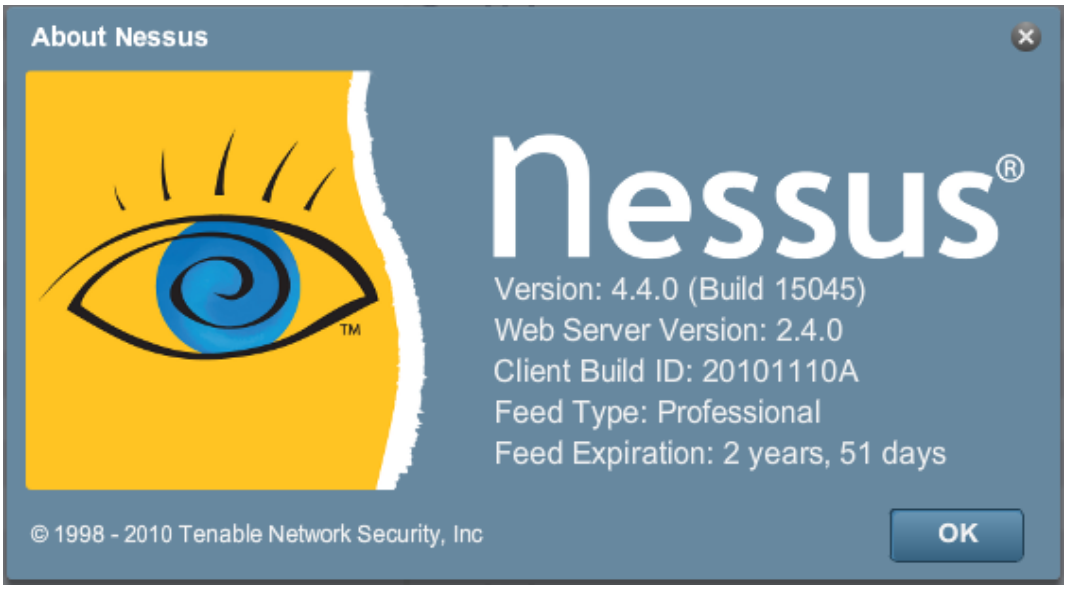
После подтверждения исключения браузером отобразится следующий экран-заставка:



Пройдите проверку подлинности с помощью учетной записи и пароля, созданных ранее администратором сервера. После успешного прохождения проверки подлинности появится интерфейс пользователя с меню для выполнения сканирования:



В любой момент во время пользования сканером Nessus в правом верхнем углу будут присутствовать команды. Ссылка admin (администратор), находящаяся в верхнем правом углу показанного выше экрана, — это текущая учетная запись. Щелкнув эту ссылку, можно изменить свой текущий пароль. Ссылка Help (справка) указывает на документацию Nessus, в которой приведены подробные инструкции по использованию программного обеспечения. Ссылка About (о программе) позволяет просмотреть информацию об установленном программном обеспечении Nessus, включая версию, тип канала, срок действия канала, сборку клиента и версию веб-сервера. Ссылка Log out (выход) позволяет завершить текущий сеанс.



Обзор политики

Политика Nessus состоит из параметров конфигурации, связанных с выполнением сканирования уязвимостей. Эти параметры включают (не ограничиваясь только этим) следующее.

- Параметры управления техническими аспектами сканирования, например таймауты, количество хостов, тип сканера портов и прочее.
- Учетные данные для локального сканирования (например, Windows, SSH), сканирования баз данных Oracle с проверкой подлинности, а также проверки подлинности на базе HTTP, FTP, POP, IMAP или Kerberos.
- Спецификации сканирования на основе фрагментированного семейства или подключаемых модулей.
- Проверки политики соответствия базы данных, подробность отчетов, настройки сканирования обнаружения служб, проверки соответствия Unix и прочее.

Политики по умолчанию

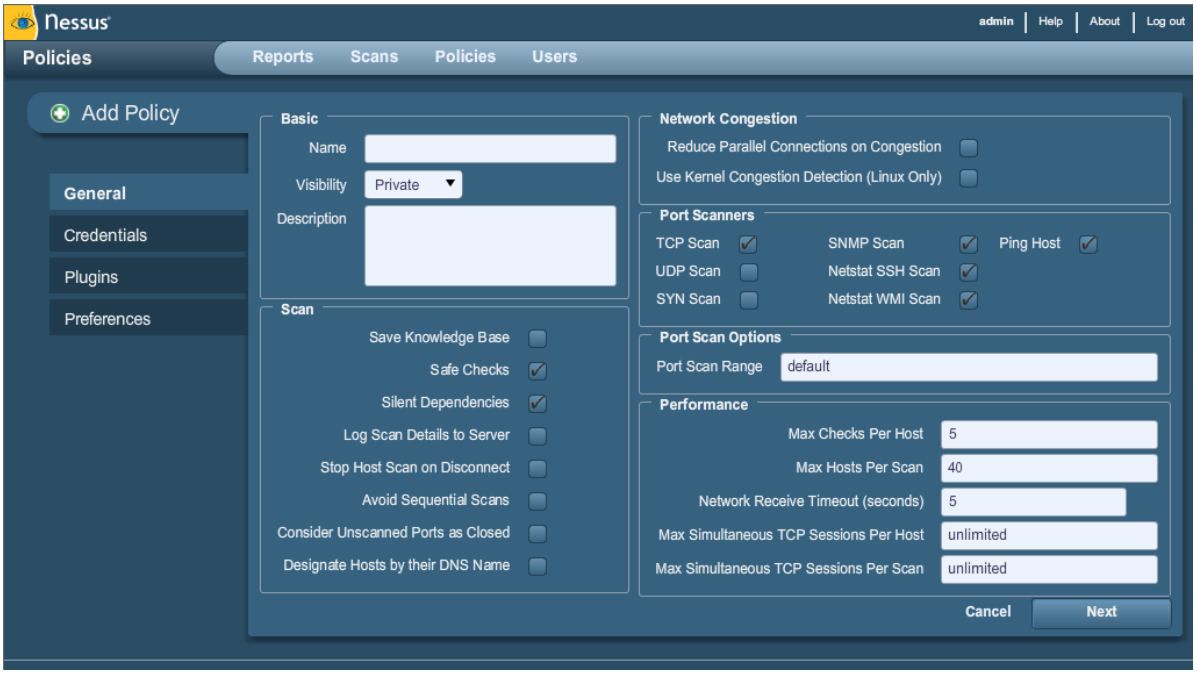
Nessus поставляется с несколькими политиками по умолчанию, предоставляемыми компанией Tenable Network Security, Inc. Их можно использовать в качестве шаблонов для создания индивидуально настроенных политик для вашей организации или же применять без изменений для запуска простого сканирования ресурсов.

Имя политики	Описание
External Network Scan (сканирование внешней сети)	Эта политика настроена для сканирования хостов с внешним выходом, которые обычно предоставляют меньшее количество служб сети. В этой политике включены подключаемые модули, связанные с известными уязвимостями веб-приложений (семейства подключаемых модулей CGI Abuses и CGI Abuses: XSS). Кроме того, для каждого целевого объекта сканируются все 65 535 портов.
Internal Network Scan (сканирование внутренней сети)	Эта политика настроена для оптимальной производительности с учетом того, что она может быть использована для сканирования крупных внутренних сетей с большим количеством хостов, несколькими незащищенными службами и встроенными системами, например принтерами. Подключаемые модули CGI Abuse не включены, и выполняется сканирование стандартного набора портов, а не всех 65 535 портов.
Web App Tests (тесты веб-приложений)	Если вам требуется выполнить сканирование своих систем и обнаружить при помощи Nessus известные и неизвестные уязвимости в своих веб-приложениях, то данная политика предназначена именно для этого. В этой политике включены функции «нечеткого тестирования» Nessus, благодаря которым Nessus будет проверять все обнаруженные веб-сайты и искать уязвимости, присутствующие в каждом из параметров, включая XSS, SQL, внедрение команд и прочее.
Prepare for PCI DSS audits (аудиты подготовки к стандартам PCI DSS)	Эта политика позволяет выполнить встроенные проверки соответствия стандартам PCI DSS, которые сравнивают результаты сканирования со стандартами PCI и выдают отчет о состоянии соответствия стандартам. Очень важно

	отметить, что успешное сканирование на соответствие стандартам не гарантирует соответствия или безопасности инфраструктуры. Организации, подготавливающие оценку соответствия стандартам PCI DSS, могут использовать эту политику для подготовки своей сети и систем к соответствию стандартам PCI DSS.

Создание новой политики

После подключения и интерфейсу пользователя сервера Nessus можно создать пользовательскую политику, щелкнув параметр **Policies** (политики) на верхней панели, а затем нажав кнопку **+ Add** (добавить) справа. Откроется следующее диалоговое окно **Add Policy** (добавление политики):



Обратите внимание, что есть четыре вкладки конфигурации: **General** (общие), **Credentials** (учетные данные), **Plugins** (подключаемые модули) и **Preferences** (предпочтения). Для большинства сред настройки по умолчанию изменять не требуется, но они позволяют более точно управлять работой сканера Nessus. Эти вкладки описаны ниже.

General (общие)

Вкладка General (общие) позволяет назначить имя политике и настроить связанные со сканированием операции. Здесь располагаются шесть групп параметров, управляющих поведением сканера.

В разделе **Basic** (основные) определяются аспекты самой политики.

Параметр	Описание
Name (имя)	Позволяет ввести имя, которое будет отображаться в интерфейсе пользователя Nessus для обозначения этой политики.
Visibility (видимость)	Определяет, будет ли политика *общей* с другими пользователями (Shared) или *закрытой* только для вашего использования (Private). Предоставлять общий доступ к политикам могут только пользователи с правами администратора.
Description (описание)	Используется для ввода краткого описания политики сканирования. Обычно бывает полезно кратко выразить общую цель политики (например, «Сканирование веб-серверов без локальных проверок и служб, не являющихся службами HTTP»).

В разделе **Scan** (сканирование) дополнительно определяются параметры, связанные с поведением сканирования.

Параметр	Описание
Save Knowledge Base (сохранить базу знаний)	Сканер Nessus может сохранять информацию сканирования в базу знаний сервера Nessus для дальнейшего использования. Эта информация включает сведения об открытых портах, успешно работающих подключаемых модулях, обнаруженных службах и т. д.
Safe Checks (безопасные проверки)	При включении параметра Safe Checks (безопасные проверки) будут отключены все подключаемые модули, которые могут отрицательно повлиять на удаленный хост.
Silent Dependencies (скрытые зависимости)	При выборе этого параметра список зависимостей не включается в отчет. Если требуется включить в отчет список зависимостей, снимите этот флажок.
Log Scan Details to Server (сохранение подробного журнала сканирования на сервер)	Сохранение дополнительных сведений о сканировании в журнале сервера Nessus (`nessusd.messages`), включая запуск подключаемых модулей, завершение работы подключаемых модулей, а также аварийное прекращение работы подключаемых модулей. Получаемый в результате журнал можно использовать для подтверждения того, что определенные подключаемые модули были использованы и хосты были просканированы.
Stop Host Scan on Disconnect (остановка сканирования хоста при разрыве соединения)	Если этот флажок установлен, Nessus прекратит сканирования, если обнаружит, что хост перестал отвечать на запросы. Это может происходить в случае отключения пользователями своих ПК во время сканирования, прекращения ответов сервера после

	выполнения подключаемого модуля типа «отказ в обслуживании» или блокирования обмена данными с сервером каким-либо механизмом безопасности (например, IDS). Продолжение сканирования таких машин приведет к отправке ненужного трафика по сети и задержке сканирования.
Avoid Sequential Scans (избегать последовательного сканирования)	По умолчанию сервер Nessus сканирует список IP-адресов по порядку. В случае установки этого флажка Nessus будет сканировать список хостов в случайном порядке. Обычно это бывает полезно для распределения сетевого трафика, направленного в определенную подсеть во время объемных сканирований.
Consider Unscanned Ports as Closed (считать не просканированные порты закрытыми)	Если порт не был просканирован выбранным сканером портов (например, если он не входит в выбранный диапазон портов), сервер Nessus будет считать его открытым.
Designate Hosts by their DNS Name (обозначать хосты их именами DNS)	Использовать имя хоста, а не IP-адрес в отчете.

В разделе **Network** (сеть) приведены параметры, позволяющие лучше управлять сканированием на основании сканируемой сети.

Параметр	Описание
Reduce Parallel Connections on Congestion (сокращать количество параллельных соединений при перегрузке)	Этот параметр позволяет серверу Nessus обнаруживать, когда он отправляет слишком много пакетов и пропускная способность сети исчерпывается. В случае обнаружения такой ситуации сервер Nessus ограничит сканирования для устранения и снижения перегрузки сети. После ослабления перегрузки сервер Nessus автоматически снова попытается использовать доступную пропускную способность сети.
Use Kernel Congestion Detection (Linux Only) (использовать обнаружение перегрузки ядра (только для Linux))	Позволяет серверу Nessus отслеживать перегрузку ЦП и других внутренних процессов и соответственно масштабировать свою нагрузку. Сервер Nessus всегда будет пытаться максимально использовать доступные ресурсы. Эта функция доступна только для сканеров Nessus, развернутых в ОС Linux.

В разделе **Port Scanners** (сканеры портов) осуществляется управление методами сканирования портов, применяемыми при сканировании.

Параметр	Описание
TCP Scan (сканирование TCP)	Использование встроенного в сервер Nessus сканера TCP для определения открытых портов TCP на сканируемых машинах. Этот сканер оптимизирован и имеет некоторые функции самонастройки.  На некоторых платформах (например, Windows и Mac OS X) в случае возникновения серьезных проблем производительности системы при использовании сканера TCP сервер Nessus запустит сканер SYN.
UDP Scan (сканирование UDP)	Этот параметр включает встроенный в сервер Nessus сканер UDP для определения открытых портов UDP на сканируемых машинах.  Протокол UDP не поддерживает состояний. Это означает, что соединение устанавливается без обмена подтверждениями. Связь на основе протокола UDP не всегда надежна, и из-за характера служб UDP, а также контролирующих доступ устройств они не всегда могут быть обнаружены удаленно.
SYN Scan (сканирование SYN)	Использование встроенного в сервер Nessus сканера SYN для определения открытых портов TCP на сканируемых машинах. Сканирование SYN представляет собой популярный метод сканирования портов и считается несколько менее влияющим на работу системы, чем сканирование TCP. Сканер отправляет пакет SYN на порт, ожидает ответа SYN-ACK и определяет состояние порта на основании наличия или отсутствия ответа.
SNMP Scan (сканирование SNMP)	Укажите серверу Nessus сканировать хосты в плане службы SNMP. Сервер Nessus подберет соответствующие настройки SNMP во время сканирования. Если настройки предоставляются пользователем в разделе Preferences (предпочтения), это позволяет серверу Nessus лучше протестировать удаленный хост и получить более подробные результаты аудита. Например, есть много проверок маршрутизаторов Cisco, которые позволяют определить существующие уязвимости путем проверки версии возвращенной строки SNMP. Эта информация необходима для указанных аудитов.
Netstat SSH Scan (сканирование Netstat SSH)	Этот параметр использует команду **`netstat`** для проверки открытых портов с локальной машины. При этом предполагается доступность команды **`netstat`** через соединение SSH со сканируемым хостом. Это

	сканирование предназначено для систем на базе Unix и требует наличия учетных данных для проверки подлинности.
Netstat WMI Scan (сканирование Netstat WMI)	Этот параметр использует команду **`netstat`** для проверки открытых портов с локальной машины. При этом предполагается доступность команды **`netstat`** через соединение WMI со сканируемым хостом. Это сканирование предназначено для систем на базе Windows и требует наличия учетных данных для проверки подлинности.  При сканировании на основе WMI для определения открытых портов используется команда **`netstat`**, при этом любые указанные диапазоны портов игнорируются. В случае успешного выполнения какого-либо перечислителя портов (Netstat или SNMP) диапазону портов присваивается значение all (все).
Ping Host (проверка связи с хостом)	Этот параметр включает проверку связи с удаленными хостами с помощью команды ping по нескольким портам.

В разделе **Port Scan Options** (параметры сканирования портов) настраивается сканирование определенного диапазона портов. Параметр Port Scan Range (диапазон сканирования портов) может иметь следующие значения.

Значение	Описание
“default” (по умолчанию)	При использовании ключевого слова default (по умолчанию) сервер Nessus выполнит сканирование примерно 4 790 наиболее часто используемых портов. Список портов приведен в файле **`nessus-services`**.
“all” (все)	При использовании ключевого слова all (все) сервер Nessus выполнит сканирование всех 65 535 портов.
Custom List (пользовательский список)	Пользовательский диапазон портов может быть выбран с помощью разделенного запятыми списка портов или диапазонов портов. Например, допустимы такие списки: “21,23,25,80,110” или “1-1024,8080,9000-9200”. При использовании значения “1-65535” выполняется сканирование всех портов.

 Указанный диапазон сканирования портов применяется для сканирования TCP и UDP.

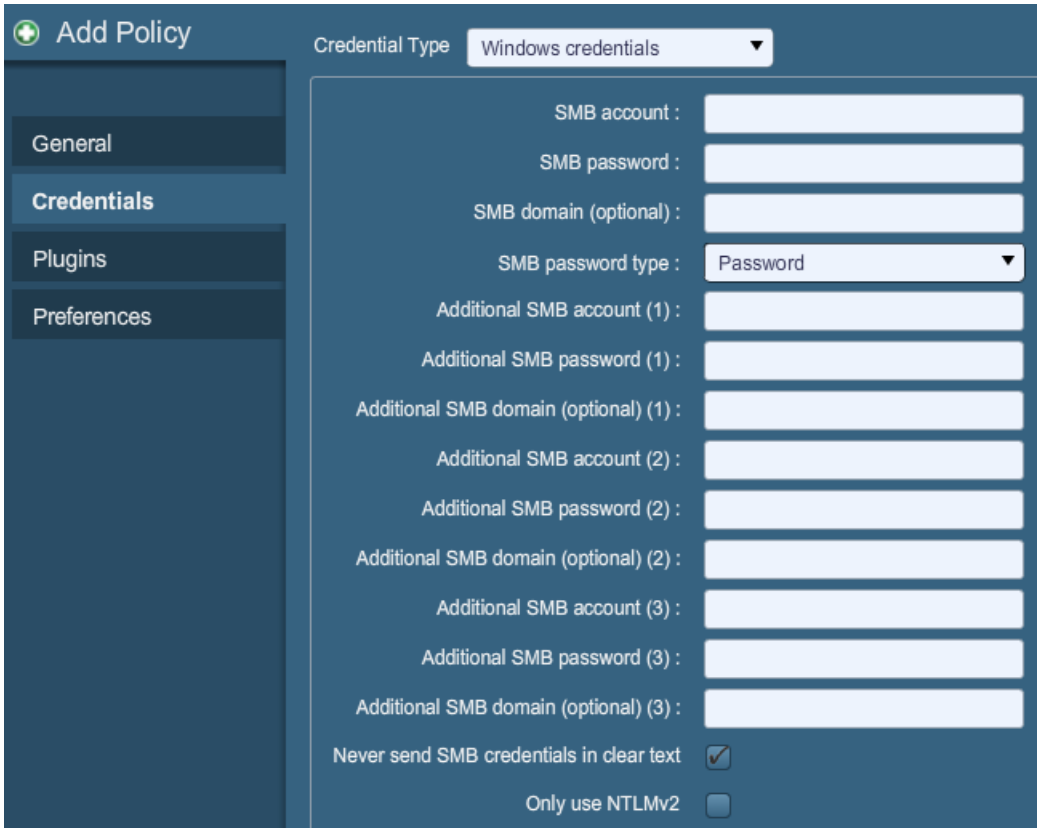
В разделе **Performance** (производительность) расположены два параметра, управляющие количеством запускаемых сканирований. Эти параметры, пожалуй,

наиболее важны при настройке сканирования. Потому что они сильнее всего влияют на время сканирования и активность сети.

Параметр	Описание
Max Checks Per Host (максимальное количество проверок одного хоста)	Эта настройка ограничивает максимальное количество проверок, выполняемых сканером Nessus одновременно по одному хосту.
Max Hosts Per Scan (максимальное количество хостов при одном сканировании)	Эта настройка ограничивает максимальное количество хостов, одновременно сканируемых сканером Nessus.
Network Receive Timeout (seconds) (таймаут ответа сети (секунды))	По умолчанию установлено значение пять секунд. Это время ожидания сервером Nessus ответа от хоста, если иное не определено в подключаемом модуле. В случае сканирования через медленное соединение стоит установить большее количество секунд.
Max Simultaneous TCP Sessions Per Host (максимальное количество одновременных сеансов TCP на один хост)	Эта настройка ограничивает максимальное количество устанавливаемых сеансов TCP на один хост.
Max Simultaneous TCP Sessions Per Scan (максимальное количество одновременных сеансов TCP на сканирование)	Эта настройка ограничивает максимальное количество устанавливаемых сеансов TCP на все сканирование, независимо от количества сканируемых хостов.  Для сканеров Nessus, установленных на хосты с ОС Windows XP, Vista и 7, для получения точных результатов это значение должно быть 19 или меньше.

Credentials (учетные данные)

Вкладка Credentials (учетные данные), показанная ниже, позволяет настроить сканер Nessus для использования учетных данных проверки подлинности при сканировании. При настройке учетных данных сканер Nessus может выполнять более широкий спектр проверок, что дает в итоге более точные результаты сканирования.



Элемент раскрывающегося меню **Windows credentials** (учетные данные Windows) содержит настройки, предоставляющие серверу Nessus такую информацию, как имя учетной записи SMB, пароль и имя домена. Server Message Block (SMB) — это протокол совместного доступа к файлам, обеспечивающий прозрачный обмен информацией между компьютерами в сети. Предоставление этой информации серверу Nessus позволит ему находить локальную информацию от удаленного хоста Windows. Например, использование учетных данных позволяет серверу Nessus определять, применены ли важные исправления безопасности. Нет необходимости изменять другие параметры SMB, установленные по умолчанию.

В случае создания служебной учетной записи SMB с ограниченными правами администрирования сервер Nessus может легко и безопасно сканировать многочисленные домены.

Tenable рекомендует сетевым администраторам рассмотреть возможность создания определенных доменных учетных записей для удобства тестирования. Сканер Nessus включает различные проверки безопасности для ОС Windows NT, 2000, Server 2003, XP, Vista, Windows 7 и Windows 2008, которые обеспечивают большую точность в случае указания доменной учетной записи. Сканер Nessus не пытается выполнить несколько проверок в большинстве случаев, если учетная запись не указана.

Служба удаленного управления реестром ОС Windows позволяет удаленным компьютерам с учетными данными получать доступ к реестру проверяемого компьютера. Если служба не запущена, то чтение разделов и значений из реестра невозможно даже при наличии полных учетных данных.

Дополнительные сведения см. в блоге Tenable в публикации под названием Dynamic Remote Registry Auditing - Now you see it, now you don't! (динамический удаленный аудит реестра — когда он доступен, а когда нет).

Пользователи могут выбрать команду **SSH settings** (настройки SSH) из раскрывающегося меню и ввести учетные данные для сканирования систем Unix. Эти учетные данные используются для получения локальной информации от удаленных систем Unix для аудита исправлений или проверок соответствия стандартам. Есть поле для ввода имени пользователя SSH для учетной записи, которая будет выполнять проверки на сканируемой системе Unix, а также ввода пароля SSH или пары открытого и закрытого ключа SSH. Есть также поле для ввода парольной фразы для ключа SSH, если требуется.

Nessus 4 поддерживает алгоритмы шифрования **`blowfish-cbc`**, **`aes-cbc`** и **`aes-ctr`**.

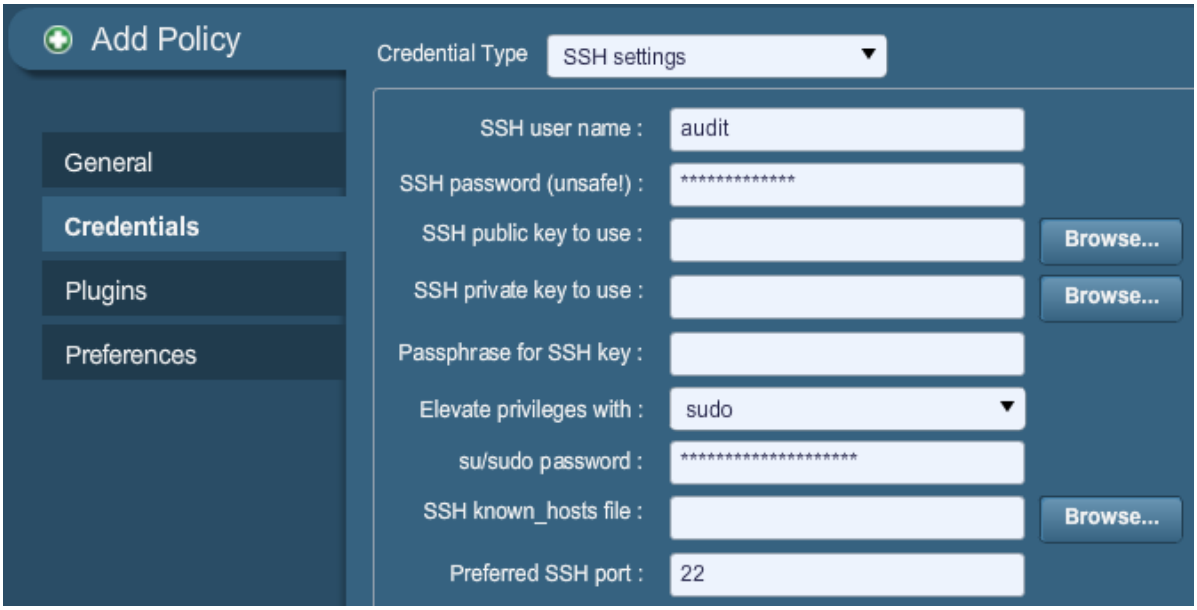
Наиболее эффективно сканирование с учетными данными, если предоставлены учетные данные с правами root. Поскольку многие узлы не допускают удаленного входа с правами root, пользователи Nessus могут вызывать команды **`su`** или **`sudo`** с отдельным паролем для учетной записи, которой присвоены права **`su`** или **`sudo`**.

Сервер Nessus может использовать доступ на основе ключей SSH для проверки подлинности удаленным сервером. Если файл SSH known_hosts доступен и предоставлен в рамках политики сканирования, сервер Nessus будет пытаться выполнить вход только в хосты, указанные в этом файле. Наконец, может быть задан параметр Preferred SSH port (предпочтительный порт SSH) для подключения сервера Nessus к серверу SSH, если он выполняется не на порту 22, а на любом другом порту.

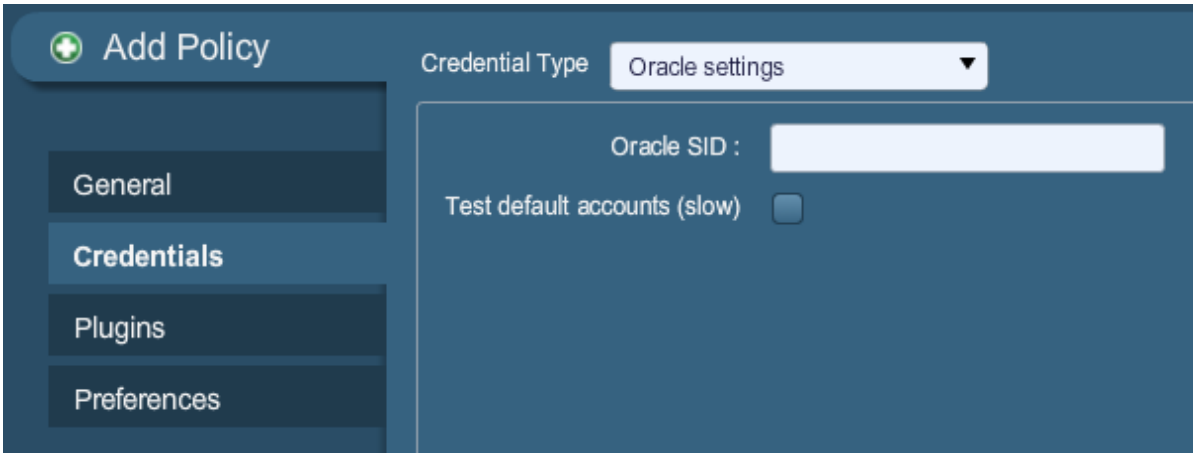
Сервер Nessus шифрует все пароли, сохраняемые в политиках. Однако рекомендуется использовать для проверки подлинности ключи SSH, а не пароли SSH. Это помогает гарантировать, что имя пользователя и пароль, используемые вами для аудита известных серверов SSH, не будут использованы для попытки несанкционированного входа в систему. Таким образом не рекомендуется использовать пароли SSH, если в этом нет необходимости.

Сервер Nessus также поддерживает настройку su+sudo, которая может использоваться в случае, если система не позволяет имеющим привилегии учетным записям использовать права удаленного входа.

Ниже приведен пример снимка экрана с использованием команды **`sudo`** для повышения уровня прав для сканирования. В этом примере учетная запись пользователя — audit, которая была добавлена в файл **`/etc/sudoers`** на сканируемой системе. Предоставленный пароль является паролем учетной записи audit, а не паролем root:

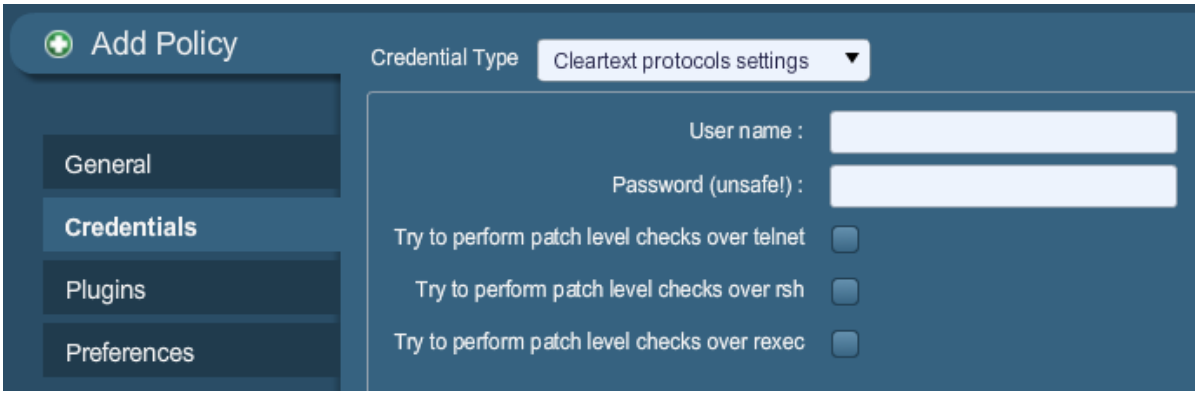


На вкладке Credentials (учетные данные) также есть команда в раскрывающемся меню для конфигурации **Oracle settings** (настроек Oracle), а именно Oracle SID и параметра тестирования на наличие известных учетных записей по умолчанию в программном обеспечении Oracle:



Настройка **Kerberos configuration** (конфигурация Kerberos) позволяет указать учетные данные с помощью ключей Kerberos с удаленной системы:

Наконец, при отсутствии защищенного метода выполнения проверок с использованием учетных данных, пользователи могут настроить Nessus для попытки выполнения проверок через незащищенные протоколы, выполнив конфигурацию с помощью команды раскрывающегося меню **Cleartext protocol settings** (настройки протоколов с открытым текстом). Этот параметр поддерживает следующие протоколы с открытым текстом: **telnet**, **rsh** и **rexec**.

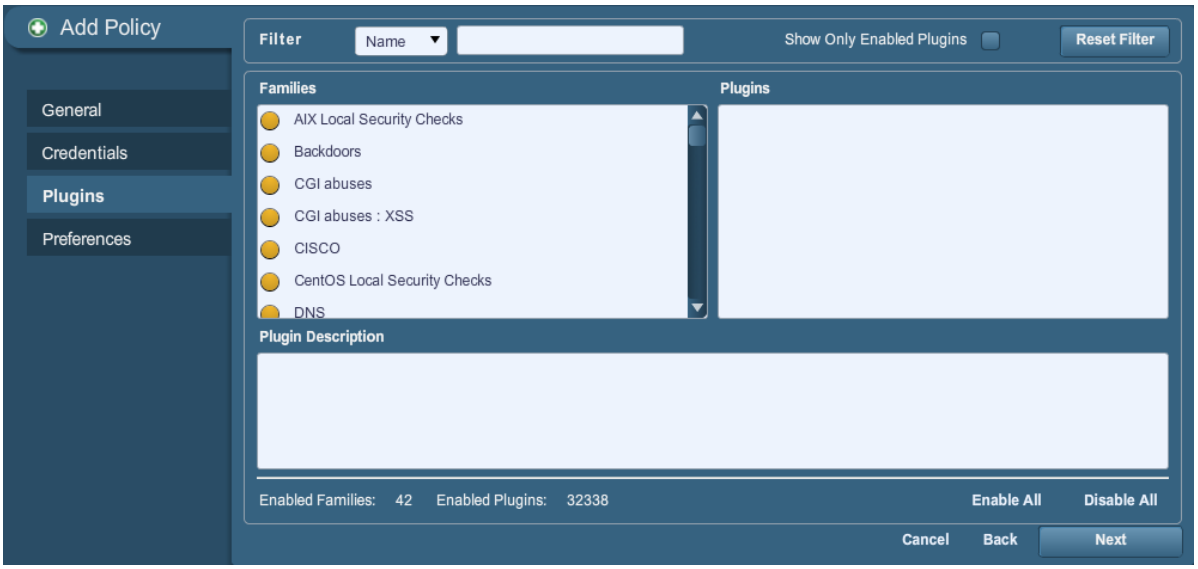


По умолчанию все пароли (и сама политика) шифруются. В случае сохранения политики в файле `.nessus` и последующего копирования этого файла `.nessus` на другую установку Nessus, все пароли политики будут недоступны для второго сканера Nessus, поскольку он не сможет их расшифровать.

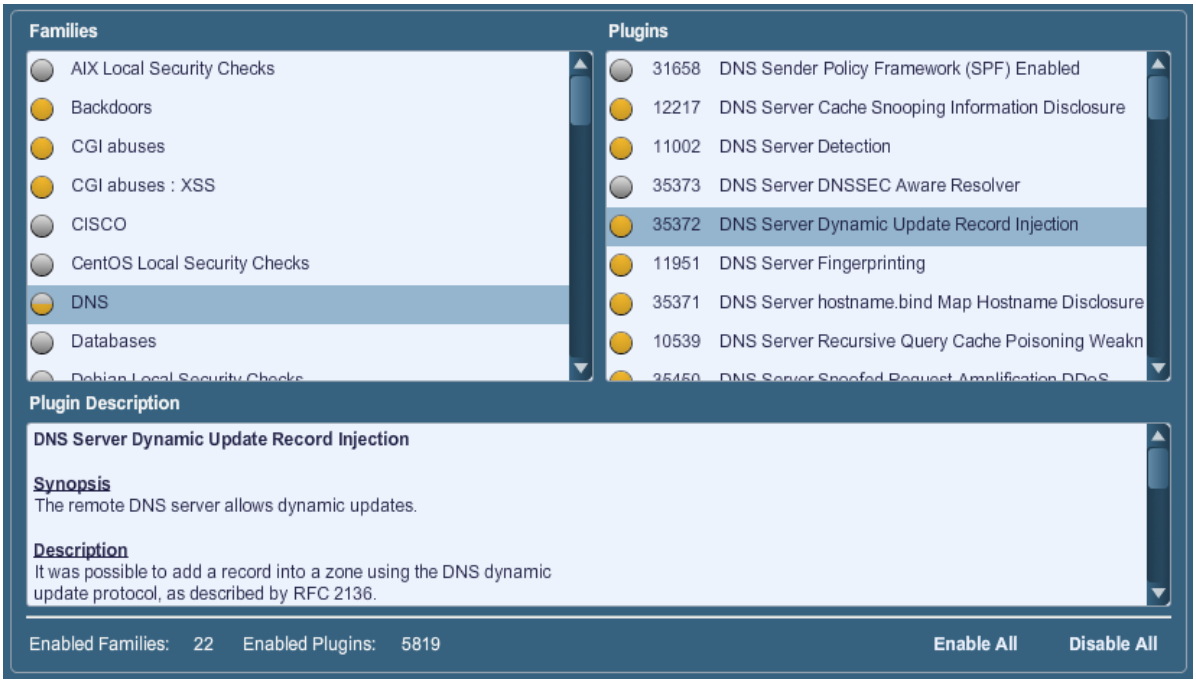
Использование открытых учетных данных каким-либо образом **не** рекомендуется! В случае удаленной отправки учетных данных (например, через сканирование Nessus), эти учетные данные могут быть перехвачены любым лицом, имеющим доступ к сети. При наличии возможности всегда используйте шифрованные механизмы проверки подлинности.

Plugins (подключаемые модули)

На вкладке Plugin Selection (выбор подключаемых модулей) пользователь может выбрать определенные проверки безопасности с помощью семейства подключаемых модулей или отдельных проверок.



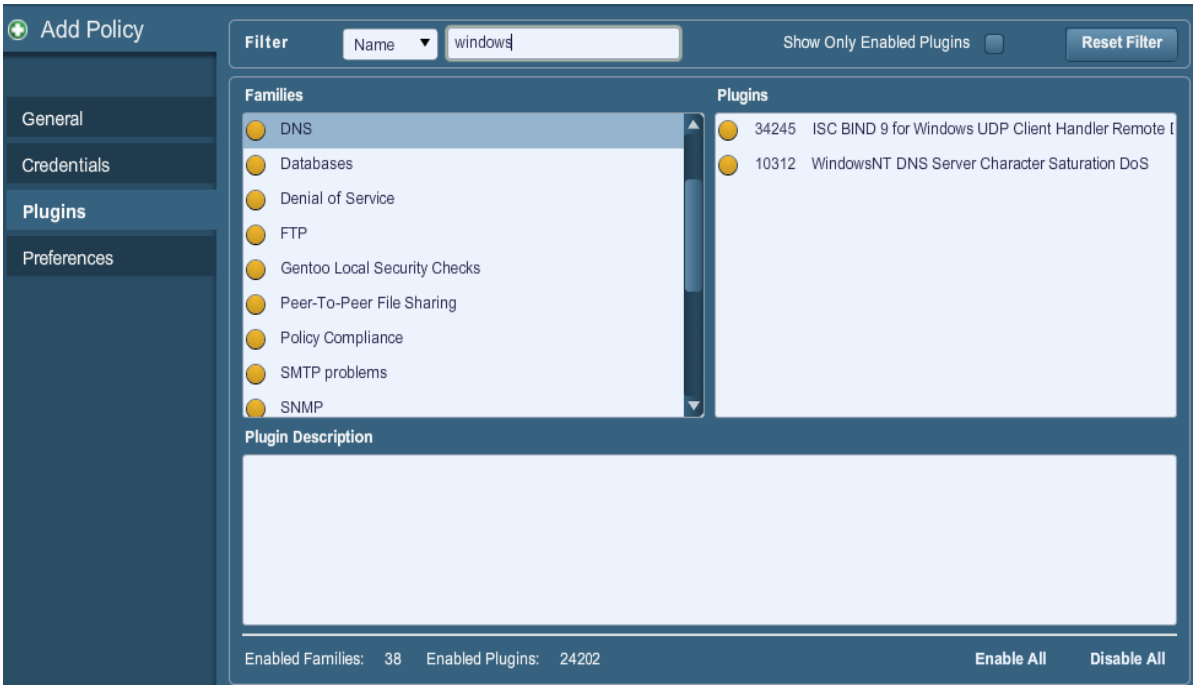
Щелчок по желтому кружку рядом с семейством подключаемых модулей включает или отключает все соответствующее семейство. При выборе какого-либо семейства на верхней правой панели отображается список входящих в него подключаемых модулей. Для создания специализированных политик сканирования можно включать или отключать отдельные подключаемые модули. При выполнении настроек общее количество выбранных семейств и отдельных подключаемых модулей отображается в нижней части окна. Если кружок рядом с семейством подключаемых модулей наполовину серый и наполовину желтый, это означает, что некоторые из входящих в него подключаемых модулей включены, но не все.



При выборе определенного подключаемого модуля отображаются выходные данные подключаемого модуля, которые будут отображаться в отчете. В разделах synopsis (сводка) и description (описание) приводятся более подробные данные о проверяемой

уязвимости. При прокрутке панели Plugin Description (описание подключаемого модуля) также отобразится информация о решении, дополнительные ссылки (при наличии) и балл CVSSv2, предоставляющий базовую оценку риска.

В верхней части вкладки семейств подключаемых модулей можно выполнять поиск определенного подключаемого модуля по имени или идентификатору. В поле, расположенном рядом с надписью **Filter** (фильтр), введите текст для поиска и нажмите клавишу Enter.



При создании и сохранении политики она регистрирует все подключаемые модули, которые были первоначально выбраны. При получении новых подключаемых модулей через канал обновления подключаемых модулей они автоматически включатся, если включено семейство, с которым они связаны. Если семейство было отключено или частично отключено, то новые подключаемые модули в этом семействе будут также автоматически отключены.

Семейство Denial of Service (отказ в обслуживании) содержит некоторые подключаемые модули, которые могут вызывать перебои в работе корпоративной сети, если не включен параметр Safe Checks (безопасные проверки). Но здесь также есть некоторые полезные проверки, которые не могут причинить никакого вреда. Семейство Denial of Service (отказ в обслуживании) может использоваться в сочетании с параметром Safe Checks (безопасные проверки), который не допускает выполнения каких-либо потенциально опасных подключаемых модулей. В то же время не рекомендуется использовать семейство Denial of Service (отказ в обслуживании) в ответственных сетях.

Под окном plugins (подключаемые модули) находятся два параметра, которые помогают выбирать подключаемые модули.

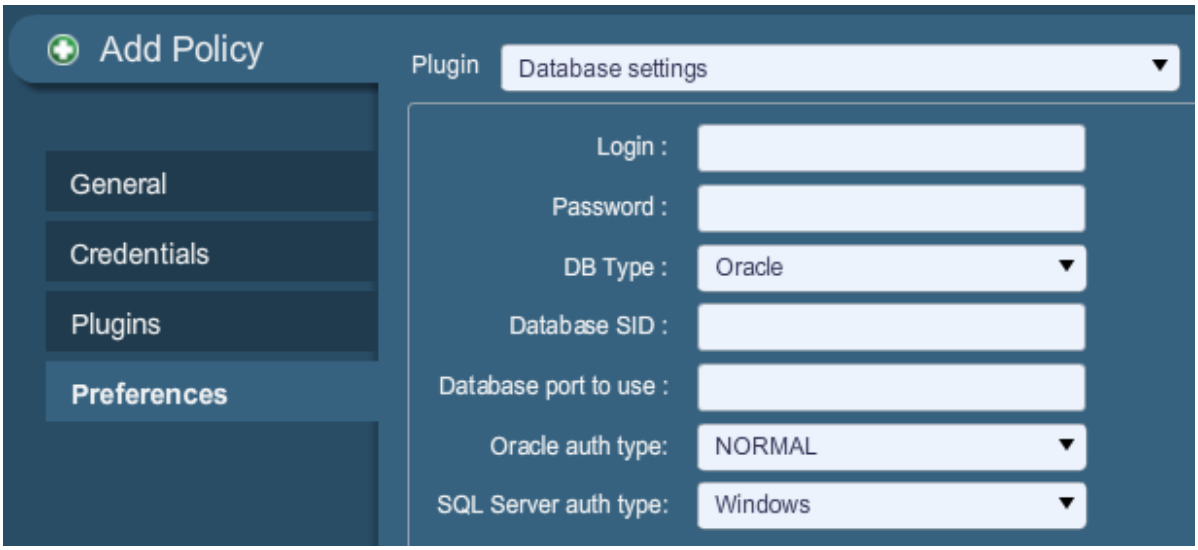
Параметр	Описание
Enable all (включить все)	Выбирает и включает все подключаемые модули и их семейства. С помощью этого параметра удобно повторно включать все подключаемые модули после создания политики с некоторыми отключенными семействами или подключаемыми модулями. Обратите внимание, что для некоторых подключаемых модулей могут потребоваться дополнительные настройки.
Disable all (отключить все)	Отменяет выбор и отключает все подключаемые модули и их семейства. Выполнение сканирования со всеми отключенными подключаемыми модулями не даст каких-либо результатов.

Preferences (предпочтения)

Вкладка **Preferences** (предпочтения) содержит средства тонкого управления настройками сканирования. При выборе элемента раскрывающегося меню отображаются дополнительные элементы конфигурации для выбранной категории. Обратите внимание, что это динамический список параметров конфигурации, зависящий от канала подключаемых модулей, политик аудита и дополнительных функций, к которым имеет доступ подключенный сканер Nessus. Сканер с настроенным каналом ProfessionalFeed может иметь больше дополнительных параметров конфигурации, чем сканер с настроенным каналом HomeFeed. Этот список также может меняться при добавлении или изменении подключаемых модулей.

Категория **Cisco IOS Compliance Checks** (проверки на соответствие Cisco IOS) позволяет клиентам канала ProfessionalFeed отправлять на сервер файлы политик, которые будут использоваться для определения того, отвечает ли проверяемое устройство на базе Cisco IOS определенным стандартам. Допускается одновременный выбор до пяти политик. Политики могут выполняться для Saved (сохраненных) (**`show config`**), Running (выполняемых) (**`show running`**) или Startup (запускаемых) (**`show startup`**) конфигураций.

Категория **Database Compliance Checks** (проверки соответствия баз данных) позволяет клиентам канала ProfessionalFeed отправлять на сервер файлы политик, которые будут использоваться для определения того, отвечает ли проверяемая база данных определенным стандартам. Допускается одновременный выбор до пяти политик.

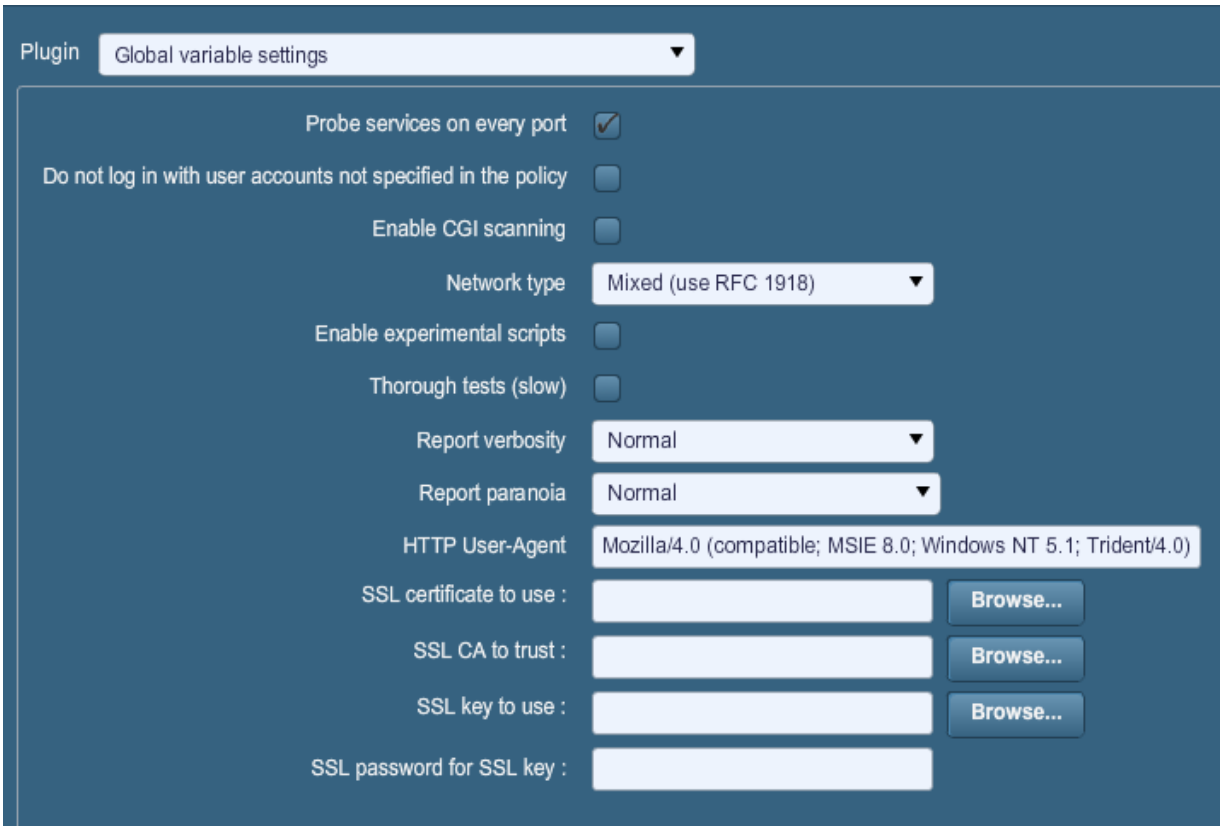


Параметры **Database settings** (настройки базы данных) используются для определения типа проверяемой базы данных, соответствующих настроек и учетных данных.

Параметр	Описание
Login (имя входа)	Имя пользователя для базы данных.
Password (пароль)	Пароль, соответствующий указанному имени пользователя.
DB Type (тип базы данных)	Поддерживаются базы данных Oracle, SQL Server, MySQL, DB2, Informix/DRDA и PostgreSQL.
Database SID (SID базы данных)	Системный идентификатор (SID) проверяемой базы данных.

Database port to use (используемый порт базы данных)	Прослушиваемый базой данных порт.
Oracle auth type (тип проверки подлинности Oracle)	Поддерживаются типы NORMAL, SYSOPER и SYSDBA.
SQL Server auth type (тип проверки подлинности SQL Server)	Поддерживаются типы Windows и SQL.

Параметр **Do not scan fragile devices** (не сканировать чувствительные устройства) при включении указывает сканеру Nessus не сканировать принтеры или хосты Novell Netware. Поскольку обе эти технологии более подвержены возникновению условий отказа в обслуживании, сканер Nessus может не выполнять их сканирование. Эта настройка рекомендуется при выполнении сканирования в рабочее время.

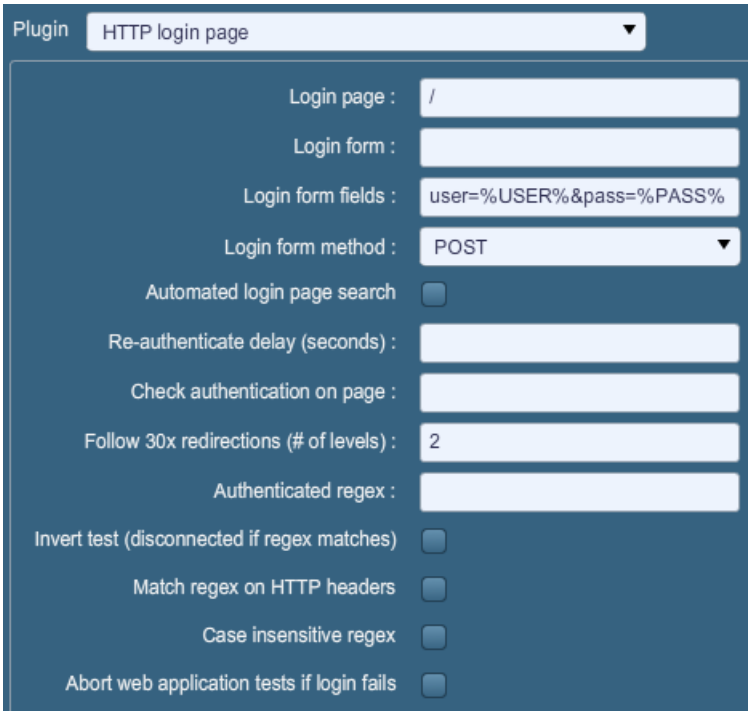


Категория **Global variable settings** (настройки глобальных переменных) содержит широкий спектр параметров конфигурации сервера Nessus.

Параметр	Описание
Probe services on every port (выполнять проверку служб на каждом порту)	Выполняется попытка сопоставить каждый открытый порт со службой, выполняемой на этом порту. Обратите внимание, что в некоторых редких случаях это может нарушать работу служб и приводить к непредсказуемым побочным эффектам.
Do not log in with user accounts not specified in the policy (не входить под именами учетных записей, не указанными в политике)	Используется для предотвращения блокировки учетных записей, если политика управления паролями настроена на блокировку учетных записей после нескольких неудачных попыток входа.
Enable CGI scanning (включить сканирование CGI)	Активирует проверки CGI. Отключение этого параметра очень значительно ускоряет аудит локальной сети.
Network type (тип сети)	Позволяет указать, используются ли общие маршрутизируемые IP-адреса, частные IP-адреса без поддержки интернет-маршрутизации или сочетание обоих видов адресов. Выберите параметр Mixed (сочетание) в случае использования адресов RFC 1918 и наличия в вашей сети нескольких маршрутизаторов.
Enable experimental scripts (включить экспериментальные скрипты)	Включает использование при сканировании подключаемых модулей, которые считаются экспериментальными. Не включайте эту настройку при сканировании производственных сетей.
Thorough tests (slow) (подробные тесты (медленно))	Приводит к «более интенсивной работе» разных подключаемых модулей. Например, при просмотре файловых ресурсов общего доступа SMB подключаемый модуль может анализировать 3 уровня в глубину вместо 1. В некоторых случаях это может вызывать гораздо больший объем сетевого трафика и анализа. Обратите внимание, что при большей подробности сканирование может оказывать большее влияние, что повышает вероятность нарушения работы сети. Хотя потенциально такое сканирование может дать более оптимальные результаты аудита.
Report verbosity (подробность отчета)	Чем выше значение этой настройки, тем больше информации о действиях подключаемых модулей будет включено в отчет.
Report paranoia (уровень «паранойи» отчетов)	В некоторых случаях сканер Nessus не может определить удаленно, присутствует нарушение или нет. Если установлен «уровень паранойи» **Paranoid** (параноидный), то нарушение будет включаться в отчет каждый раз, когда есть сомнения, подвержен ли удаленный хост этому

	нарушению. И наоборот, если установлен «уровень паранойи» **Avoid false alarm** (избегать ложных сигналов тревоги), то сканер Nessus не будет включать в отчет каких-либо нарушений при наличии неопределенности в отношении удаленного хоста. Значение по умолчанию (**Normal** (нормальный)) представляет собой средний уровень между двумя описанными выше настройками.
HTTP User-Agent (пользователь-агент HTTP)	Определяет тип веб-браузера, который будет имитировать Nessus при сканировании.
SSL certificate to use (использовать сертификат SSL)	Позволяет сканеру Nessus использовать клиентскую часть сертификата SSL для связи с удаленным хостом.
SSL CA to trust (надежный SSL CA)	Определяет центр сертификации (Certificate Authority, CA), которому будет доверять сканер Nessus.
SSL key to use (использовать ключ SSL)	Определяет локальный ключ SSL, который будет использоваться для связи с удаленным хостом.
SSL password for SSL key (пароль SSL для ключа SSL)	Пароль для управления указанным ключом SSL.

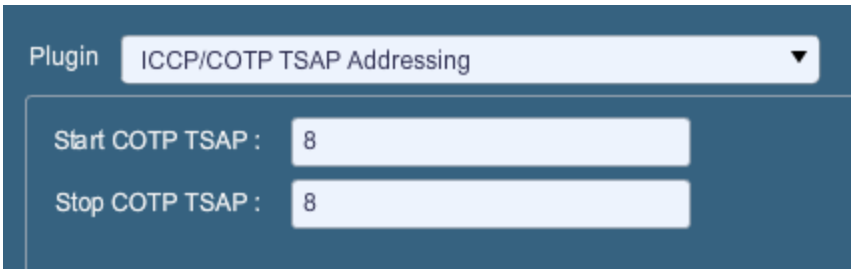
Для обеспечения тестирования веб-приложений сканер Nessus может импортировать файлы cookie HTTP из другого программного обеспечения (например, из веб-браузера, веб-прокси и т. д.) с помощью настроек **HTTP cookies import** (импорт файлов cookie HTTP). Файлы cookie могут быть отправлены на сервер, чтобы Nessus использовал эти файлы cookie при попытке доступа к веб-приложению. Файл cookie должен быть в формате Netscape.



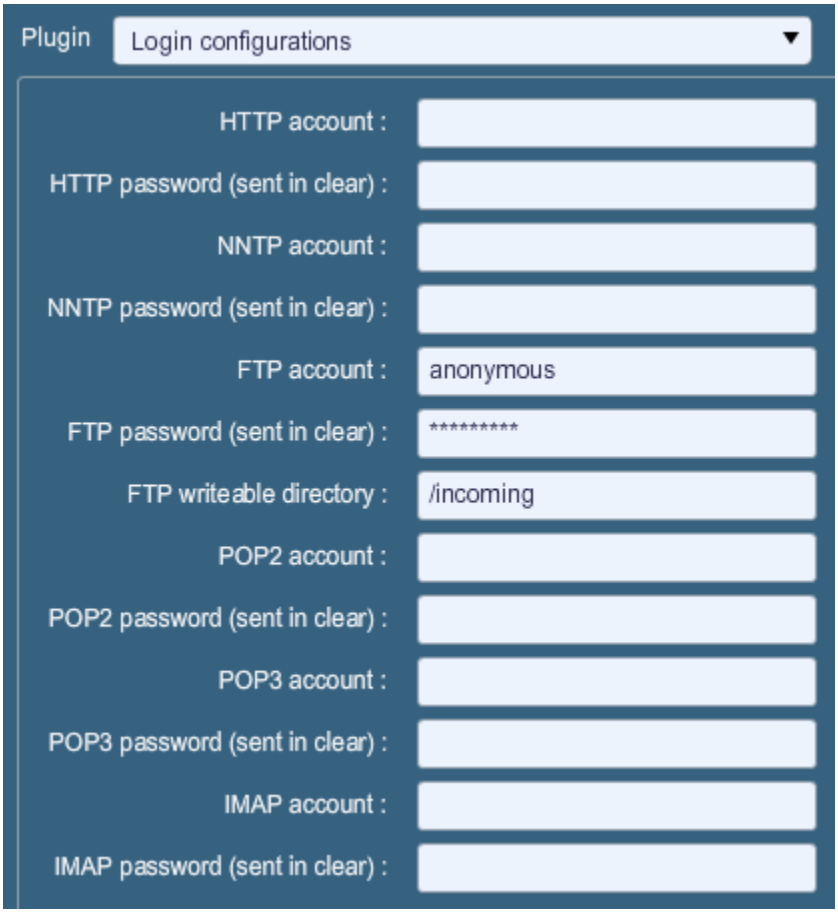
Настройки **HTTP login page** (страница входа HTTP) обеспечивают управление точкой начала тестирования пользовательского веб-приложения с проверкой подлинности.

Параметр	Описание
Login page (страница входа)	Исходный URL-адрес страницы входа в приложение.
Login form (форма входа)	Параметр action метода form. Например, параметр login form (форма входа) для `<form method="POST" name="auth_form" action="/login.php">` будет `/login.php`.
Login form fields (поля формы входа)	Укажите параметры проверки подлинности (например, **`login=%USER%&password=%PASS%`**). При использовании ключевых слов %USER% и %PASS% они будут заменены значениями, предоставленными в раскрывающемся меню Login configurations (конфигурации входа). Это поле может использоваться для предоставления более чем двух параметров (например, имени группы (group) или иной информации, требуемой для процесса проверки подлинности).
Login form method (метод формы входа)	Укажите, выполняется ли действие входа через запрос GET или POST.
Automated login page search (автоматизированный поиск страницы входа)	Указывает сканеру Nessus выполнить поиск страницы входа.

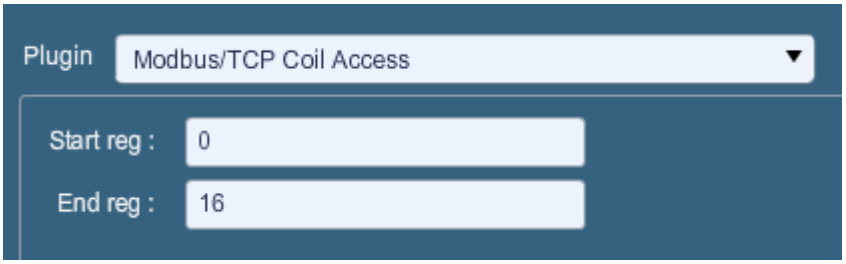
Re-authenticate delay (seconds) (задержка повторной проверки подлинности (секунды))	Задержка между попытками проверки подлинности. Это полезная настройка, позволяющая избежать срабатывания механизмов блокировки при попытке подбора учетных данных.
Check authentication on page (тестировать проверку подлинности на странице)	URL-адрес защищенной веб-страницы, которая требует проверки подлинности, чтобы помочь сканеру Nessus в определении статуса проверки подлинности.
Follow 30x redirections (# of levels) (следовать перенаправлениям 30x (кол-во уровней))	В случае получения от веб-сервера кода перенаправления 30x эта настройка указывает сканеру Nessus, следовать предоставленной ссылке или нет.
Authenticated regex (регулярное выражение успешной проверки подлинности)	Регулярное выражение, которое сканер будет ожидать от страницы входа. Просто получение ответного кода 200 не всегда достаточно для определения состояния сеанса. Сканер Nessus может попытаться найти соответствие заданной строке, например Authentication successful! (проверка подлинности успешно выполнена).
Invert test (disconnected if regex matches) (обратный тест (разорвать соединение в случае совпадения регулярного выражения))	Регулярное выражение, которое сканер будет ожидать от страницы входа, сообщающее сканеру Nessus в случае получения, что проверка подлинности не была успешной. Например, Authentication failed! (ошибка проверки подлинности).
Match regex on HTTP headers (искать регулярные выражения в заголовках HTTP)	Вместо поиска в основном тексте ответа, сканер Nessus может выполнять поиск заданных регулярных выражений в заголовках ответов HTTP, чтобы лучше определять состояние проверки подлинности.
Case insensitive regex (регулярные выражения без учета регистра)	Поиск регулярных выражений по умолчанию выполняется с учетом регистра. Эта настройка указывает сканеру Nessus игнорировать регистр.
Abort web application tests if login fails (отменять тесты веб-приложения в случае ошибки входа)	Если предоставленные учетные данные не сработают, то сканер Nessus отменит тесты пользовательского веб-приложения (но не семейств CGI подключаемых модулей).



Меню **ICCP/COTP TSAP Addressing** (адресация ICCP/COTP TSAP) предназначено специально для проверок SCADA. Оно определяет значение точек TSAP протокола COTP на сервере ICCP путем подбора возможных значений. По умолчанию устанавливается начальное и конечное значение 8.



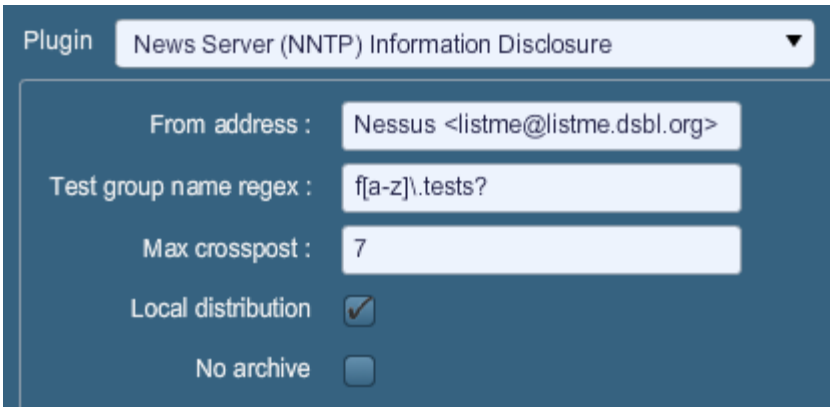
Категория **Login configurations** (конфигурации входа) позволяет сканеру Nessus использовать учетные данные при тестировании HTTP, NNTP, FTP, POP2, POP3 или IMAP. Предоставляя учетные данные, сканер Nessus, возможно, сможет выполнить более подробные проверки для выявления уязвимостей. Предоставляемые здесь учетные данные HTTP будут использоваться только для обычной или дайджест-проверки подлинности. Для конфигурации учетных данных пользовательского веб-приложения используйте раскрывающееся меню HTTP login page (страница входа HTTP).



Параметры **Modbus/TCP Coil Access** (доступ к дискретным выходам Modbus/TCP) доступны пользователям канала ProfessionalFeed. Этот элемент раскрывающегося меню генерируется динамически SCADA подключаемыми модулями, доступными пользователям канала ProfessionalFeed. Протокол Modbus использует код функции 1 для чтения дискретных выходов (coil) на сервере Modbus. Дискретные выходы представляют собой двоичные выходные настройки и обычно сопоставляются с приводами. Возможность читать дискретные выходы может помочь осуществляющему атаку лицу профилировать систему и определить диапазоны регистров для изменения с помощью сообщения write coil (запись дискретного выхода). Значениями по умолчанию являются 0 для Start reg (начальный регистр) и 16 для End reg (конечный регистр).

Параметры **Nessus SYN scanner** (сканер Nessus SYN) и **Nessus TCP scanner** (сканер Nessus TCP) позволяют лучше настроить собственные сканеры SYN и TCP для определения наличия брандмауэра.

Значение	Описание
Automatic (normal) (автоматически (нормальная настройка))	Этот параметр может помочь определить, расположен ли брандмауэр между сканером и проверяемым хостом (**по умолчанию**).
Disabled (softer) (отключить (облегченная настройка))	Отключает функцию **Firewall detection** (определение брандмауэра).
Do not detect RST rate limitation (soft) (не определять ограничение частоты сбросов (облегченная настройка))	Отключает возможность отслеживания частоты сбросов и определения того, установлено ли ограничение подчиненным устройством сети.
Ignore closed ports (aggressive) (игнорировать закрытые порты (агрессивная настройка))	Будет предпринята попытка выполнения подключаемых модулей, даже если порт выглядит закрытым. Этот параметр не рекомендуется использовать на производственных сетях.



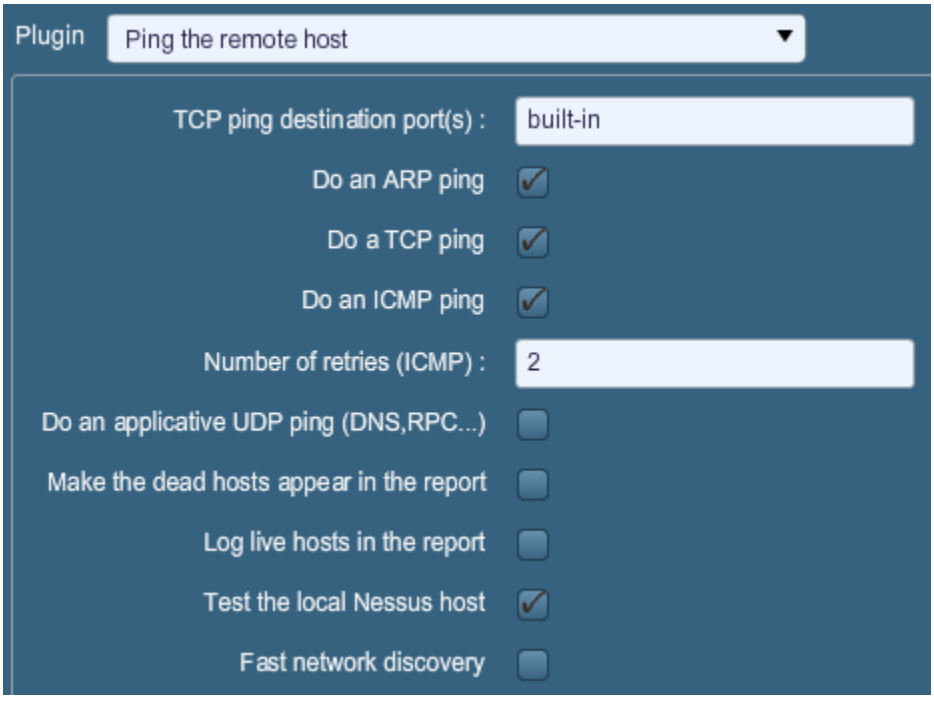
Категория **News Server (NNTP) Information Disclosure** (раскрытие информации сервера новостей (NNTP)) может использоваться для определения наличия серверов новостей, способных рассылать нежелательную почту (спам). Сканер Nessus выполнит попытку отправки сообщения новостей на серверы NNTP (Network News Transport Protocol) и может также протестировать наличие возможности отправки сообщений на вышестоящий сервер новостей.

Параметр	Описание
From address (адрес отправки)	Адрес, который сканер Nessus будет использовать для попыток отправки сообщения на серверы новостей. Это сообщение будет автоматически удалено после короткого промежутка времени.
Test group name regex (регулярное выражение имени тестовой группы)	Имя групп новостей, которые получат тестовое сообщение с указанного адреса. Имя может быть указано в виде регулярного выражения (regex), поэтому сообщение может быть отправлено в несколько групп новостей одновременно. Например, при использовании значения по умолчанию **f[a-z]\.tests?** почтовое сообщение будет отправлено во все группы новостей с именами, начинающимися с любой буквы (от «a» до «z») и заканчивающимися словом «.tests» (или какой-либо вариацией, соответствующей заданной строке). Знак вопроса действует как необязательный подстановочный знак.
Max crosspost (максимальная отправка)	Максимальное количество серверов новостей, которые получат тестовое сообщение, независимо от количества соответствующих запросу имен. Например, если установлено значение Max crosspost **7**, тестовое сообщение будет отправлено только на семь серверов новостей, даже если есть 2 000 серверов новостей, соответствующих указанному в поле регулярному выражению.
Local distribution (локальное распространение)	В случае установки этого флажка сканер Nessus будет пытаться отправить сообщение только на локальные серверы новостей. В противном случае будет выполнена

	попытка пересылки сообщения на вышестоящие серверы.
No archive (не архивировать)	В случае установки этого флажка сканер Nessus отправит запрос не архивировать тестовое сообщение, отправляемое на серверы новостей. В противном случае это сообщение будет архивироваться, как любое другое сообщение.

Категория **Oracle Settings** (настройки Oracle) позволяет настроить в сканере Nessus значение Oracle Database SID и включает параметр тестирования на наличие известных учетных записей по умолчанию в программном обеспечении Oracle.

Категория **PCI DSS Compliance** (соответствие PCI DSS) используется для сравнения сканером Nessus результатов сканирования с текущими стандартами PCI DSS. Эта функция доступна только для клиентов канала ProfessionalFeed.

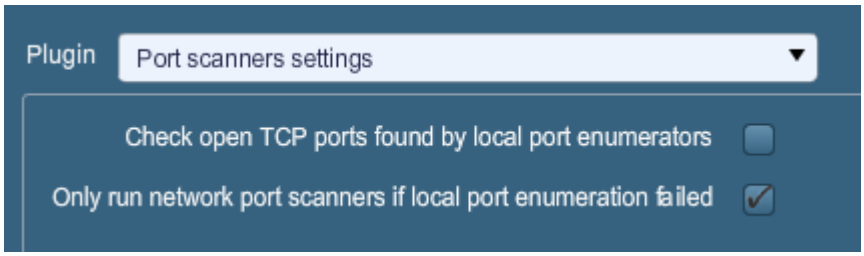


Параметры категории **Ping the remote host** (проверка связи с удаленным хостом) позволяют выполнять тонкую настройку возможностей сканера Nessus по проверке связи с хостами с помощью команды ping во время сканирования обнаружения. Это

может быть выполнено с помощью команд ARP ping, TCP ping, ICMP ping или прикладной команды UDP ping.

Параметр	Описание
TCP ping destination port(s) (проверяемые командой TCP ping порты)	Определяет список портов, которые будут проверены с помощью команды TCP ping. Если вы не уверены, какие порты указать, то оставьте значение по умолчанию built-in.
Number of Retries (ICMP)" (количество попыток (ICMP))	Позволяет указать количество попыток отправки команды ping удаленному хосту. По умолчанию установлено значение 6.
Do an applicative UDP ping (DNS, RPC...) (выполнить прикладную проверку UDP ping (DNS, RPC...))	Выполнить проверку UDP ping в отношении определенных UDP-приложений, включая DNS (порт 53), RPC (порт 111), NTP (порт 123) и RIP (порт 520).
Make the dead hosts appear in the report (показывать не отвечающие хосты в отчете)	При установке этого флажка хосты, которые не ответили на запрос ping, будут включены в отчет безопасности как не отвечающие хосты (dead hosts).
Log live hosts in the report (включать отвечающие хосты в отчет)	Установите этот флажок, чтобы включать в отчет возможность успешной проверки связи с удаленными хостами.
Test the local Nessus host (тестировать локальный хост Nessus)	Этот параметр позволяет включать или исключать локальный хост Nessus из сканирования. Это используется, когда хост Nessus входит в сканируемый диапазон номеров сети.
Fast network discovery (быстрое обнаружение сети)	По умолчанию, когда сканер Nessus выполняет проверку связи с удаленными IP-адресами с помощью команды ping и получает ответ, он выполняет дополнительные проверки, чтобы убедиться, что это не прозрачный proxy-сервер или служба балансировки нагрузки, которые возвращают шум, а не результат (некоторые устройства отвечают каждому порту 1-65535, но не представляют собой служб). Такие проверки могут занимать время, особенно если удаленный хост защищен брандмауэром. В случае включения параметра «fast network discovery» сканер Nessus не будет выполнять эти проверки.

Для сканирования гостевых систем VMware команда ping должна быть отключена. В политике сканирования в разделе Advanced -> Ping the remote host (дополнительно -> проверка связи с удаленным хостом) снимите флажки TCP, ICMP и ARP ping.



Категория **Port scanner settings** (настройки сканера портов) содержит два параметра для дополнительного управления сканированием портов.

Параметр	Описание
Check open TCP ports found by local port enumerators (проверять открытые порты TCP, найденные локальным перечислителем портов)	Если локальный перечислитель портов (например, WMI или netstat) находит порт, Nessus также проверяет удаленно, открыт ли он. Это помогает определить, используется ли какая-либо форма управления доступом (например, TCP оболочки, брандмауэр).
Only run network port scanners if local port enumeration failed (запускать сетевые сканеры портов только в случае сбоя локального перечисления портов)	В противном случае следует полагаться в первую очередь на локальное перечисление портов.

Параметр **SMB Registry: Start the Registry Service during the scan** (реестр SMB: запускать службу реестра во время сканирования) включает службу, обеспечивающую выполнение некоторых требований сканирования для машин, у которых может быть постоянно не запущен реестр SMB.

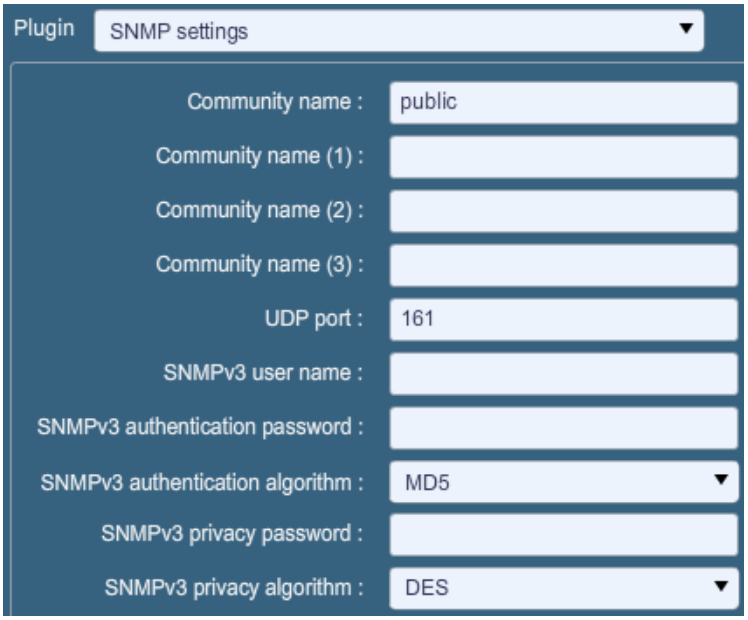
Если в меню **SMB Scope** (область SMB) включен параметр **Request information about the domain** (запрашивать информацию о домене), то запросы будут направляться пользователям домена вместо локальных пользователей.

Параметр **SMB Use Domain SID to Enumerate Users** (SMB использует SID домена для перечисления пользователей) определяет диапазон SID, используемый для выполнения обратного просмотра имен пользователей домена. Для большинства случаев сканирования рекомендуется использовать значение по умолчанию.

Параметр **SMB Use Host SID to Enumerate Users** (SMB использует SID хоста для перечисления пользователей) определяет диапазон SID, используемый для выполнения обратного просмотра локальных имен пользователей. Рекомендуется использовать значение по умолчанию.

В категории **SMTP settings** (настройки SMTP) определяются параметры тестов протокола SMTP, выполняемых на всех устройствах в пределах сканируемого домена, на которых запущены службы SMTP. Сканер Nessus выполнит попытку передачи сообщений через устройство в указанный домен **Third party domain** (сторонний домен). В случае отклонения сообщения, отправленного в домен **Third party domain** (сторонний домен), адресом, указанным в поле **To address** (адрес получателя), попытка рассылки нежелательной почты (спама) не удалась. В случае приема сообщения сервер SMTP был успешно использован для отправки нежелательной почты.

Параметр	Описание
Third party domain (сторонний домен)	Сканер Nessus выполнит попытку отправки нежелательной почты через каждое устройство SMTP на адрес, указанный в этом поле. Этот адрес стороннего домена должен находиться вне диапазона адресов сканируемого узла и сканирующего узла. В противном случае тест может быть отменен SMTP-сервером.
From address (адрес отправки)	Тестовые сообщения, отправленные SMTP-серверам, будут выглядеть, как если бы они были отправлены с указанного в этом поле адреса.
To address (адрес получателя)	Сканер Nessus выполнит попытку отправки сообщений, адресованных получателю электронной почты, указанному в этом поле. Адрес **postmaster** является значением по умолчанию, потому что это обычно действительный адрес на большинстве почтовых серверов.



Категория **SNMP settings** (настройки SNMP) позволяет выполнить конфигурацию сервера Nessus для установления связи со службой SNMP сканируемого хоста и прохождения проверки подлинности. В процессе сканирования Nessus выполнит некоторые попытки подобрать строку сообщества и использовать ее для последующих тестов. Поддерживается до четырех отдельных строк имен сообществ на одну политику сканирования. Если сканеру Nessus не удастся подобрать строку сообщества и/или пароль, ему, возможно, не удастся выполнить полный аудит службы.

Параметр	Описание
Community name (0-3) (имя сообщества (0-3))	Имя сообщества SNMP.
UDP port (UDP-порт)	Указывает сканеру Nessus выполнить сканирование другого порта, если служба SNMP выполняется не на порту 161.
SNMPv3 user name (имя пользователя SNMPv3)	Имя пользователя для учетной записи на базе SNMPv3.
SNMPv3 authentication password (пароль проверки подлинности SNMPv3)	Пароль, соответствующий указанному имени пользователя.
SNMPv3 authentication algorithm (алгоритм проверки подлинности SNMPv3)	Выберите MD5 или SHA1, в зависимости от того, какой алгоритм поддерживает удаленная служба.
SNMPv3 privacy password (пароль	Пароль, используемый для защиты зашифрованного обмена данными SNMP.

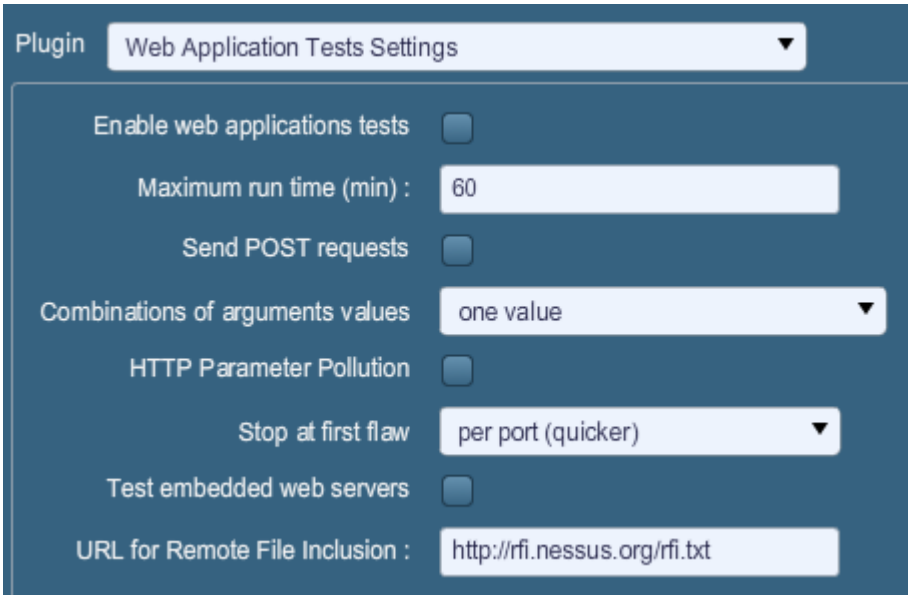
конфиденциальности SNMPv3)	
SNMPv3 privacy algorithm (алгоритм конфиденциальности SNMPv3)	Алгоритм шифрования, используемый для передачи данных SNMP.

Параметр **Service Detection** (обнаружение служб) определяет то, как сканер Nessus будет тестировать службы на базе SSL: известные порты SSL (например, 443), все порты или никаких портов. Тестирование возможности использования SSL на всех портах может нарушить работу тестируемого хоста.

Параметр **Wake-on-LAN** (пробуждение по сети) определяет, каким хостам должны отправляться пакеты WOL до выполнения сканирования и сколько времени необходимо ждать (в минутах) загрузки системы. Список MAC-адресов для отправки пакетов WOL вводится с помощью загружаемого на сервер текстового файла, в котором в каждой строке указывается один MAC-адрес хоста. Например:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```

Категория **Unix Compliance Checks** (проверки соответствия Unix) позволяет клиентам канала ProfessionalFeed отправлять на сервер файлы аудита Unix, которые будут использоваться для определения того, отвечает ли проверяемая система определенным стандартам. Допускается одновременный выбор до пяти политик.



Категория **Web Application Tests Settings** (настройки тестов веб-приложений) содержит настройки тестирования аргументов удаленных интерфейсов CGI (Common Gateway Interface), обнаруженных в процессе веб-отображения, путем попытки передачи распространенных ошибок программирования CGI, например межсайтовых скриптов, включения удаленных файлов, выполнения команд, обходных атак и

внедрения кода SQL. Это тестирование включается флажком Enable web applications tests (включить тесты веб-приложений). Эти тесты зависят от следующих подключаемых модулей NASL.

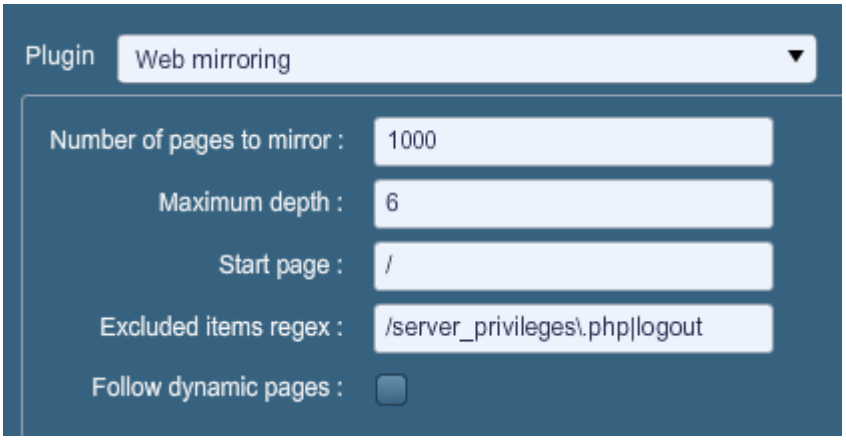
- 11139, 42424, 42479, 42426, 42427, 43160 – внедрение кода SQL (нарушения CGI)
- 39465, 44967 – выполнение команд (нарушения CGI)
- 39466, 47831, 42425, 46193, 49067 – межсайтовые скрипты (нарушения CGI: XSS)
- 39467, 46195, 46194 – обход каталога (нарушения CGI)
- 39468 – внедрение заголовка HTTP (нарушения CGI: XSS)
- 39469, 42056, 42872 – включение файла (нарушения CGI)
- 42055 – строка формата (нарушения CGI)
- 42423, 42054 – включения на стороне сервера (нарушения CGI)
- 44136 – манипуляция файлами cookie (нарушения CGI)
- 46196 – внедрение XML (нарушения CGI)
- 40406, 48926, 48927 – сообщения об ошибках
- 47830, 47832, 47834, 44134 – дополнительные атаки (нарушения CGI)

Примечание. Этот список связанных с веб-приложениями подключаемых модулей часто обновляется. Дополнительные подключаемые модули могут зависеть от настроек следующих параметров.

Параметр	Описание
Maximum run time (min) (максимальное время выполнения (мин))	Этот параметр управляет длительностью (в минутах) выполнения тестов веб-приложений. По умолчанию этот параметр имеет значение 60 минут и применяется ко всем портам и интерфейсам CGI для соответствующего веб-сайта. Сканирование локальной сети для проверки веб-сайтов с небольшими приложениями обычно завершается менее чем за час, однако для веб-сайтов с большими приложениями может потребоваться большее значение.
Send POST requests (отправлять запросы POST)	Запросы POST используются для расширенного тестирования веб-форм. По умолчанию тесты веб-приложений используют только запросы GET, если не включен этот параметр. В общем случае, более сложные приложения используют метод POST, когда пользователь отправляет данные приложению. Эта настройка обеспечивает более тщательное тестирование, но может значительно увеличивать требуемое время. При установке этого флажка сканер Nessus будет тестировать каждый скрипт/переменную обоими запросами, GET и POST.
Combinations of arguments values (комбинации значений аргументов)	Этот параметр управляет комбинацией значений аргументов, используемых в запросах HTTP. В этом раскрывающемся меню есть три параметра: **one value** (одно значение) — при этой настройке выполняется тестирование одного параметра строкой

	атаки, без испытания вариаций «без атаки» для дополнительных параметров. Например, сканер Nessus испытает строку `/test.php?arg1=XSS&b=1&c=1`, где b и c допускают другие значения, не тестируя каждую комбинацию. Это самый быстрый метод тестирования с минимальным генерируемым набором результатов. **All pairs (slower but efficient)** (все пары (медленнее, но эффективнее)) — эта форма тестирования немного медленнее, но более эффективна, чем тест one value. При тестировании нескольких параметров будет протестирована строка атаки, вариации для одной переменной, а затем будет использовано первое значение для всех других переменных. Например, сканер Nessus испытает строку `/test.php?a=XSS&b=1&c=1&d=1`, а затем переберет переменные, чтобы одной присвоить строку атаки, для одной перебрать все возможные значения (обнаруженные в процессе отображения), а любым другим переменным присвоить первое значение. В этом случае сканер Nessus никогда не протестирует `/test.php?a=XSS&b=3&c=3&d=3`, если первое значение каждой переменной будет 1. **All combinations (extremely slow)** (все комбинации (очень медленно)) — этот метод тестирования выполнит исчерпывающее тестирование всех возможных комбинаций строк атаки с допустимыми входными значениями переменных. Если при тестировании с настройкой All-pairs (все пары) создается меньший набор данных для повышения скорости, то с настройкой all combinations (все комбинации) не принимается никаких компромиссов для экономии времени и используется полный набор данных тестирования. Это метод тестирования может занять **длительное** время.
HTTP Parameter Pollution (засорение параметров HTTP)	Во время выполнения тестирования веб-приложений делается попытка обойти любые механизмы фильтрации путем внедрения содержимого в переменную, передавая при этом ту же переменную с действительным содержимым. Например, нормальный тест на внедрение SQL может выглядеть следующим образом: `/target.cgi?a='&b=2`. При включенной настройке HTTP Parameter Pollution (HPP) запрос может выглядеть так: `/target.cgi?a='&a=1&b=2`.
Stop at first flaw (остановиться на первом недостатке)	Этот параметр определяет, когда обнаруживается новый недостаток. Это касается уровня скриптов; обнаружение недостатка XSS не прекращает поиск внедрения SQL или внедрения заголовков, но вы получаете не более одного отчета каждого типа по каждому порту, если не включена настройка thorough tests (подробные тесты). Обратите внимание, что иногда в отчет может включаться несколько

	недостатков одинакового типа (например, XSS, SQLi и т. д.), если они были обнаружены одной атакой. В этом раскрывающемся меню есть четыре параметра: **per CGI** (на CGI) – если скриптом будет обнаружен какой-либо недостаток интерфейса CGI, сканер Nessus переключается на следующий известный интерфейс CGI того же сервера или (если других интерфейсов CGI нет) на следующий порт/сервер. Это значение по умолчанию. **per port (quicker)** **(на порт (быстрее))** – если скриптом будет обнаружен какой-либо недостаток на веб-сервере, сканер Nessus остановится и переключится на другой веб-сервер на другом порту. **per parameter (slow)** **(на параметр (медленно))** – если обнаруживается один тип недостатка в каком-либо параметре CGI (например, XSS), сканер Nessus переключается на следующий параметр того же интерфейса CGI или на следующий порт/сервер. **look for all flaws (slower)** **(искать все недостатки (медленнее))** – выполняет расширенные тесты, независимо от обнаруженных недостатков. При использовании этого параметра могут получаться очень объемные отчеты, поэтому в большинстве случаев он не рекомендуется.
Test Embedded web servers (тестировать внедренные веб-серверы)	Внедренные веб-серверы часто бывают статическими и не содержат настраиваемых скриптов CGI. Кроме того, внедренные веб-серверы могут быть подвержены сбоям или переставать отвечать при сканировании. Компания Tenable рекомендует выполнять сканирование внедренных веб-серверов отдельно от остальных веб-серверов с помощью этого параметра.
URL for Remote File Inclusion (URL для включения удаленных файлов)	При тестировании включения удаленных файлов (Remote File Inclusion, RFI) этот параметр указывает файл на удаленном хосте, который должен использоваться для тестирования. По умолчанию сканер Nessus использует надежный файл, размещенный на веб-сервере компании Tenable для тестирования RFI. Если сканер не может связаться с Интернетом, для более точных результатов тестирования RFI рекомендуется использовать файл, размещенный на внутреннем хосте.



В категории **Web Mirroring** (веб-отображение) настраиваются параметры конфигурации для собственной служебной программы зеркального отображения содержимого веб-серверов Nessus. Сканер Nessus выполняет зеркальное отображение веб-содержимого для более оптимального анализа содержимого в плане уязвимости и помогает свести к минимуму влияние на сервер.

Если параметры зеркального веб-отображения настроены таким образом, чтобы отображался весь веб-сайт, это может приводить к значительным объемам трафика при сканировании. Например, если на веб-сервере размещен 1 гигабайт материалов, а сканер Nessus настроен на полное отображение содержимого, то при сканировании генерируется не менее 1 гигабайта трафика от сервера к сканеру Nessus.

Параметр	Описание
Number of pages to mirror (количество отображаемых страниц)	Максимальное количество отображаемых страниц.
Maximum depth (максимальная глубина)	Предельное количество ссылок, которые будет проверять сканер Nessus для каждой начальной страницы.
Start page (начальная страница)	URL-адрес первой страницы, которая будет протестирована. Если необходимо указать несколько страниц, следует использовать для их разделения двоеточие (например, «/:/php4:/base»).
Excluded items regex (регулярное выражение исключенных элементов)	Применяет исключение частей веб-сайта из обхода. Например, для исключения каталога «/manual» и всех интерфейсов Perl CGI введите в это поле: **(^/ manual) | (\ . pl (\ ?. *) ?$) .**
Follow dynamic pages (переходить на динамические страницы)	При установке этого флажка сканер Nessus будет переходить по динамическим ссылкам и может превысить рассмотренные выше параметры.

Категория **Windows Compliance Checks** (проверки соответствия Windows) позволяет клиентам канала ProfessionalFeed отправлять на сервер файлы конфигурации аудита Microsoft Windows, которые будут использоваться для определения того, отвечает ли проверяемая система определенным стандартам. Допускается одновременный выбор до пяти политик.

Категория **Windows File Contents Compliance Checks** (проверки соответствия файлов содержимого Windows) позволяет клиентам канала ProfessionalFeed отправлять на сервер файлы аудита Windows, которые выполняют поиск определенного типа содержимого в системе (например, кредитных карт, номеров Social Security (социального страхования)) для определения соответствия корпоративным нормам или сторонним стандартам.

После выполнения необходимой конфигурации всех параметров нажмите кнопку **Submit** (отправить) для сохранения политики и возврата на вкладку Policies (политики). В любое время можно нажать кнопку **Edit** (правка) для внесения изменений в уже созданную политику или нажать кнопку **Delete** (удалить) для полного удаления политики.

Импорт, экспорт и копирование политик

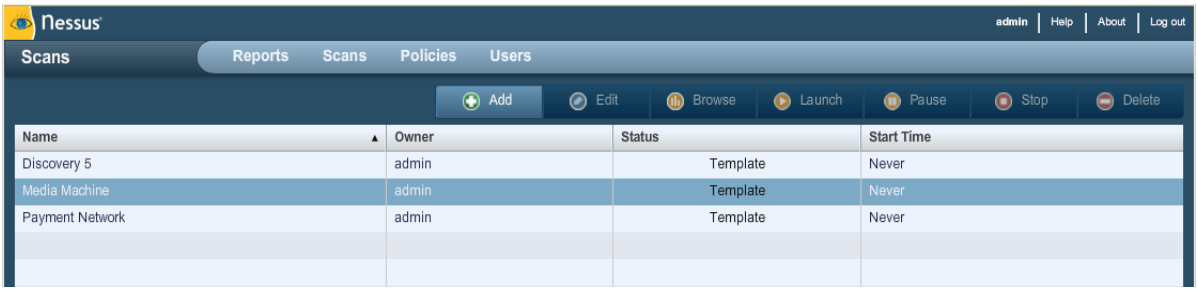
Кнопка **Import** (импорт) на верхней правой панели меню позволяет отправлять ранее созданные политики на сканер. С помощью диалогового окна **Browse...** (обзор...) выберите политику в своей локальной системе и нажмите кнопку **Submit** (отправить).

Кнопка **Export** (экспорт) на панели меню позволяет загружать существующие политики из сканера в локальную файловую систему. Диалоговое окно загрузки в браузере позволяет открыть политику во внешней программе (например, в текстовом редакторе) или сохранить политику в выбранный каталог.

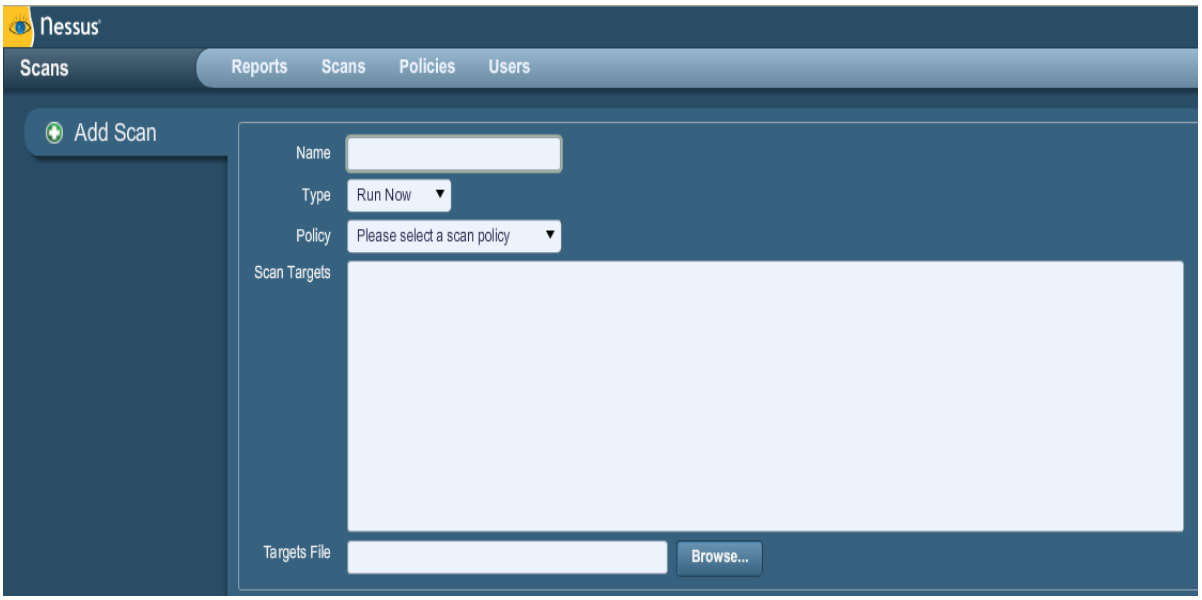
Содержащиеся в политике пароли и файлы `.audit` **не** будут экспортированы.

При необходимости создания политики, аналогичной существующей с минимальными изменениями, можно выбрать базовую политику в списке и нажать кнопку **Copy** (копировать) на верхней правой панели меню. При этом будет создана копия исходной политики, в которую можно внести все необходимые изменения. Это полезно для создания стандартных политик с небольшими изменениями, необходимыми для соответствующей среды.

Создание, запуск и планирование сканирований



После создания политики можно создать новое сканирование, нажав кнопку **Scans** (сканирования) на панели меню в верхней части окна, а затем кнопку **+ Add** (+ добавить), расположенную справа. Откроется следующее диалоговое окно **Add Scan** (добавление сканирования):



Для определения цели сканирования есть пять полей:

- **Name** (имя) — позволяет ввести имя, которое будет отображаться в интерфейсе пользователя Nessus для определения сканирования.
- **Type** (тип) — выберите Run Now (выполнить сейчас) (немедленное выполнение сканирования после отправки), Scheduled (запланированное) (выбрать время начала сканирования) или Template (шаблон) (сохранить как шаблон для повторного сканирования).
- **Policy** (политика) — выберите ранее созданную политику, которая будет использоваться сканированием для настройки параметров поведения сервера Nessus при сканировании.
- **Scan Targets** (цели сканирования) — целевые машины можно указать с помощью отдельных IP-адресов (например, 192.168.0.1), диапазонов IP-адресов (например, 192.168.0.1-192.168.0.255), подсети с обозначением CIDR (например, 192.168.0.0/24) или разрешаемого имени хоста (например, www.nessus.org).
- **Targets File** (файл целей) — текстовый файл со списком хостов можно импортировать, нажав кнопку **Browse...** (обзор) и выбрав файл с локальной машины.

Файл хостов должен быть в текстовом формате ASCII, в каждой строке указывается один хост без дополнительных пробелов или строк. Кодировки Unicode/UTF-8 не поддерживаются.

Примеры формата файла хостов:

Отдельные хосты:

192.168.0.100
192.168.0.101
192.168.0.102

Диапазон хостов:

192.168.0.100-192.168.0.102

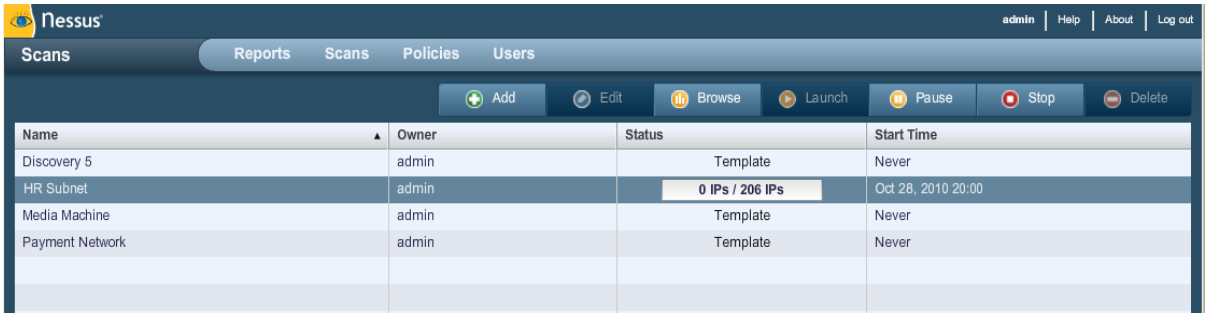
Блок хостов CIDR:

192.168.0.1/24

Виртуальные серверы:

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

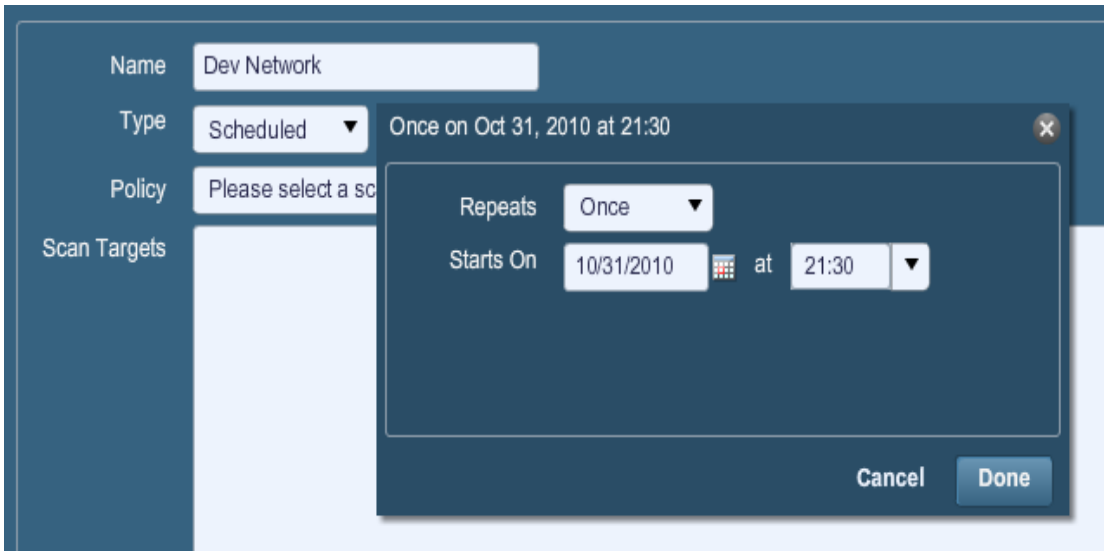
После ввода информации сканирования нажмите кнопку **Submit** (отправить). После отправки сканирование начнется немедленно (если выбрана настойка Run Now) до возврата на основную страницу **Scans** (сканирования).



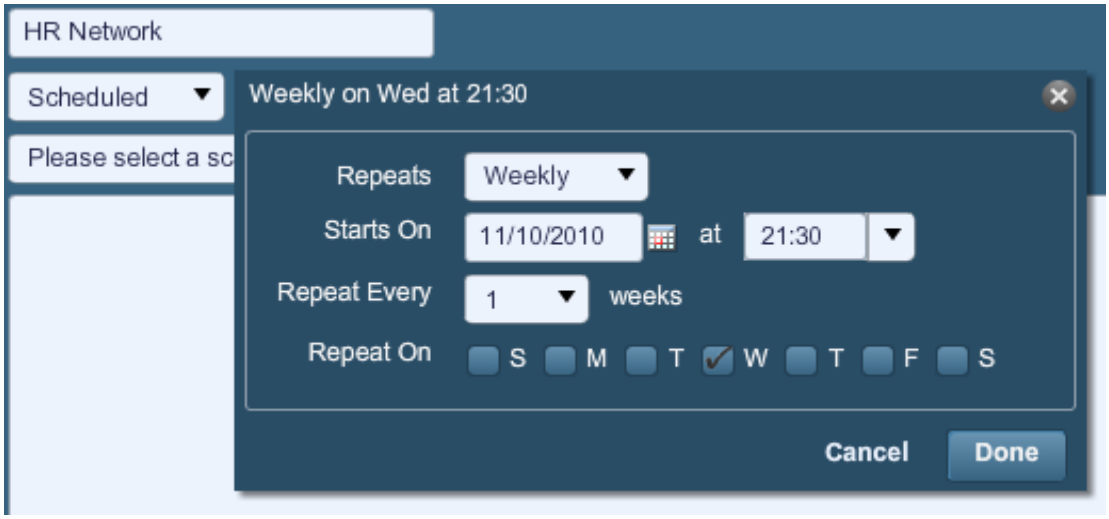
После запуска сканирования в списке Scans (сканирования) будут отображаться все текущие выполняемые, приостановленные или сохраненные в виде шаблонов сканирования, а также базовая информация о каждом сканировании. После выбора определенного сканирования из списка кнопки действий в верхней правой части окна позволяют выполнять следующие действия: **Browse** (обзор) результатов сканирования в процессе выполнения, **Pause** (пауза) и **Resume** (возобновление) сканирования, **Stop** (остановка) и **Delete** (удаление) сканирования полностью. Пользователь также может применять функцию **Edit** (правка) к шаблонам сканирований.

Когда сканирование завершается (по любой причине), оно удаляется из списка **Scans** (сканирования) и становится доступным на вкладке **Reports** (отчеты) для рассмотрения результатов.

При выборе типа сканирования Scheduled (запланированное) появится параметр установки необходимого времени начала и частоты сканирования:

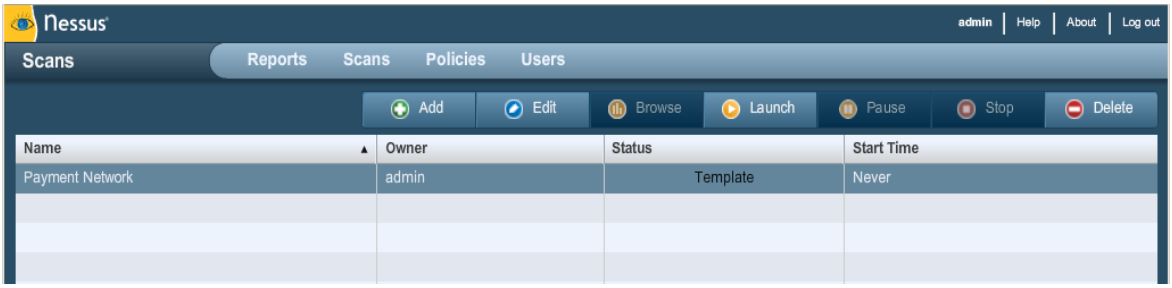


С помощью раскрывающегося меню Repeats (повторы) можно запланировать однократное, ежедневное, еженедельное, ежемесячное или ежегодное выполнение сканирования. Затем этот выбор можно уточнить, указав начало сканирования в определенный день и время. После сохранения сканирования Nessus запустит выполнение сканирования в указанное время.



Сканирования запускаются по времени, установленному на сервере сканера Nessus.

Если сканирование сохраняется в виде шаблона, оно появляется в списке сканирований с соответствующим обозначением и ожидает запуска.



Запланированные сканирования доступны только для клиентов канала ProfessionalFeed.

Отчеты

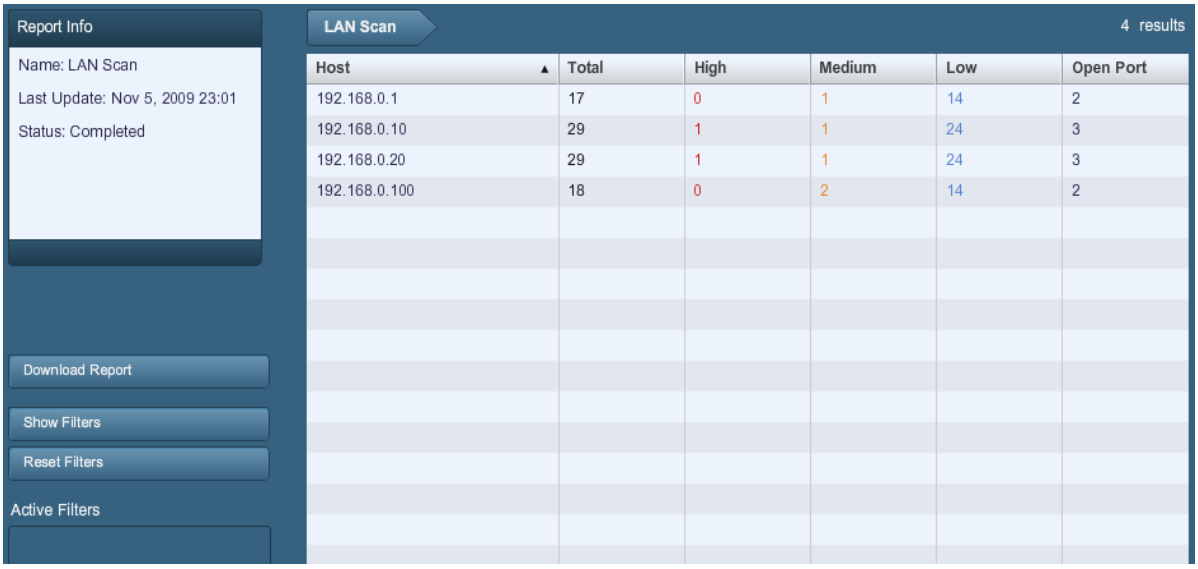
Начиная с выпуска Nessus 4.2 таблицы стилей отчетов стали лучше интегрированы в систему отчетности. С помощью фильтров отчетов и функций экспорта пользователи могут создавать собственные динамические отчеты, а не только выбирать из определенного списка. Кроме того, была расширена поддержка таблиц стилей, которая теперь позволяет выполнять обновления или добавление таблиц стилей через канал подключаемых модулей. Это позволит компании Tenable выпускать дополнительные таблицы стилей, не требуя установки обновления или основного выпуска.

При выборе вкладки **Reports** (отчеты) на панели меню в верхней части интерфейса откроется список выполняемых и завершенных сканирований:

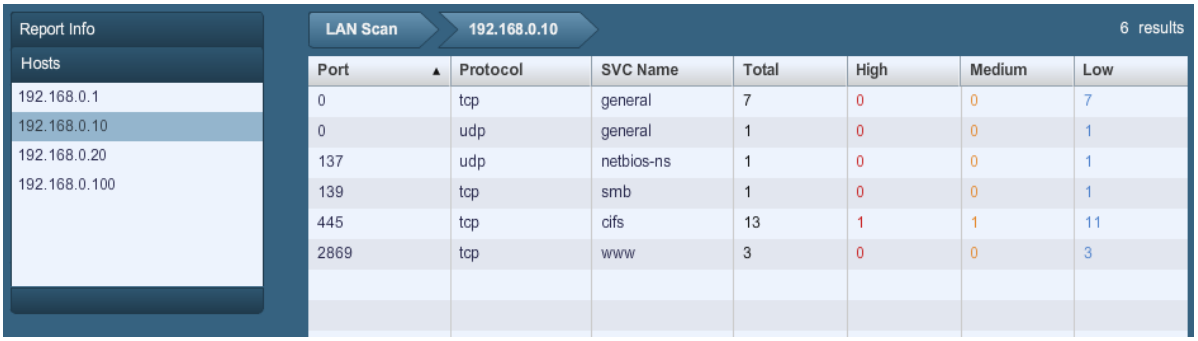
Экран Reports (отчеты) действует как исходная точка для просмотра, сравнения, отправки и загрузки результатов сканирования. Для выбора одновременно нескольких отчетов используйте клавишу Shift или Ctrl.

Обзор

Для просмотра результатов сканирования выберите имя сканирования в списке Reports (отчеты) и нажмите кнопку **Browse** (обзор). Это позволяет просмотреть результаты, выбирая хосты, порты и определенные уязвимости. На первом обзорном экране отображается каждый просканированный хост с данными о количестве уязвимостей и открытых портов:



При выборе хоста отчет классифицируется по номерам портов и отображает связанную с каждым портом информацию, такую как протокол и имя службы, а также сводка уязвимостей, классифицированная по серьезности риска. При навигации по результатам сканирования интерфейс пользователя будет сохранять список хостов, а также последовательности стрелок, доступных для щелчка мышью, которые помогают быстро переходить к определенным компонентам отчета:



При выборе порта отображаются все найденные уязвимости, связанные с соответствующим портом и службой:


LAN Scan › 192.168.0.10 › 445 / tcp — List | Detail — 13 results

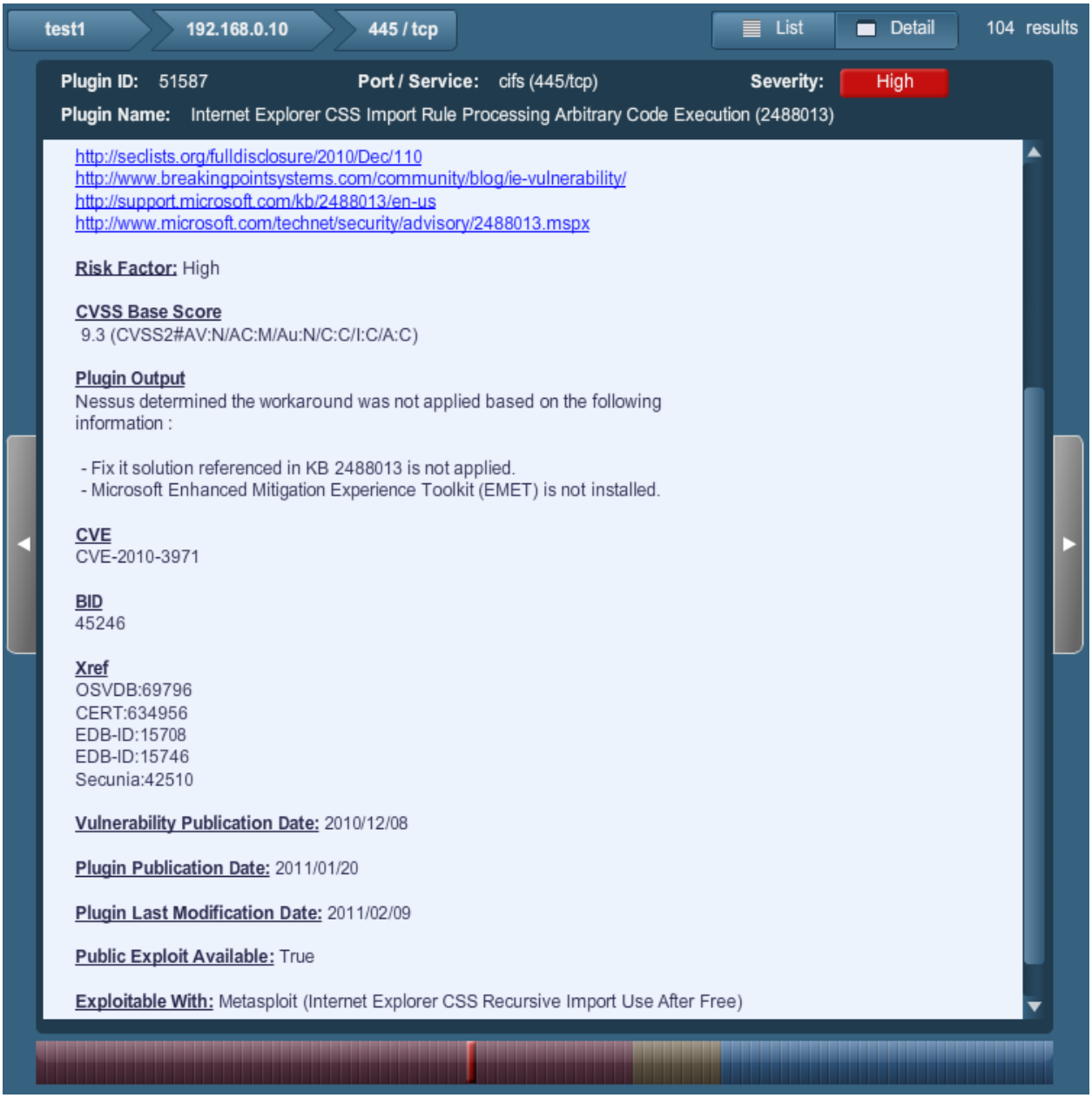
Plugin ID	Name	Port	Severity
11011	SMB Detection	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

В приведенном выше примере мы видим, что хост 192.168.0.10 насчитывает 13 уязвимостей, связанных с портом TCP 445 (CIFS или Common Internet File System). В сводке результатов отображается идентификатор подключаемого модуля Nessus, имя уязвимости, порт, протокол и уровень серьезности. При однократном щелчке по заголовку любого столбца результаты сортируются по содержимому соответствующего столбца. При втором щелчке порядок сортировки результатов меняется на противоположный:


LAN Scan › 192.168.0.10 › 445 / tcp — List | Detail — 13 results

Plugin ID	Name	Port	Severity ▾
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
11011	SMB Detection	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

При выборе уязвимости из списка отображаются полные сведения о найденной уязвимости, включая сводку, техническое описание, решение, фактор риска, балл CVSS, соответствующие выходные данные, демонстрирующие сделанный вывод, внешние ссылки, дату публикации уязвимости, дату публикации/изменения подключаемого модуля и наличие эксплойта:



В разделе наличия эксплойта отображаются все известные открытые эксплойты для соответствующей уязвимости, включая найденные в платформах уязвимостей (открытых или коммерческих), например CANVAS, CORE или Metasploit.

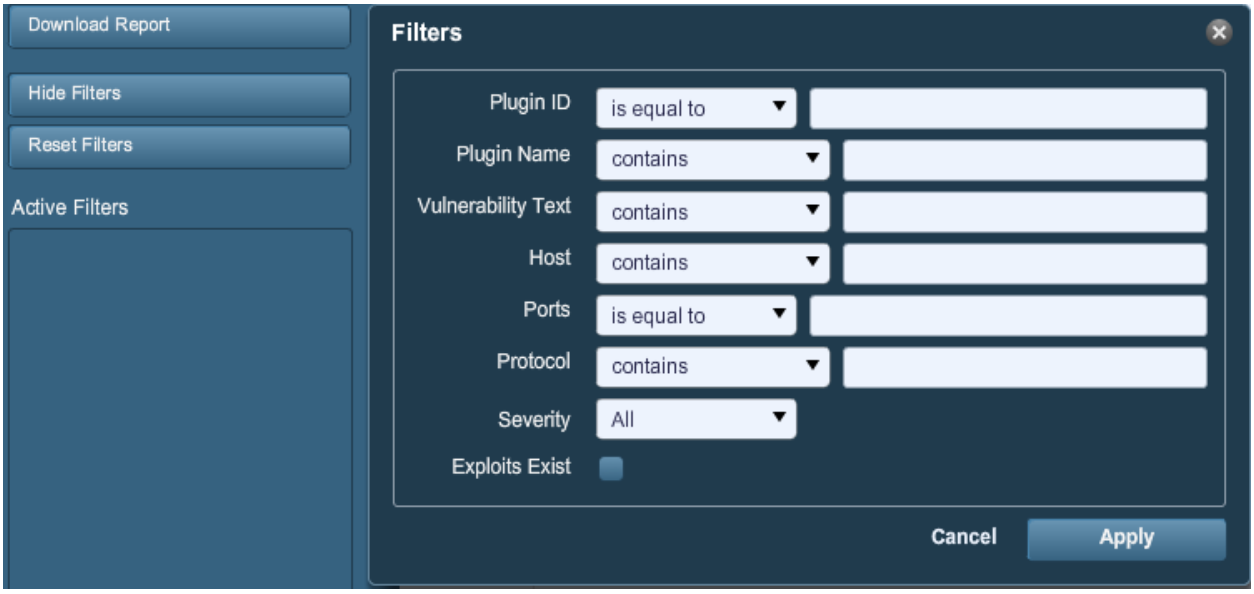
На экране сведений об уязвимости есть несколько методов навигации по отчету:

- Стрелки в верхней части экрана позволяют переходить назад к порту, хосту или обзору сканирования.
- Кнопки **List** (список) и **Detail** (сведения) позволяют переключаться между сведениями об уязвимости и последним списком (в рассмотренном выше примере — списком уязвимостей, связанных с портом 445).
- Серые стрелки слева и справа позволяют переключаться между уязвимостями, связанными с выбранным портом.
- Панель кнопок в нижней части экрана позволяет переходить к определенной уязвимости в списке с учетом серьезности риска. В приведенном выше примере выделяются уязвимости со средней и высокой серьезностью риска.

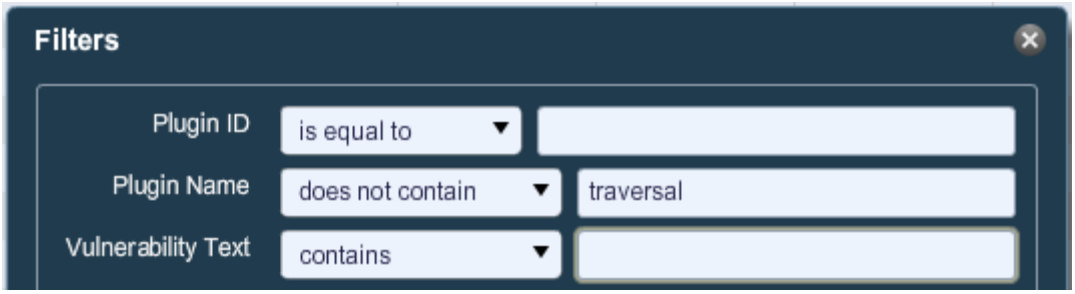
Фильтры отчетов

Сканер Nessus предлагает гибкую систему фильтров, помогающих отображать определенные результаты отчетов. Фильтры могут использоваться для отображения результатов на основании любого аспекта найденных уязвимостей. С помощью нескольких фильтров можно создавать более подробные и индивидуально настроенные представления отчетов.

Для создания фильтра сначала нажмите кнопку **Show Filters** (показать фильтры) в левой части экрана. Фильтры могут создаваться с экранов обзора отчетов, хостов или классификации портов.



Фильтр создается путем выбора поля, аргумента фильтра и значения, по которому будет выполняться фильтрация:



Фильтры отчетов предоставляют широкий выбор критериев:

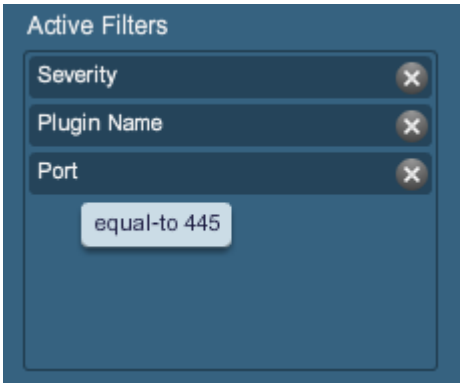
Параметр	Описание
Plugin ID (идентификатор подключаемого модуля)	Фильтрация результатов, если идентификатор подключаемого модуля равен (*is equal to*) или не равен (*is not equal to*) определенному числу (например, 42111).
Plugin Name (имя подключаемого модуля)	Фильтрация результатов, если имя подключаемого модуля содержит (*contains*), не содержит (*does not contain*), начинается с (*starts with*) или не начинается с (*does not start with*) определенной строки (например, Microsoft Windows).
Vulnerability Text (текст уязвимости)	Фильтрация результатов, если выходные данные подключаемого модуля содержат (*contains*), не содержат (*does not contain*), начинаются с (*starts with*) или не начинаются с (*does not start with*) определенной строки (например, denial of service (отказ в обслуживании)).
Host (хост)	Фильтрация результатов, если обозначение хоста содержит (*contains*), не содержит (*does not contain*), начинается с (*starts with*), не начинается с (*does not start with*), равно (*is equal to*) или не равно (*is not equal to*) определенной строке (например, 192.168).
Ports (порты)	Фильтрация результатов на основании того, равен номер порта (*is equal to*) или не равен (*is not equal to*) заданному числу (например, 443).
Protocol (протокол)	Фильтрация результатов, если название протокола содержит (*contains*), не содержит (*does not contain*), начинается с (*starts with*) или не начинается с (*does not start with*) определенной строки (например, http).
Severity (серьезность)	Фильтрация результатов на основании серьезности риска: низкая (*Low*), средняя (*Medium*), высокая (*High*) или критическая (*Critical*). Уровни серьезности определяются по соответствующему баллу CVSS, где балл меньше 5 соответствует уровню Low (низкий),

	меньше 7 — Medium (средний), меньше 10 — High (высокий), а балл CVSS, равный 10, обозначается как Critical (критический).
Exploits Exist (существуют эксплойты)	Фильтрация результатов на основании наличия известного открытого эксплойта.

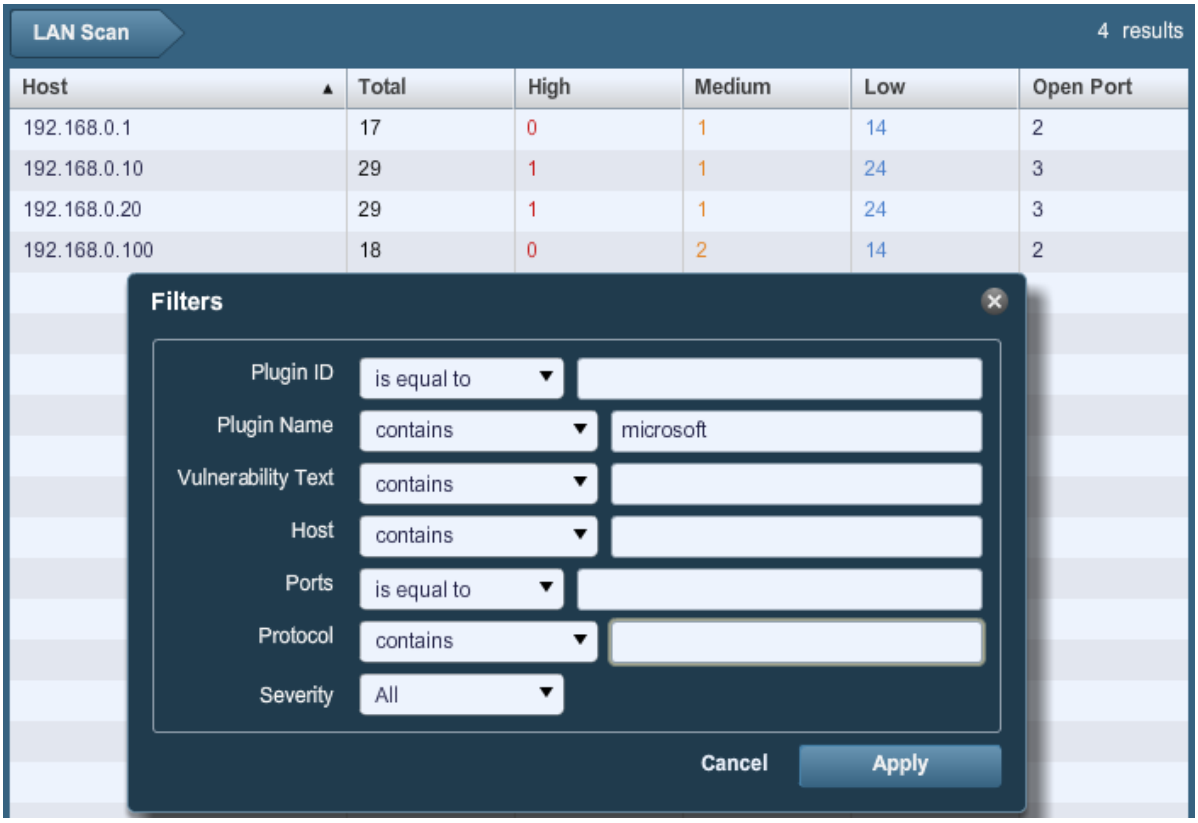
При использовании фильтра строки или числовые значения могут быть разделены запятыми для фильтрации по нескольким строкам. Например, для фильтрации результатов с целью отображения только веб-серверов можно создать фильтр Ports, выбрать аргумент is equal to (равен) и ввести строку 80,443,8000,8080. При этом будут показаны результаты, связанные с этими четырьмя портами.

В критериях фильтров **не** учитывается регистр.

При создании фильтров их список отображается слева. Для просмотра сведений об активном фильтре наведите указатель мыши на имя соответствующего фильтра:



После создания фильтра результаты сканирования будут обновляться с учетом критериев нового фильтра. В приведенном ниже примере создание фильтра, отображающего только результаты с текстом Microsoft в имени подключаемого модуля, большинство результатов скрывается:



После применения фильтра:

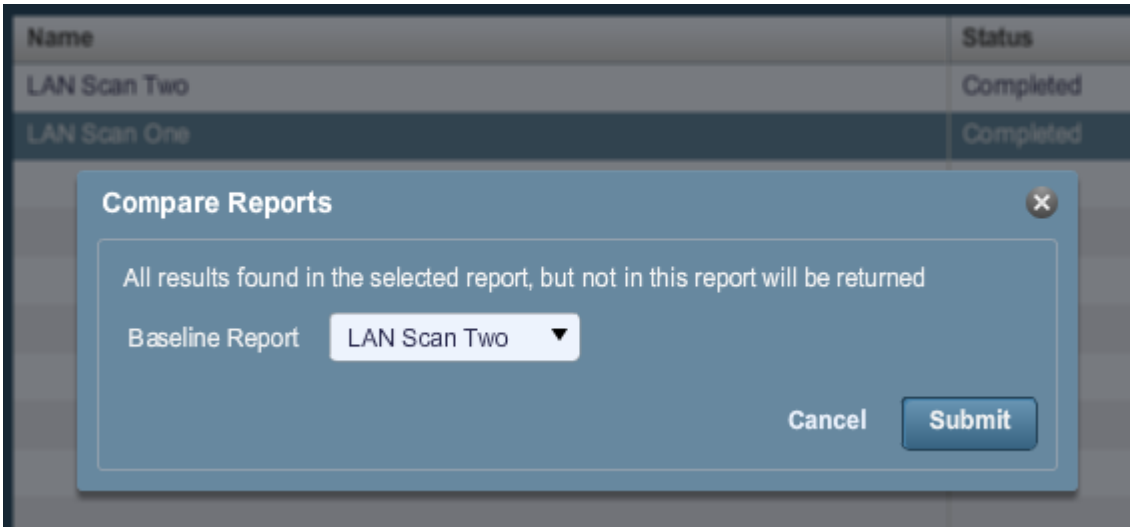
После фильтрации результатов для получения только необходимых данных можно нажать кнопку **Download Report** (загрузить отчет) для экспорта только отфильтрованных результатов.

Сравнение

Функция Compare (сравнение) доступна только пользователям канала ProfessionalFeed.

С помощью Nessus 4.4 можно сравнивать два отчета сканирования друг с другом для выявления различий. Возможность отображения различий в результатах сканирования помогает выявлять изменения в системе или сети с течением времени. Это помогает при анализе соответствия стандартам, показывая, сколько уязвимостей было устранено, если к системам применяются исправления по мере выявления новых уязвимостей, или как два сканирования могут быть направлены на разные хосты.

Для сравнения отчетов сначала выберите сканирование из списка **Reports** (отчеты) и нажмите кнопку **Compare** (сравнить) на панели меню справа. В открывшемся диалоговом окне будет раскрывающийся список других отчетов для сравнения. Выберите один отчет и нажмите кнопку **Submit** (отправить):

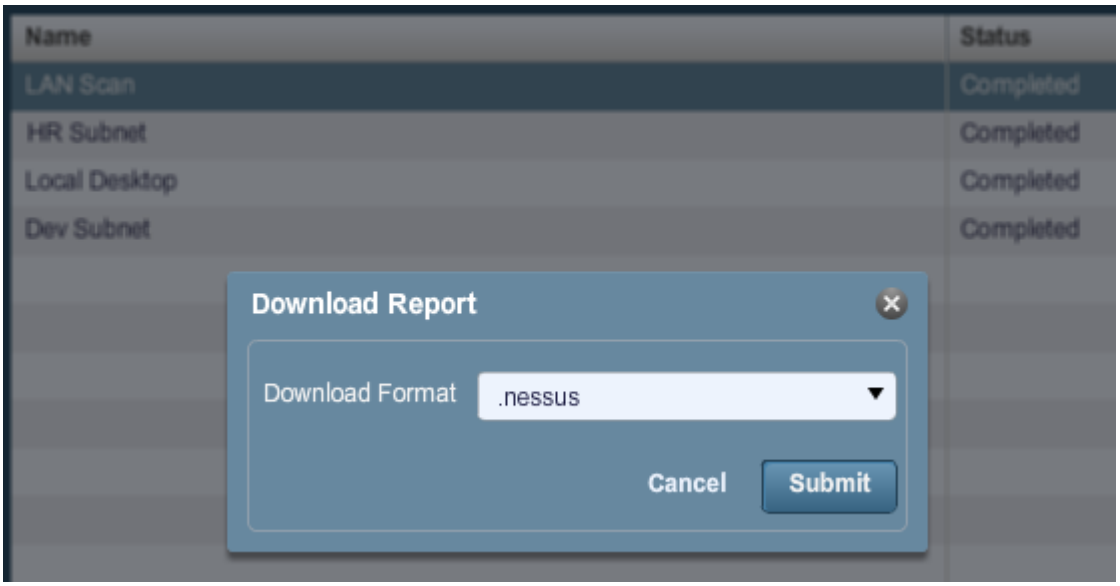


Сканер Nessus сравнит два отчета и выдаст список результатов, не найденных в обоих отчетах. Эти результаты представляют собой отличия сканирований и отмечают те уязвимости, которые были найдены вновь или устранены между двумя сканированиями. В приведенном выше примере LAN Scan One является сканированием всей подсети 192.168.0.0/24, а LAN Scan Two — сканированием трех выбранных хостов подсети 192.168.0.0/24. Функция Compare (сравнить) отображает отличия, выделяя хосты, которые не были просканированы в ходе сканирования LAN Scan Two:

Отправка и загрузка

Результаты сканирования можно экспортировать с одного сканера и импортировать в другой сканер. Функции **Upload** (отправка) и **Download** (загрузка) помогают лучше управлять сканированиями, сравнением отчетов, резервным копированием отчетов и обменом данными между группами или организациями в рамках компании.

Для экспорта сканирования сначала выберите его на экране **Reports** (отчеты) и нажмите кнопку **Download** (загрузить). При этом откроется диалоговое окно загрузки отчетов:



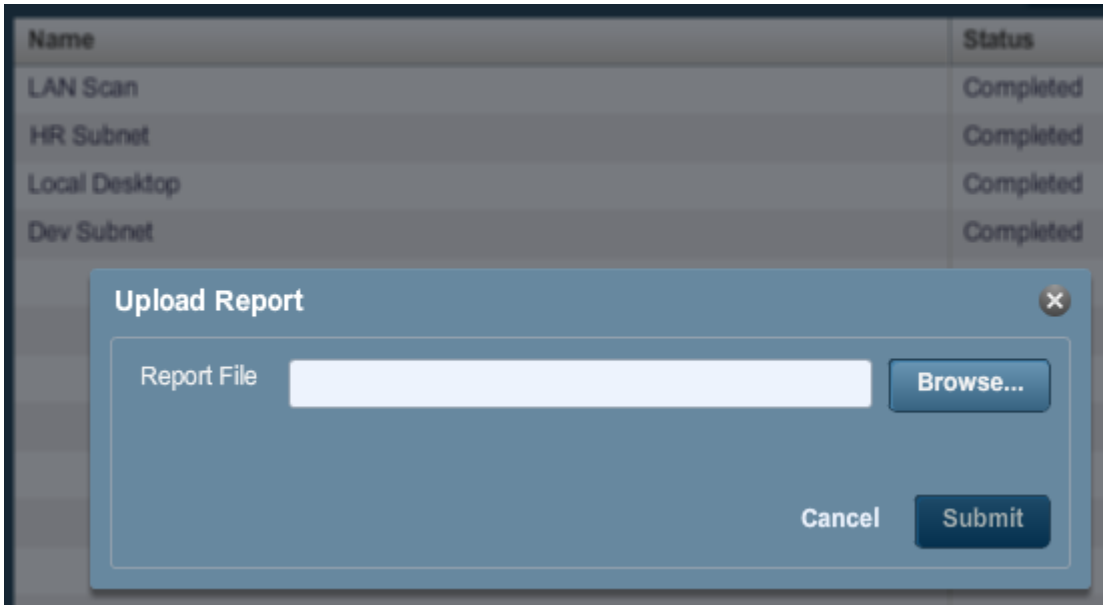
Отчеты можно загружать в любом из четырех форматов:

Параметр	Описание
`.nessus`	Формат на основе XML и фактический стандарт в версии Nessus 4.2 и более поздних версиях. В этом формате используется расширенный набор тегов XML, позволяющий более точно извлекать и анализировать информацию.
`.nessus` **(v1)**	Формат на основе XML, используемый в версиях с Nessus 3.2 по 4.0.2, совместим с Nessus 4.x и Security Center 3.
Detailed HTML Report (by finding) (подробный отчет HTML (по обнаруженным уязвимостям))	Отчет, генерируемый с помощью стандартного формата HTML, который можно просматривать в любом веб-браузере. Отчет классифицирован по уязвимостям (Nessus Plugin ID (идентификатор подключаемого модуля Nessus)).
Detailed RTF Report (by finding) (подробный отчет RTF (по обнаруженным	Отчет, генерируемый с помощью формата RTF, просмотр.

уязвимостям))	
Executive HTML export (top 10 most vulnerable hosts) (краткий экспорт HTML (10 самых уязвимых хостов)	Отчет, генерируемый с помощью стандартного формата HTML, который включает только 10 хостов, в которых были обнаружены наибольшие уязвимости.
HTML export (экспорт HTML)	Отчет, генерируемый с помощью стандартного формата HTML, классифицированный по хостам.
NBE export (экспорт NBE)	Экспорт с разделением данных символом вертикальной черты, который может использоваться для импорта во многие внешние программы.

После выбора формата **.nessus** или NBE откроется стандартное диалоговое окно Save File (сохранить файл) используемого веб-браузера, которое позволяет сохранить результаты сканирования в нужное расположение. Отчеты HTML отображаются в браузере и могут сохраняться с помощью функции File -> Save (файл -> сохранить).

Для импорта сканирования нажмите кнопку **Upload** (отправка) на экране **Reports** (отчеты):



С помощью кнопки **Browse...** (обзор...) выберите файл сканирования **.nessus**, который необходимо импортировать, и нажмите кнопку **Submit** (отправить). Сервер Nessus проанализирует информацию и сделает ее доступной в интерфейсе **Reports** (отчеты).

Формат файлов .nessus

Сканер Nessus использует определенный формат файлов (**.nessus**) для экспорта и импорта сканирований. Этот формат обладает следующими преимуществами.

- Основан на языке XML, что упрощает обеспечение прямой и обратной совместимости, а также упрощает реализацию.
- Самодостаточный: единый файл `.nessus` содержит список целевых машин, определенные пользователем политики, а также сами результаты сканирования.
- Безопасный: пароли в файл не сохраняются. Вместо этого используются ссылки на пароли, сохраненные в безопасном расположении на локальном хосте.

Процесс создания файла `.nessus`, содержащего целевые машины, политики и результаты сканирования, начинается с генерирования политики и ее сохранения. Затем генерируется список целевых адресов и, наконец, выполняется сканирование. После завершения сканирования вся информация может быть сохранена в файл `.nessus` с помощью функции **Download** (загрузить) из вкладки **Reports** (отчеты). Дополнительную информацию о файлах `.nessus` см. в документе «Nessus File Format» (Формат файлов Nessus).

Удаление

После окончания работы с результатами сканирования можно выбрать сканирование из списка Reports (отчеты) и нажать кнопку **Delete** (удалить). При этом сканирование будет удалено из интерфейса пользователя. **Это действие невозможно отменить**! Используйте функцию **Download** (загрузить) для экспорта результатов сканирования перед удалением.

Пользователи

Вкладка **Users** (пользователи) является интерфейсом для управления пользователями сканера Nessus. Новых пользователей можно добавлять с помощью диспетчера Nessus Server Manager (Mac OS X/Windows), команды `nessus-adduser` (*nix) или через интерфейс пользователя (все платформы). Для создания нового пользователя через интерфейс пользователя Nessus нажмите кнопку **Add** (добавить) в верхнем правом меню. При этом появится диалоговое окно для ввода имени пользователя и пароля с флажком, позволяющим сделать пользователя администратором сканера Nessus:

Для изменения или удаления пользователя выберите имя пользователя в списке **Users** (пользователи) и нажмите соответственно кнопку **Edit** (правка) или **Delete** (удалить) в верхнем правом меню.

ДРУГИЕ КЛИЕНТЫ NESSUS

Помимо Nessus GUI (графического интерфейса пользователя Nessus) компания Tenable поддерживает два других метода обмена данными с сервером Nessus: интерфейс командной строки и консоль SecurityCenter.

Интерфейс командной строки

При работе с сервером Nessus доступен интерфейс командной строки (CLI). Для запуска сканирования из командной строки необходимо запустить сканирование в пакетном режиме с помощью следующего синтаксиса команд:

ОС	Команда
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
FreeBSD	`# /usr/local/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
Mac OS X	`# /Library/Nessus/run/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
Windows	`%programfiles%\Tenable\Nessus\nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`

В приведенной ниже таблице объясняются разные аргументы, используемые для запуска сканирования в пакетном режиме.

Аргумент	Описание
`-q`	Пакетный режим. Запуск сканирования Nessus не в пакетном режиме.

-p	Получение списка подключаемых модулей, установленных на сервере.
-p	Получение списка предпочтений сервера и подключаемых модулей.
-S	Выдача результатов SQL для аргументов **-p** и **-P**.
<host>	Хост **nessusd**, к которому необходимо выполнить подключение.
<port>	Порт, к которому будет выполняться подключение на удаленном хосте **nessusd**.
<user>	Имя пользователя **nessusd**, с помощью которого будет выполняться подключение.
<password>	Пароль, соответствующий имени пользователя.
<targets-file>	Имя файла, содержащего список целевых машин для сканирования.
<results-file>	Имя файла, в который будут сохранены результаты по окончании сканирования.

Есть и другие параметры, доступные при выполнении сканирования в пакетном режиме. Они разъясняются в следующей таблице.

Параметр	Описание
-V	Включает отображение на экране сообщений состояния в пакетном режиме.
-x	Не проверять сертификаты SSL.
-v	Версия. Отображение номера версии и выход.
-h	Справка. Вывод на экран сводки команд и выход.
-T <type>	Сохранение данных как <type>, где <type> может быть nbe, html, nessus или text.

Преобразование отчета

Сканер Nessus можно использовать для преобразования форматов отчетов. Сканер Nessus может принять любой отчет в формате NBE и преобразовать его в текстовый формат, формат HTML или **.nessus**.

Для преобразования отчета используйте следующую команду:

ОС	Команда
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
FreeBSD	`# /usr/local/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Mac OS X	`# /Library/Nessus/run/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Windows	`%programfiles%\Tenable\Nessus\nessus -i in.nbe -o out.[html|txt|nessus]`

Параметр **-i** определяет файл NBE для преобразования. Параметр **-o** определяет имя и тип файла, в который будет преобразован отчет (это может быть текстовый формат, формат HTML или **.nessus**).

Содержащиеся в файлах **.nessus** отчеты также могут быть преобразованы в формат HTML из командной строки. Для этого используется следующий синтаксис:

Чтобы преобразование в HTML сработало, файл **.nessus** должен быть сохранен в формате загрузки nessus (v1).

ОС	Команда
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
FreeBSD	`# /usr/local/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Mac OS X	`# /Library/Nessus/run/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus in.nessus -i <ReportName> -o out.html`

Параметр **--dot-nessus** указывает файл входных данных **.nessus**, который будет использоваться. <ReportName> — это имя отчета, указанное в файле входных данных **.nessus**.

Использование файлов .nessus с помощью командной строки

Есть несколько аргументов, которые могут передаваться для разрешения работы с файлами **.nessus** входных данных или выходных данных из командной строки. Они разъясняются в следующей таблице.

Аргумент	Описание
--dot-nessus <file>	При использовании этот параметр всегда предоставляется для передачи в качестве первого параметра двоичному

	файлу **nessus**, чтобы указать, что будет использоваться файл **.nessus**. <file> — это расположение и имя файла **.nessus**, который будет использоваться.
--policy-name <policy>	Имя политики, содержащейся в назначенном файле **.nessus**. Параметр политики предоставляется при запуске сканирования из командной строки. Обратите внимание, что предоставленное имя политики должно точно соответствовать имени политики, включая одиночные кавычки, в соответствии с отображаемыми с помощью параметра **--list-policies** данными (см. ниже).
--list-policies	Предоставление имен всех политик сканирования, содержащихся в назначенном файле **.nessus**.
--list-reports	Предоставление имен всех отчетов, содержащихся в назначенном файле **.nessus**.
--target-file <file>	Переопределение целевых машин, указанных в файле **.nessus**, и использование вместо этого содержащихся в указанном файле.

Следующая команда отображает список всех отчетов, содержащихся в файле **scan.nessus**:

Файл **.nessus** должен быть сохранен в формате загрузки nessus (v1), чтобы аргумент **--list-reports** сработал.

ОС	Команда
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-reports**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-reports**
Mac OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-reports**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-reports**

Ниже приведен пример выходных данных:

```
List of reports contained in scan.nessus:
- '08/03/10 11:19:55 AM - Full Safe w/ Compliance'
- '08/03/10 01:01:01 PM - Full Safe w/ Compliance'
- '08/03/10 01:32:10 PM - Full Safe w/ Compliance'
- '08/03/10 02:13:01 PM - Full Safe w/ Compliance'
- '08/03/10 02:45:00 PM - Full Safe w/ Compliance'
```

Следующая команда отображает список всех политик, содержащихся в файле **scan.nessus**:

Файл **.nessus** должен быть сохранен в формате загрузки nessus (v1), чтобы аргумент **--list-policies** сработал.

ОС	Команда
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
Mac OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-policies**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-policies**

Ниже приведен пример выходных данных при использовании этой команды:

```
List of policies contained in scan.nessus:
- 'Full Safe w/ Compliance'
```

Обратите внимание, что при передаче имен отчетов или политик сканеру Nessus в качестве параметров командной строки имя должно передаваться точно так, как отображается в результате применения описанных выше команд, включая одиночные кавычки (`'Safe w/ Compliance'`).

Команда сканирования

При условии, что указанная в приведенных выше примерах политика существует, сканирование может быть запущено со следующими параметрами:

Файл **.nessus**, указанный в сканировании, должен быть в формате nessus (v1), чтобы сканирование было произведено.

ОС	Команда
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>**
Mac OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance'**

	`<host> <port> <user> <password> <results-file>`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --policy-name "Full Safe w/Compliance" <host> <port> <user> <password> <results-file>`

В приведенном выше примере параметры **<host>**, **<port>**, **<user>**, **<password>** и **<results-file>** предоставляются в соответствии с приведенной выше документацией. Параметр <targets-file> не требуется, потому что для сканирования используется список целевых машин, содержащийся в файле `.nessus`.

Формат генерируемого отчета определяется на основании расширения файла, предоставленного в команде `nessus`. Если в приведенной выше команде имя файла, предоставленное в параметре <results-file>, будет `report.nbe`, то отчет будет сохранен в формате `.nbe`. А если имя файла будет "`report.nessus`, то отчет будет сохранен в формате `.nessus`.

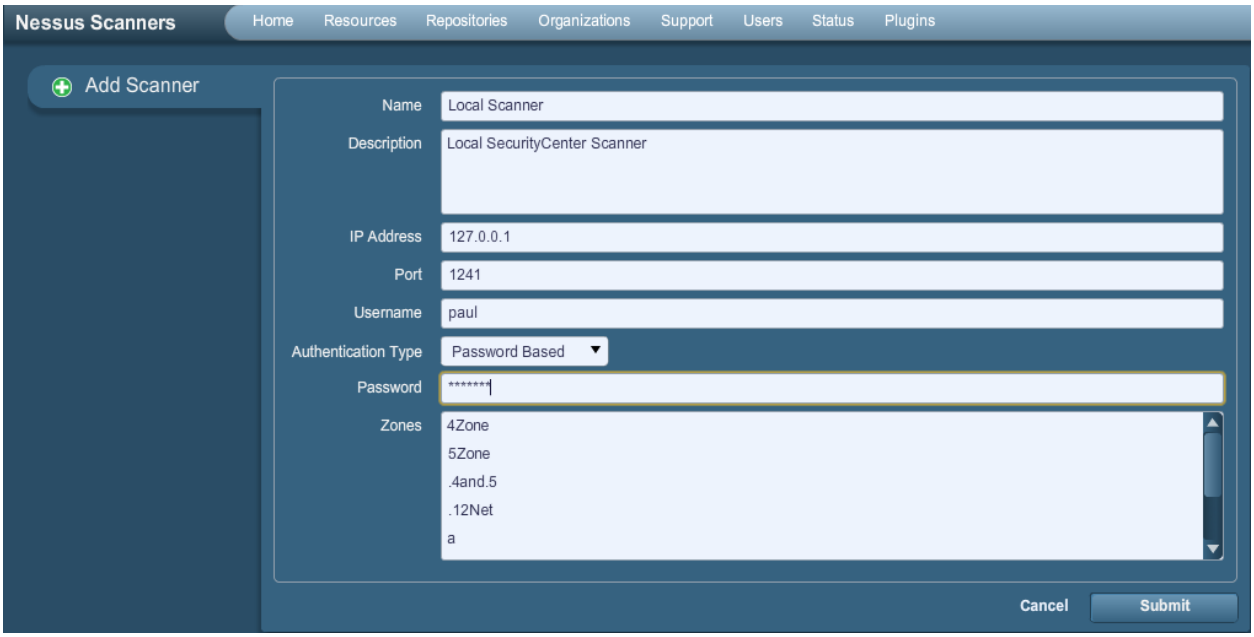
Если в параметре <results-file> не предоставить никаких данных, то отчет будет добавлен в файл `scan.nessus`.

SecurityCenter

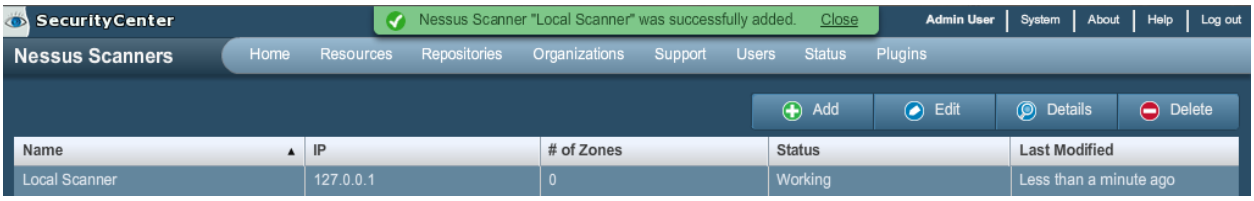
Настройка консоли SecurityCenter

Сервер Nessus Server можно добавить через интерфейс администрирования SecurityCenter. С помощью этого интерфейса SecurityCenter можно настроить для доступа и управления практически любым сканером Nessus. Выберите вкладку Resources (ресурсы), затем щелкните **Nessus Scanners** (сканеры Nessus). Нажмите кнопку **Add** (добавить), чтобы открыть диалоговое окно Add Scanner (добавить сканер). Требуется IP-адрес сканера Nessus, порт сканера Nessus (по умолчанию: 1241), идентификатор входа администратора, тип проверки подлинности и пароль (созданные при настройке сканера Nessus). В случае выбора типа проверки подлинности SSL Certificate (сертификат SSL) поля паролей недоступны. Кроме того, можно выбрать значения Zones (зоны), которым будет назначен сканер Nessus.

Ниже приведен пример снимка экрана страницы Add Scanner (добавление сканера) ПО SecurityCenter:



После успешного добавления сканера и выбора сканера отобразится следующая страница:



Дополнительные сведения см. в «Руководстве по администрированию SecurityCenter».

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Компания Tenable подготовила различные документы, содержащие подробные сведения об установке, развертывании, настройке, пользовательской эксплуатации и общем тестировании сканера Nessus. Список этих документов приведен ниже.

- **Руководство по установке Nessus** — пошаговое руководство по установке.
- **Проверки Nessus с использованием учетных данных для Unix и Windows** — сведения о порядке выполнения сканирования сетей с проверкой подлинности при помощи сканера уязвимостей Nessus.
- **Проверки соответствия Nessus** — руководство высокого уровня для понимания и выполнения проверок соответствия с помощью сканера Nessus и консоли SecurityCenter.
- **Справочник по проверкам соответствия Nessus** — полное руководство по синтаксису проверок соответствия Nessus.
- **Формат файлов Nessus v2** — содержит описание структуры формата файлов `.nessus`, который был введен с версиями Nessus 3.2 и NessusClient 3.2.
- **Спецификация протокола Nessus XML-RPC** — содержит описание протокола XML-RPC и интерфейса в Nessus.

- **Контроль соответствия в режиме реального времени** — содержит обзор того, как решения компании Tenable могут использоваться для обеспечения выполнения разных типов государственных и финансовых норм.

Без колебаний пишите нам по адресам электронной почты support@tenable.com, sales@tenable.com или посетите наш веб-сайт по адресу http://www.tenable.com/.

О КОМПАНИИ TENABLE NETWORK SECURITY

Компания Tenable Network Security, ведущая компания в области комплексного мониторинга безопасности, является разработчиком сканера уязвимостей Nessus, а также создателем решения корпоративного класса, не требующего агентов, для непрерывного мониторинга уязвимостей, слабых мест конфигураций, утечек данных, управления журналами и обнаружения взломов с целью обеспечения безопасности сетей и соответствия требованиям FDCC, FISMA, SANS CAG и PCI. Продукты компании Tenable, заслужившие различные награды, используются организациями из списка Global 2000 и государственными учреждениями для упреждающего понижения связанных с сетями рисков до минимума. Дополнительные сведения см. на веб-сайте http://www.tenable.com/.

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