
# Nessus 4.4
# Руководство по установке

14 июня 2011 г.

**(редакция 9)**



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 установка и настройка сканера уязвимостей **Nessus 4.4** компании Tenable Network Security. Мы будем рады получить ваши комментарии и предложения по адресу электронной почты support@tenable.com.

Компания Tenable Network Security, Inc. является автором и оператором сканера уязвимостей Nessus. Помимо постоянного совершенствования ядра Nessus, компания Tenable разрабатывает большую часть доступных подключаемых модулей для сканера, а также проверок соответствия и широкого спектра политик аудита.

В этом документе рассматриваются необходимые условия, параметры развертывания и пошаговая процедура установки. Предполагается базовое понимание системы Unix и процесса сканирования уязвимостей.

Начиная с версии Nessus 4.4 управление пользователями сервера Nessus выполняется через веб-интерфейс, при этом использование отдельного клиента NessusClient больше не требуется. Отдельный клиент NessusClient по-прежнему будет подключаться и управлять сканером, но не будут обновляться.

## Поддержка операционных систем

Сканер Nessus предлагается и поддерживается для различных операционных систем и платформ:

- Debian 5 (i386 и x86-64)
- Fedora Core 12, 13 и 14 (i386 и x86-64)
- FreeBSD 8 (i386 и x86-64)
- Mac OS X 10.4, 10.5 и 10.6 (i386, x86-64, ppc)
- Red Hat ES 4 / CentOS 4 (i386)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 и x86-64)
- Red Hat ES 6 / CentOS 6 (i386 и x86-64) [Server, Desktop, Workstation]
- Solaris 10 (sparc)
- SuSE 9.3 (i386)
- SuSE 10.0 и 11 (i386 и x86-64)
- Ubuntu 8.04, 9.10, 10.04 и 10.10 (i386 и x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2, Vista и 7 (i386 и x86-64)

## 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 **`setup.exe`**.

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.

## ОБЩИЕ СВЕДЕНИЯ

Nessus – это мощный, современный и простой в использовании сетевой сканер безопасности. В настоящее время он считается одним из лучших продуктов своего типа во всей отрасли безопасности и одобрен профессиональными организациями по информационной безопасности, такими как институт SANS. Сканер Nessus позволяет выполнять удаленный аудит определенной сети и определять, была ли она взломана или использована каким-либо ненадлежащим образом. Сканер Nessus также дает возможность выполнять локальный аудит определенных машин в плане уязвимостей, соответствия стандартам, нарушений политик в отношении содержимого и т. д.

- **Интеллектуальное сканирование —** в отличие от многих других сканеров безопасности, Nessus ничего не принимает без проверки. Т. е. не предполагает, что определенная служба выполняется на фиксированном порту. Это означает, что если ваш веб-сервер работает на порту 1234, сканер Nessus обнаружит его и надлежащим образом протестирует его безопасность. При возможности он выполнит попытку проверки уязвимости путем моделирования взлома. В случаях, когда это ненадежно или может отрицательно повлиять на сканируемую машину, сканер Nessus может положиться при определении наличия уязвимости на заголовок сервера. В таких случаях в результатах отчета будет четко указано, что использовался этот метод.

- **Модульная архитектура —** архитектура клиент/сервер обеспечивает гибкость развертывания сканера (сервера) и подключение графического интерфейса пользователя (клиента) с любой машины при помощи веб-браузера, что сокращает расходы на управление (к одному серверу могут получать доступ несколько клиентов).

- **Совместимость с CVE —** большинство подключаемых модулей связаны с базой CVE, чтобы администраторы могли извлекать дополнительную информацию об опубликованных уязвимостях. Они также часто включают ссылки на базы Bugtraq (BID), OSVDB и оповещения по вопросам безопасности поставщиков.

- **Архитектура в виде подключаемых модулей —** каждый тест безопасности написан как внешний подключаемый модуль, все модули сгруппированы в 42 семейства. Таким образом можно легко добавлять собственные тесты, выбирать нужные подключаемые модули или целые семейства без необходимости изучать код

ядра сервера Nessus, **nessusd.** Полный перечень подключаемых модулей Nessus доступен по адресу http://www.nessus.org/plugins/index.php?view=all.

- **NASL —** сканер Nessus включает NASL (Nessus Attack Scripting Language) — язык, разработанный специально для удобного и быстрого написания тестов безопасности.

- **Своевременно обновляемая база данных уязвимостей —** компания Tenable сосредоточена на разработке проверок безопасности, связанных с новыми обнаруживаемыми уязвимостями. Наша база данных проверок безопасности обновляется ежедневно, и все новейшие проверки безопасности доступны по адресу http://www.nessus.org/scripts.php.

- **Одновременное тестирование нескольких хостов —** в зависимости от конфигурации системы сканера Nessus, можно тестировать одновременно большое количество хостов.

- **Интеллектуальное распознавание служб —** сканер Nessus не предполагает, что на сканируемых хостах соблюдаются назначенные IANA номера портов. Это означает, что он обнаружит FTP-сервер, работающий на нестандартном порту (например, 31337) или веб-сервер, работающий на порту 8080 вместо порта 80.

- **Несколько служб —** если на хосте работают два или более веб-серверов (например, один на порту 80, а другой на порту 8080), сканер Nessus определит и протестирует все серверы.

- **Взаимодействие подключаемых модулей —** тесты безопасности, выполняемые подключаемыми модулями Nessus, взаимодействуют между собой, чтобы не выполнялись ненужные проверки. Если ваш FTP-сервер не допускает анонимного входа, то связанные с анонимным входом проверки безопасности выполняться не будут.

- **Полные отчеты —** сканер Nessus не только сообщит о существующих в вашей сети уязвимостях безопасности и уровне риска каждой из них (Low (низкий), Medium (средний), High (высокий) и Critical (критический)), но также сообщит о том, как их устранить, предложив решения.

- **Полная поддержка SSL —** сканер Nessus может проверять службы, предоставляемые через SSL, например HTTPS, SMTPS, IMAPS и т. д.

- **Интеллектуальное управление подключаемыми модулями (по выбору) —** сканер Nessus определяет, какие подключаемые модули должны или не должны подключаться для удаленного хоста. Например, сканер Nessus не будет тестировать уязвимости Sendmail на сервере Postfix. Эта настройка называется optimization (оптимизация).

- **Отсутствие нарушения работы (по выбору) —** некоторые проверки могут нарушать работу определенных сетевых служб. Если вы не хотите создавать риск нарушения работы какой-либо службы в своей сети, включите параметр сканера Nessus safe checks (безопасные проверки), при включении которого сервер Nessus

будет полагаться на заголовки, а не пытаться эксплуатировать реальные недостатки в системе безопасности для определения наличия уязвимости.

- **Открытый форум —** Нашли ошибку? У вас возникли вопросы о Nessus? Начните обсуждение по адресу https://discussions.nessus.org/.

## НЕОБХОДИМЫЕ УСЛОВИЯ

Компания Tenable рекомендует использовать для работы Nessus минимум 2 ГБ памяти. Для проведения более крупных сканирований нескольких сетей рекомендуется не менее 3 ГБ памяти (но может потребоваться до 4 ГБ).

Рекомендуется процессор Pentium 3 с тактовой частотой 2 ГГц или выше. При работе под Mac OS X рекомендуется двухъядерный процессор Intel® с тактовой частотой 2 ГГц или выше.

Сканер Nessus может работать на виртуальной машине VMware. Но в случае использования имитируемой машиной преобразования сетевых адресов (NAT) для доступа к сети, это может отрицательно повлиять на многие из проверок уязвимостей Nessus, перечисление хостов и определение операционной системы.

### NESSUS UNIX

До начала установки Nessus на ОС Unix/Linux необходимо установить несколько библиотек. Многие операционные системы устанавливают эти библиотеки по умолчанию, при этом отдельная установка обычно не требуется.

- OpenSSL (например, openssl, libssl, libcrypto).
- zlib.
- GNU C Library (т. е. libc).

### NESSUS WINDOWS

Корпорация Microsoft внесла изменения в ОС Windows XP SP2 и более новые версии (выпуски Home и Pro), которые могут повлиять на производительность Nessus Windows. Для повышения производительности и надежности сканирования настоятельно рекомендуется устанавливать Nessus Windows на серверные версии семейства ОС Microsoft Windows, например Windows Server 2003. Дополнительные сведения по этому вопросу см. в разделе Устранение неполадок Nessus Windows.

## ПАРАМЕТРЫ РАЗВЕРТЫВАНИЯ

При развертывании Nessus часто бывают полезны знания о маршрутизации, фильтрах и политиках брандмауэров. Рекомендуется развертывать сервер Nessus таким образом, чтобы он имел хорошую IP-связь с сетями, которые он сканирует. Развертывание за устройством NAT нежелательно, за исключением сканирования внутренней сети. При сканировании уязвимостей через NAT или прокси приложения любого типа проверка может быть нарушена и может дать ложный положительный или отрицательный результат. Кроме того, если на системе, на которой выполняется Nessus, включен личный или настольный брандмауэр, эти средства могут резко ограничить эффективность удаленного сканирования уязвимостей.

Выполняемые на хостах брандмауэры могут мешать сетевому сканированию уязвимостей. В зависимости от конфигурации брандмауэра он может не допускать, искажать или скрывать проверки сканирования Nessus.

# ПОДПИСКИ НА ПОДКЛЮЧАЕМЫЕ МОДУЛИ УЯЗВИМОСТЕЙ

Каждый день поставщиками ПО, исследователями и прочими источниками публикуются многочисленные новые уязвимости. Компания Tenable стремится тестировать и делать доступными проверки недавно опубликованных уязвимостей как можно быстрее, обычно в течение 24 часов с момента их раскрытия. Проверка на наличие определенной уязвимости называется в сканере Nessus «plugin» (подключаемый модуль). Полный перечень всех подключаемых модулей Nessus доступен по адресу http://www.nessus.org/plugins/index.php?view=all. Компания Tenable распространяет новейшие подключаемые модули Nessus для проверки уязвимостей в двух режимах: ProfessionalFeed и HomeFeed.

Подключаемые модули загружаются непосредственно с сервера Tenable через автоматизированный процесс, реализованный в Nessus. Сканер Nessus проверяет цифровые подписи всех загруженных подключаемых модулей для обеспечения их целостности. Для установок Nessus без доступа к Интернету есть автономный процесс обновления, который может использоваться для обеспечения своевременного обновления сканера.

В версии Nessus 4 вам необходимо зарегистрироваться на канал подключаемых модулей и обновить подключаемые модули, прежде чем сканер Nessus запустится и станет доступен интерфейс сканирования Nessus. После начальной регистрации сканера обновление подключаемых модулей происходит в фоновом режиме и может занимать несколько минут.

## Какой канал вам подходит?

Конкретные инструкции по конфигурации сканера Nessus для получения канала HomeFeed или ProfessionalFeed приведены ниже в этом документе. Чтобы определить, какой канал Nessus лучше подходит для вашей среды, рассмотрите следующую информацию.

### *Канал HomeFeed*

В случае использования сканера Nessus дома для непрофессиональных целей можно подписаться на канал HomeFeed. Новые подключаемые модули для выявления последних уязвимостей немедленно предоставляются пользователям канала HomeFeed. Плата за пользование каналом HomeFeed не взимается, но есть отдельная лицензия для канала HomeFeed, условия которой должны подтвердить и соблюдать пользователи. Чтобы зарегистрироваться для использования канала HomeFeed, посетите веб-сайт http://www.nessus.org/register/ и зарегистрируйте свой экземпляр Nessus для использования канала HomeFeed. При настройке обновления Nessus воспользуйтесь кодом активации (Activation Code), который получите в процессе регистрации. Пользователи канала HomeFeed не получают доступа к порталу поддержки Tenable Support Portal, проверкам соответствия стандартам и политикам аудита содержимого.

### *Канал ProfessionalFeed*

В случае использования сканера Nessus для коммерческих целей (например, для консультирования), в бизнес-среде или в среде государственного учреждения следует приобрести подписку на канал ProfessionalFeed. Новые подключаемые модули для выявления последних уязвимостей немедленно предоставляются пользователям канала ProfessionalFeed. Клиенты, пользующиеся консолью SecurityCenter, автоматически получают подписку на канал ProfessionalFeed, им не требуется приобретать дополнительный канал, если у них нет сканера Nessus, который не управляется консолью SecurityCenter.

Компания Tenable предоставляет коммерческую поддержку через портал поддержки Tenable Support Portal или по электронной почте клиентам ProfessionalFeed, которые используют Nessus 4. Канал ProfessionalFeed также включает набор проверок соответствия на базе хостов для ОС Unix и Windows, которые очень полезны при выполнении аудитов соответствия, таких как соответствие стандартам SOX, FISMA или FDCC.

Подписку на канал ProfessionalFeed можно приобрести либо через интернет-магазин компании Tenable по адресу https://store.tenable.com/, либо посредством оформления заказа на покупку через программу авторизованных партнеров ProfessionalFeed. Затем вы получите от компании Tenable код активации (Activation Code). Этот код необходимо использовать при настройке обновлений своего экземпляра Nessus.

При использовании сканера Nessus в сочетании с консолью SecurityCenter компании Tenable консоль SecurityCenter будет иметь доступ к каналу ProfessionalFeed и будет автоматически обновлять ваши сканеры Nessus.

Определенные сетевые устройства, выполняющие проверки с отслеживанием состояния, например брандмауэры, службы балансировки нагрузки и системы обнаружения/предотвращения проникновений, могут отрицательно реагировать в случае проведения сканирования через них. Сканер Nessus имеет несколько параметров настройки, позволяющих снизить влияние сканирования через такие устройства. Но лучшим методом избежать проблем, связанных со сканированием через такие сетевые устройства, является выполнение сканирования с проверкой подлинности.

## ПОДДЕРЖКА IPV6

Начиная с версии 3.2 BETA сканер Nessus поддерживает сканирование ресурсов на базе протокола IPv6. Многие операционные системы и устройства поставляются с включенной поддержкой IPv6 по умолчанию. Для выполнения сканирования IPv6-ресурсов на хосте, на котором установлен Nessus, должен быть настроен хотя бы один интерфейс протокола IPv6, и сканер Nessus должен находиться в совместимой с протоколом IPv6 сети (Nessus не может сканировать IPv6-ресурсы через протокол IPv4, но может перечислять интерфейсы протокола IPv6 посредством сканирования с проверкой подлинности через IPv4). При инициализации сканирования поддерживается и полный, и сжатый формат IPv6.

В ОС Microsoft Windows отсутствуют некоторые необходимые интерфейсы API, которые требуются для фальсификации пакетов IPv6 (например, получения MAC-адреса маршрутизатора, таблицы маршрутизации и т. д.). Это в свою очередь не позволяет сканеру портов работать надлежащим образом. Компания Tenable работает над усовершенствованиями, которые обеспечат эффективный обход ограничений API в будущих версиях сканера Nessus.

# UNIX/LINUX

## Обновление

В этом разделе рассматривается обновление сканера Nessus с предыдущей установки Nessus.

В следующей таблице представлены инструкции по обновлению сервера Nessus на всех ранее поддерживавшихся платформах. Созданные ранее настройки конфигурации и пользователи останутся без изменений.

Прежде чем выполнять остановку **nessusd**, необходимо убедиться, что все выполняемые сканирования завершились.

Все особые инструкции по обновлению приведены в примечании после примера.

| Платформа | Инструкции по обновлению |
|---|---|
| **Red Hat ES 4 (32-разрядная), ES 5 (32- и 64-разрядная)** | |
| **Команды обновления** | `# service nessusd stop`<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Red Hat:<br><br>`# rpm -Uvh Nessus-4.4.0-es4.i386.rpm`<br>`# rpm -Uvh Nessus-4.4.0-es5.i386.rpm`<br>`# rpm -Uvh Nessus-4.4.0-es5.x86_64.rpm`<br><br>После завершения обновления перезапустите службу `nessusd` с помощью следующей команды:<br><br>`# service nessusd start` |
| **Пример выходных данных** | `# service nessusd stop`<br>`Shutting down Nessus services: [ OK ]`<br>`# rpm -Uvh Nessus-4.4.0-es4.i386.rpm`<br>`Preparing...`<br>`########################################### [100%]`<br>`Shutting down Nessus services:`<br>`1:Nessus`<br>`########################################### [100%]` |

| | |
|---|---|
| | nessusd (Nessus) 4.4.0 for Linux<br>(C) 1998 – 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br>- Please run /opt/nessus/sbin/nessus-adduser to add an admin user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /sbin/service nessusd start<br><br># **service nessusd start**<br>Starting Nessus services: [ OK ]<br># |
| **Fedora Core 12, 13 и 14 (32- и 64-разрядная)** | |
| **Команды обновления** | # **service nessusd stop**<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Fedora Core:<br><br># **rpm -Uvh Nessus-4.4.0-fc12.i386.rpm**<br># **rpm -Uvh Nessus-4.4.0-fc12.x86_64.rpm**<br># **rpm -Uvh Nessus-4.4.0-fc14.i386.rpm**<br># **rpm -Uvh Nessus-4.4.0-fc14.x86_64.rpm**<br><br>После завершения обновления перезапустите службу `nessusd` с помощью следующей команды:<br><br># **service nessusd start** |
| **Пример выходных данных** | # **service nessusd stop**<br>Shutting down Nessus services: [ OK ]<br># **rpm -Uvh Nessus-4.4.0-fc12.i386.rpm**<br>Preparing...<br>########################################### [100%]<br>Shutting down Nessus services:<br>1:Nessus<br>########################################### [100%]<br>nessusd (Nessus) 4.4.0 for Linux<br>(C) 1998 – 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br>- Please run /opt/nessus/sbin/nessus-adduser to add an admin user<br>- Register your Nessus scanner at |

| | |
|---|---|
| | http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /sbin/service<br>nessusd start<br><br># **service nessusd start**<br>Starting Nessus services: [ OK ]<br># |
| **SuSE 9.3 (32-разрядная), 10 (32- и 64-разрядная)** | |
| **Команды обновления** | # **service nessusd stop**<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС SuSE:<br><br># **rpm -Uvh Nessus-4.4.0-suse9.3.i586.rpm**<br># **rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm**<br># **rpm -Uvh Nessus-4.4.0-suse10.x86_64.rpm**<br><br>После завершения обновления перезапустите службу `nessusd` с помощью следующей команды:<br><br># **service nessusd start** |
| **Пример выходных данных** | # **service nessusd stop**<br>Shutting down Nessus services: [ OK ]<br># **rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm**<br>Preparing...<br>########################################### [100%]<br>Shutting down Nessus services:<br>1:Nessus<br>########################################### [100%]<br>nessusd (Nessus) 4.4.0 for Linux<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br>- Please run /opt/nessus/sbin/nessus-adduser to add an admin user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /sbin/service nessusd start<br><br># **service nessusd start**<br>Starting Nessus services: [ OK ]<br># |

| Debian 5 (32- и 64-разрядная) | |
|---|---|
| **Команды обновления** | **# /etc/init.d/nessusd stop**<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Debian:<br><br>**# dpkg -i Nessus-4.4.0-debian5_i386.deb**<br>**# dpkg -i Nessus-4.4.0-debian5_amd64.deb**<br><br>**# /etc/init.d/nessusd start** |
| **Пример выходных данных** | **# /etc/init.d/nessusd stop**<br><br>**# dpkg -i Nessus-4.4.0-debian5_i386.deb**<br>(Reading database ... 19831 files and directories currently installed.)<br>Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-debian5_i386.deb) ...<br>Shutting down Nessus : .<br>Unpacking replacement nessus ...<br><br>Setting up nessus (4.4.0) ...<br><br>nessusd (Nessus) 4.4.0. for Linux<br>(C) 2009 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add an admin user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br><br>**# /etc/init.d/nessusd start**<br><br>Starting Nessus : .<br># |
| **Ubuntu 8.04, 9.10, 10.04 и 10.10 (32- и 64-разрядная)** | |
| **Команды обновления** | **# /etc/init.d/nessusd stop**<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Ubuntu:<br><br>**# dpkg -i Nessus-4.4.0-ubuntu804_i386.deb**<br>**# dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb** |

| | |
|---|---|
| | **# dpkg -i Nessus-4.4.0-ubuntu910_i386.deb**<br>**# dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb**<br>**# dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb**<br>**# dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb**<br><br>**# /etc/init.d/nessusd start** |
| **Пример выходных данных** | **# /etc/init.d/nessusd stop**<br><br>**# dpkg -i Nessus-4.4.0-ubuntu804_i386.deb**<br>(Reading database ... 19831 files and directories currently installed.)<br>Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-ubuntu810_i386.deb) ...<br>Shutting down Nessus : .<br>Unpacking replacement nessus ...<br><br>Setting up nessus (4.4.0) ...<br><br>nessusd (Nessus) 4.4.0. for Linux<br>(C) 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add an admin user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br><br>**# /etc/init.d/nessusd start**<br><br>Starting Nessus : .<br># |
| **Solaris 10 (sparc)** | |
| **Команды обновления** | **# /etc/init.d/nessusd stop**<br>**# pkginfo \| grep nessus**<br><br>Следующие выходные данные, получаемые в результате применения предыдущей команды, содержат сведения о пакете Nessus:<br><br>application TNBLnessus The Nessus Network Vulnerability Scanner<br><br>Для удаления пакета Nessus из системы Solaris выполните следующую команду: |

| | |
|---|---|
| | # **pkgrm <package name>**<br><br># **gunzip Nessus-4.x.x-solaris-sparc.pkg.gz**<br># **pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg**<br><br>The following packages are available:<br>  1  TNBLnessus-4-2-0  TNBLnessus<br>  (sparc) 4.4.0<br><br>Select package(s) you wish to process (or 'all' to process<br>all packages). (default: all) [?,??,q]: 1<br><br># **/etc/init.d/nessusd start** |
| **Пример выходных данных** | # **/etc/init.d/nessusd stop**<br># **pkginfo \| grep nessus**<br><br>application TNBLnessus  The Nessus Network Vulnerability Scanner<br><br># **pkgrm TNBLnessus**<br>(output redacted)<br>## Updating system information.<br><br>Removal of <TNBLnessus> was successful.<br><br># **gunzip Nessus-4.4.0-solaris-sparc.pkg.gz**<br># **pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg**<br><br>The following packages are available:<br>  1  TNBLnessus  The Nessus Network Vulnerability Scanner<br>  (sparc) 4.4.0<br>Select package(s) you wish to process (or 'all' to process<br>all packages). (default: all) [?,??,q]: 1<br><br>Processing package instance <TNBLnessus> from </export/home/cbf/TENABLE/Nessus-4.4.0-solaris-sparc.pkg><br><br>The Nessus Network Vulnerability Scanner<br>(sparc) 4.4.0<br>## Processing package information.<br>## Processing system information.<br>  13 package pathnames are already properly installed.<br>## Verifying disk space requirements.<br>## Checking for conflicts with packages already installed.<br>## Checking for setuid/setgid programs.<br><br>This package contains scripts which will be executed with super-user<br>permission during the process of installing this package. |

| | |
|---|---|
| | Do you want to continue with the installation of <TNBLnessus> [y,n,?]y<br><br>Installing The Nessus Network Vulnerability Scanner as <TNBLnessus><br><br>## Installing part 1 of 1.<br>(output redacted)<br>## Executing postinstall script.<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add a user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br><br>Installation of <TNBLnessus> was successful.<br><br># **/etc/init.d/nessusd start**<br># |
| **Примечания** | Для обновления сервера Nessus на ОС Solaris необходимо сначала удалить существующую версию, а затем установить самый новый выпуск сервера. В результате этого процесса не будут удалены файлы конфигурации, а также файлы, не входившие в исходную установку.<br><br>В случае возникновения ошибок совместимости библиотек убедитесь, что к системе применен последний рекомендованный кластер исправлений Solaris, загружаемый с веб-сайта Sun. |
| **FreeBSD 8 (32- и 64-разрядная)** | |
| **Команды обновления** | # **killall nessusd**<br># **pkg_info**<br><br>Эта команда выдаст список всех установленных пакетов и их описания. Следующие выходные данные, получаемые в результате применения предыдущей команды, содержат сведения о пакете Nessus:<br><br>Nessus-4.2.2 A powerful security scanner<br><br>Удалите пакет Nessus с помощью следующей команды:<br><br># **pkg_delete <package name>**<br><br>Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС FreeBSD: |

| | |
|---|---|
| | **# pkg_add Nessus-4.4.0-fbsd8.tbz**<br>**# pkg_add Nessus-4.4.0-fbsd8.amd64.tbz**<br><br>**# /usr/local/nessus/sbin/nessusd -D** |
| **Пример выходных данных** | **# killall nessusd**<br>**# pkg_delete Nessus-4.2.2**<br>**# pkg_add Nessus-4.4.0-fbsd8.tbz**<br><br>nessusd (Nessus) 4.4.0. for FreeBSD<br>(C) 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br><br>- Please run /usr/local/nessus/sbin/nessus-adduser to add an<br>admin user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to<br>obtain all the newest plugins<br>- You can start nessusd by typing /usr/local/etc/rc.d/nessusd.sh start<br><br>**# /usr/local/nessus/sbin/nessusd -D**<br><br>nessusd (Nessus) 4.4.0. for FreeBSD<br>(C) 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br># |
| **Примечания** | Для обновления сервера Nessus на ОС FreeBSD необходимо сначала удалить существующую версию, а затем установить самый новый выпуск сервера. В результате этого процесса не будут удалены файлы конфигурации, а также файлы, не входившие в исходную установку. |

## Установка

При первом обновлении сканера Nessus и обработке подключаемых модулей это может занять несколько минут. Веб-сервер отобразит сообщение «Nessus is initializing...» (выполняется инициализация Nessus...) и выполнит перезагрузку, когда будет готов.

Загрузите самую новую версию сервера Nessus с веб-сайта http://www.nessus.org/download/ или через портал поддержки Tenable Support Portal.

Проверьте целостность установочного пакета путем сравнения контрольной суммы MD5 загрузки с контрольной суммой, указанной в файле **MD5.asc**, находящемся здесь.

Если не указано иное, все команды должны выполняться под привилегированным пользователем (root) системы. Обычные учетные записи, как правило, не имеют необходимых разрешений для установки этого программного обеспечения.

В следующей таблице представлены инструкции по установке сервера Nessus на всех поддерживаемых платформах. Все особые инструкции по установке приведены в примечании после примера.

| Платформа | Инструкции по установке |
|---|---|
| **Red Hat ES 4 (32-разрядная), ES 5 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Red Hat:<br><br>**# rpm -ivh Nessus-4.4.0-es4.i386.rpm**<br>**# rpm -ivh Nessus-4.4.0-es5.i386.rpm**<br>**# rpm -ivh Nessus-4.4.0-es5.x86_64.rpm** |
| **Пример выходных данных** | **# rpm -ivh Nessus-4.4.0-es4.i386.rpm**<br>Preparing...<br>########################################### [100%]<br>1:Nessus<br>########################################### [100%]<br>nessusd (Nessus) 4.4.0. for Linux<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br>- Please run /opt/nessus//sbin/nessus-adduser to add a user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins<br>- You can start nessusd by typing /sbin/service nessusd start<br># |
| **Fedora Core 12, 13 и 14 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Fedora Core:<br><br>**# rpm -ivh Nessus-4.4.0-fc12.i386.rpm**<br>**# rpm -ivh Nessus-4.4.0-fc12.x86_64.rpm**<br>**# rpm -ivh Nessus-4.4.0-fc14.i386.rpm**<br>**# rpm -ivh Nessus-4.4.0-fc14.x86_64.rpm** |
| **Пример выходных** | **# rpm -ivh Nessus-4.4.0-fc12.i386.rpm**<br>Preparing... |

| | |
|---|---|
| **данных** | ```<br>########################################<br>[100%]<br>   1:Nessus<br>########################################<br>[100%]<br>nessusd (Nessus) 4.4.0. for Linux<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br> - Please run /opt/nessus//sbin/nessus-adduser to add a<br>user<br> - Register your Nessus scanner at<br>http://www.nessus.org/register/ to obtain<br>   all the newest plugins<br> - You can start nessusd by typing /sbin/service nessusd<br>start<br><br>#<br>``` |
| **SuSE 9.3 (32-разрядная), 10 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС SuSE:<br><br>**# rpm -ivh Nessus-4.4.0-suse9.3.i586.rpm**<br>**# rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm**<br>**# rpm -ivh Nessus-4.4.0-suse10.x86_64.rpm** |
| **Пример выходных данных** | ```<br># rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm<br>Preparing...   ################################## [100%]<br>   1:Nessus           ##################################<br>[100%]<br>Nessusd {Nessus} 4.4.0. for Linux<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br>- Please run /opt/nessus//sbin/nessus-adduser to add a<br>user<br>- Register your Nessus scanner at<br>http://www.nessus.org/register/ to obtain<br>all the newest plugins<br>- You can start nessusd by typing /etc/rc.d/nessusd start<br>#<br>``` |
| **Debian 5 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Debian:<br><br>**# dpkg -i Nessus-4.4.0 -debian5_i386.deb**<br>**# dpkg -i Nessus-4.4.0 -debian5_amd64.deb** |
| **Пример выходных данных** | ```<br># dpkg -i Nessus-4.4.0-debian5_i386.deb<br>Selecting previously deselected package nessus.<br>(Reading database ... 36954 files and directories<br>currently installed.)<br>Unpacking nessus (from Nessus-4.4.0-debian5_i386.deb) ...<br>``` |

| | |
|---|---|
| | Setting up nessus (4.4.0) ...<br>nessusd (Nessus) 4.4.0. for Linux<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add a user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br># |
| **Примечания** | Демон сервера Nessus не может быть запущен, пока Nessus не будет зарегистрирован и не будет выполнена загрузка подключаемых модулей. По умолчанию сервер Nessus поставляется с пустым набором подключаемых модулей. При попытке запуска сервера Nessus без подключаемых модулей будут возвращены следующие выходные данные:<br><br># **/etc/init.d/nessusd start**<br>Starting Nessus : .<br># Missing plugins. Attempting a plugin update...<br>Your installation is missing plugins. Please register and try again.<br>To register, please visit http://www.nessus.org/register/ |
| **Ubuntu 8.04, 9.10, 10.04 и 10.10 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС Ubuntu:<br><br># **dpkg -i Nessus-4.4.0-ubuntu804_i386.deb**<br># **dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb**<br># **dpkg -i Nessus-4.4.0-ubuntu910_i386.deb**<br># **dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb**<br># **dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb**<br># **dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb** |
| **Пример выходных данных** | # **dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb**<br>Selecting previously deselected package nessus.<br>(Reading database ... 32444 files and directories currently installed.)<br>Unpacking nessus (from Nessus-4.4.0-ubuntu804_amd64.deb) ...<br>Setting up nessus (4.4.0) ...<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add a user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br># |

| Solaris 10 (sparc) | |
|---|---|
| **Команда установки** | **# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz**<br>**# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg**<br><br>The following packages are available:<br>1 TNBLnessus The Nessus Network Vulnerability Scanner<br>(sparc) 4.4.0<br><br>Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:1 |
| **Пример выходных данных** | **# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz**<br>**# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg**<br><br>The following packages are available:<br>1 TNBLnessus The Nessus Network Vulnerability Scanner<br>(sparc) 4.4.0<br><br>Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:1<br>Processing package instance <TNBLnessus> from </tmp/Nessus-4.4.0-solaris-sparc.pkg><br><br>The Nessus Network Vulnerability Scanner(sparc) 4.4.0<br>## Processing package information.<br>## Processing system information.<br>## Verifying disk space requirements.<br>## Checking for conflicts with packages already installed.<br>## Checking for setuid/setgid programs.<br><br>This package contains scripts which will be executed with super-user<br>permission during the process of installing this package.<br><br>Do you want to continue with the installation of <TNBLnessus> [y,n,?]y<br>Installing The Nessus Network Vulnerability Scanner as <TNBLnessus><br><br>## Installing part 1 of 1.<br>(output redacted)<br>## Executing postinstall script.<br><br>- Please run /opt/nessus/sbin/nessus-adduser to add a user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain<br>all the newest plugins<br>- You can start nessusd by typing /etc/init.d/nessusd start<br><br>Installation of <TNBLnessus> was successful. |

| | |
|---|---|
| | # **/etc/init.d/nessusd start**<br># |
| **Примечания** | В случае возникновения ошибок совместимости библиотек убедитесь, что к системе применен последний рекомендованный кластер исправлений Solaris, загружаемый с веб-сайта Sun. |
| **FreeBSD 8 (32- и 64-разрядная)** | |
| **Команда установки** | Используйте одну из приведенных ниже необходимых команд, соответствующую версии установленной ОС FreeBSD:<br><br># **pkg_add Nessus-4.4.0-fbsd8.tbz**<br># **pkg_add Nessus-4.4.0-fbsd8.amd64.tbz** |
| **Пример выходных данных** | # **pkg_add Nessus-4.4.0-fbsd8.tbz**<br><br>nessusd (Nessus) 4.4.0 for FreeBSD<br>(C) 1998 - 2011 Tenable Network Security, Inc.<br><br>Processing the Nessus plugins...<br>[##################################################]<br><br>All plugins loaded<br><br>- Please run /usr/local/nessus/sbin/nessus-adduser to add an admin<br>  user<br>- Register your Nessus scanner at http://www.nessus.org/register/ to obtain<br>  all the newest plugins<br>- You can start nessusd by typing /usr/local/etc/rc.d/nessusd.sh start<br># |

После установки сервера Nessus рекомендуется подстроить предоставленный файл конфигурации в соответствии с собственной средой, как описано в разделе Конфигурация.

Сервер Nessus должен устанавливаться в каталог **/opt/nessus**. Однако если **/opt/nessus** является символической ссылкой, указывающей на другое расположение, это допустимо.

## Конфигурация

### *Основные каталоги сервера Nessus*

В следующей таблице приведено расположение установки и основные каталоги, используемые сервером Nessus:

| Домашний каталог сервера Nessus | Подкаталоги сервера Nessus | Назначение |
|---|---|---|
| **Распределение для ОС Unix** | | |
| **Red Hat, SuSE, Debian, Ubuntu, Solaris:** `/opt/nessus` | `./etc/nessus/` | Файлы конфигурации |
| | `./var/nessus/users/<username>/kbs/` | Сохраненная на диске пользовательская база знаний |
| **FreeBSD:** `/usr/local/nessus` | `./lib/nessus/plugins/` | Подключаемые модули Nessus |
| **Mac OS X:** `/Library/Nessus/run` | `./var/nessus/logs/` | Файлы журналов Nessus |

### *Создание пользователя Nessus*

Создайте как минимум одного пользователя Nessus, чтобы клиентские служебные программы могли входить на сервер Nessus для инициализации сканирования и извлечения результатов.

Если не указано иное, выполняйте все команды под привилегированным пользователем (root) системы.

Для проверки подлинности с помощью пароля используйте команду `nessus-adduser` для добавления пользователей. Рекомендуется, чтобы первый создаваемый пользователь был администратором.

Каждый пользователь сканера Nessus имеет набор правил, называемых «правилами пользователя», которые определяют, что может, а что не может сканировать соответствующий пользователь. По умолчанию, если правила пользователя не указаны во время создания нового пользователя Nessus, то пользователь может сканировать любой диапазон IP-адресов. Сканер Nessus поддерживает глобальный набор правил, который хранится в файле **`nessusd.rules`**. Эти правила имеют приоритет над любыми правилами отдельных пользователей. При создании правил для отдельного пользователя они дополнительно уточняют существующие глобальные правила.

```
# /opt/nessus/sbin/nessus-adduser
Login : sumi_nessus
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
       etc...) (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that sumi_nessus has the right to test. For instance, you may want
```

```
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)



Login             : sumi_nessus
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
#
```

Не являющийся администратором пользователь не может загружать подключаемые модули в сервер Nessus, не может перезапускать его удаленно (это требуется после загрузки подключаемых модулей), а также не может переопределять настройки **max_hosts/max_checks** в файле **nessusd.conf**. **Если пользователь будет использоваться консолью SecurityCenter, этот пользователь должен быть администратором.** Консоль SecurityCenter поддерживает собственный список пользователей и наборы разрешений для своих пользователей.

Один сканер Nessus может поддерживать сложную систему из многочисленных пользователей. Например, организации может требоваться, чтобы много сотрудников имели доступ к одному сканеру Nessus, но с возможностью сканирования разных диапазонов IP-адресов, что давало бы возможность сканирования ограниченных диапазонов IP-адресов только некоторым сотрудникам.

В следующем примере рассматривается создание второго пользователя сканера Nessus с проверкой подлинности при помощи пароля и правил пользователя, ограничивающих возможность сканирования этим пользователем подсети класса B 172.20.0.0/16. Дополнительные примеры и синтаксис правил пользователя см. на страницах руководства man для **nessus-adduser**.

```
# /opt/nessus/sbin/nessus-adduser
Login : tater_nessus
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
       etc...) (y/n) [n]: n
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that tater_nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax
```

```
Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
accept 172.20.0.0/16
deny 0.0.0.0/0



Login             : tater_nessus
Password          : ***********
Rules             :
accept 172.20.0.0/16
deny 0.0.0.0/0
Is that ok ? (y/n) [y] y
User added
#
```

Для просмотра страницы руководства nessus-adduser(8) man на некоторых операционных системах может потребоваться выполнение следующих команд:

```
# export MANPATH=/opt/nessus/man
# man nessus-adduser
```

В версии Nessus 4.0.x и более ранних версиях проверка подлинности между клиентом Nessus Client и сервером Nessus настраивалась с помощью сертификатов SSL. Это больше не требуется, поскольку доступ к серверу Nessus осуществляется через веб-авторизацию SSL, а не через отдельный клиент Nessus Client. Единственным исключением является проверка подлинности между консолью SecurityCenter и сервером Nessus, поскольку консоль SecurityCenter действует как клиент Nessus. Информацию о проверке подлинности сертификатов SSL для этой конфигурации см. в документации к SecurityCenter.

### *Установка кода активации подключаемого модуля*

В случае использования консоли Tenable SecurityCenter управление кодом активации (Activation Code) и обновлениями подключаемых модулей осуществляется через SecurityCenter. Для связи с консолью SecurityCenter необходимо запустить сканер Nessus, что при нормальном использовании не происходит при отсутствии действительного кода активации и подключаемых модулей. Чтобы сканер Nessus проигнорировал это требование и запустился (чтобы он мог получить обновления подключаемых модулей от SecurityCenter), выполните следующую команду:

```
# nessus-fetch --security-center
```

Сразу после выполнения приведенной выше команды **nessus-fetch** воспользуйтесь соответствующей командой для запуска сервера Nessus. Сервер Nessus теперь может быть добавлен в консоль SecurityCenter через

> веб-интерфейс SecurityCenter. Сведения о конфигурации централизованного канала подключаемых модулей для нескольких сканеров Nessus см. в документации SecurityCenter.

До первого запуска сервера Nessus необходимо предоставить код активации для загрузки текущих подключаемых модулей. Первоначальная загрузка и обработка подключаемых модулей потребует дополнительного времени, прежде чем сервер Nessus будет готов.

В зависимости от используемой службы подписки вы получили код активации, позволяющий получать подключаемые модули канала ProfessionalFeed или HomeFeed. Это синхронизирует сканер Nessus со всеми доступными подключаемыми модулями. Коды активации могут быть строками, состоящими из 16 или 20 буквенно-цифровых символов с дефисами.

Чтобы установить код активации, в системе, в которой выполняется сервер Nessus, введите следующую команду, где **<license code>** – полученный вами код регистрации:

**Linux и Solaris:**

```
# /opt/nessus/bin/nessus-fetch --register <Activation Code>
```

**FreeBSD:**

```
# /usr/local/nessus/bin/nessus-fetch --register <Activation Code>
```

> После первоначальной регистрации сервер Nessus загрузит и выполнит компиляцию подключаемых модулей, полученных с узла plugins.nessus.org, plugins-customers.nessus.org или plugins-us.nessus.org, в фоновом режиме. При первом выполнении это может занять до 10 минут, прежде чем сервер Nessus будет готов. Когда в журнале **nessusd.messages** появится сообщение «nessusd is ready» (nessusd готов), сервер Nessus начнет принимать подключения клиентов и станет доступен интерфейс сканирования. Код активации **не** учитывает регистр.

> Для этого этапа необходимо подключение к Интернету. В случае выполнения сервера Nessus на системе, не имеющей подключения к Интернету, для установки кода активации выполните действия, описанные в разделе Nessus без доступа к Интернету.

В приведенном ниже примере показаны действия, выполняемые для регистрации кода активации подключаемых модулей, получения новых подключаемых модулей с веб-сайта Nessus и проверки успешной загрузки.

```
# /opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
```

```
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200912160934";
PLUGIN_FEED = "ProfessionalFeed (Direct)";
```

Файл **plugin_feed_info.inc**, расположенный в каталоге **/opt/nessus/lib/nessus/plugins/,** проверяет, какой установлен набор подключаемых модулей и тип канала. Проверка этого файла помогает убедиться, что установлены последние подключаемые модули.

## Запуск демона Nessus

Сервер Nessus не запустится, пока сканер не будет зарегистрирован и пока не будут загружены подключаемые модули. Пользователям диспетчера SecurityCenter, которые ввели следующую команду, не потребуется предоставлять код регистрации и загружать подключаемые модули:

```
# nessus-fetch --security-center
```

Запустите службу Nessus как пользователь root с помощью следующей команды:

**Linux и Solaris:**

```
# /opt/nessus/sbin/nessus-service -D
```

**FreeBSD:**

```
# /usr/local/nessus/sbin/nessus-service -D
```

Ниже приведен пример экрана выходных данных при запуске `nessusd` для Red Hat:

```
# /opt/nessus/sbin/nessus-service -D

nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2011 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
#
```

Чтобы скрыть выходные данные команды, используйте параметр `-q` следующим образом:

**Linux и Solaris:**

```
# /opt/nessus/sbin/nessus-service -q -D
```

**FreeBSD:**

```
# /usr/local/nessus/sbin/nessus-service -q -D
```

Вместо этого службу Nessus можно запустить с помощью следующей команды, в зависимости от операционной системы:

| Операционная система | Команда для запуска `nessusd` |
|---|---|
| **Red Hat** | `# /sbin/service nessusd start` |
| **Fedora Core** | `# /sbin/service nessusd start` |
| **SuSE** | `# /etc/rc.d/nessusd start` |
| **Debian** | `# /etc/init.d/nessusd start` |
| **FreeBSD** | `# /usr/local/etc/rc.d/nessusd.sh start` |
| **Solaris** | `# /etc/init.d/nessusd start` |
| **Ubuntu** | `# /etc/init.d/nessusd start` |

После запуска службы `nessusd` для пользователей консоли SecurityCenter установка и конфигурация сканера Nessus 4 будет завершена. Если консоль SecurityCenter не используется для подключения к `nessusd`, продолжите выполнение следующих инструкций для установки кода активации подключаемых модулей.

## Остановка демона Nessus

При необходимости остановить службу `nessusd` по какой-либо причине следующая команда остановит сервер Nessus, а также прервет все текущие сканирования:

```
# killall nessusd
```

Вместо этого рекомендуется использовать более мягкие скрипты завершения работы:

| Операционная система | Команда для остановки `nessusd` |
|---|---|
| **Red Hat** | `# /sbin/service nessusd stop` |
| **Fedora Core** | `# /sbin/service nessusd stop` |
| **SuSE** | `# /etc/rc.d/nessusd stop` |

| | |
|---|---|
| **Debian** | `# /etc/init.d/nessusd stop` |
| **FreeBSD** | `# /usr/local/etc/rc.d/nessusd.sh stop` |
| **Solaris** | `# /etc/init.d/nessusd stop` |
| **Ubuntu** | `# /etc/init.d/nessusd stop` |

## Параметры командной строки Nessusd

Помимо запуска сервера `nessusd`, есть еще несколько параметров командной строки, которые могут использоваться в соответствующих случаях. Следующая таблица содержит информацию об этих дополнительных командах.

| Параметр | Описание |
|---|---|
| **`-c <config-file>`** | При запуске сервера `nessusd` этот параметр используется, чтобы указать используемый файл конфигурации на стороне сервера `nessusd`. Это позволяет использовать другой файл конфигурации вместо стандартного **`/opt/nessus/etc/nessus/nessusd.conf`** (или **`/usr/local/nessus/etc/nessus/nessusd.conf`** для FreeBSD). |
| **`-a <address>`** | При запуске сервера `nessusd` этот параметр используется для указания серверу прослушивать только соединения по адресу **`<address>`**, который является IP-адресом, а не именем машины. Этот параметр используется в случае выполнения `nessusd` на шлюзе и если вы не хотите, чтобы выполнялись подключения к вашему серверу `nessusd` извне. |
| **`-S <ip[,ip2,...]>`** | При запуске сервера `nessusd` принудительно присваивается IP-адрес источника соединений, устанавливаемых сервером Nessus во время сканирования с **`<ip>`.** Этот параметр полезен только в случае использования многосетевой машины с несколькими общими IP-адресами, которые необходимо использовать вместо адреса по умолчанию. Чтобы эта настройка сработала, хост, на котором выполняется **`nessusd`**, должен иметь несколько сетевых адаптеров с установленными соответствующими IP-адресами. |
| **`-p <port-number>`** | При запуске сервера `nessusd` этот параметр настраивает сервер на прослушивание клиентских соединений на порту **`<port-number>`** вместо прослушивания порта 1241, который прослушивается по умолчанию. |
| **`-D`** | При запуске сервера `nessusd` использование этого параметра приводит к работе сервера в фоновом режиме (режиме демона). |

| | |
|---|---|
| **-v** | Отображение номера версии и выход. |
| **-l** | Отображение информации о лицензии канала подключаемых модулей и выход. |
| **-h** | Вывод на экран сводки команд и выход. |
| **--ipv4-only** | Прослушивание только сокета IPv4. |
| **--ipv6-only** | Прослушивание только сокета IPv6. |
| **-q** | Работа в «тихом» режиме, с подавлением всех сообщений для **stdout**. |
| **-R** | Применение повторной обработки подключаемых модулей. |
| **-t** | Проверка меток времени каждого подключаемого модуля при запуске. |
| **-K** | Установка основного пароля для сканера. |

В случае установки основного пароля сканер Nessus будет шифровать все политики и содержащиеся в них учетные данные с помощью предоставленного пользователем ключа (существенно более надежно, чем использование ключа по умолчанию). В случае установки пароля веб-интерфейс будет запрашивать этот пароль при запуске.

**ВНИМАНИЕ!** В случае установки и утери основного пароля, он не может быть восстановлен вашим администратором или службой технической поддержки компании Tenable.

Пример использования приведен ниже:

**Linux:**

```
# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
```

**FreeBSD:**

```
# /usr/local/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
```

## Соединение с клиентом

После завершения установки, а также обновления и обработки подключаемых модулей сервер Nessus готов к соединению с клиентами. Компания Tenable обеспечивает доступ к серверу Nessus через собственный веб-сервер (по умолчанию порт 8834), командную строку или интерфейс SecurityCenter (рассматривается в разделе Работа с консолью SecurityCenter). Информация о доступе к веб-серверу (интерфейсу пользователя) и управлению с помощью командной строки приведена в документе «Руководство

пользователя сканера Nessus» по адресу http://www.tenable.com/products/nessus/documentation.

При первом обновлении сканера Nessus и обработке подключаемых модулей это может занять несколько минут. Веб-сервер будет доступен, но не будет разрешать выполнить вход до завершения обработки подключаемых модулей.

## Обновление подключаемых модулей

Следующая команда используется для обновления сканера Nessus последними подключаемыми модулями:

**Linux и Solaris:**

```
# /opt/nessus/sbin/nessus-update-plugins
```

**FreeBSD:**

```
# /usr/local/nessus/sbin/nessus-update-plugins
```

Поскольку новые уязвимости обнаруживаются и публикуются каждый день, новые подключаемые модули Nessus также пишутся ежедневно. Чтобы сканер Nessus пополнялся новейшими подключаемыми модулями, обеспечивая максимальную точность сканирования, необходимо часто выполнять обновление подключаемых модулей.

### *Как часто необходимо обновлять подключаемые модули?*

В общем случае, для большинства организаций достаточно обновлять подключаемые модули Nessus один раз в день. В случае совершенной необходимости использования самых новых подключаемых модулей и постоянного обновления в течение дня, достаточно выполнять обновление не чаще одного раза в четыре часа, поскольку более частое обновление практически бесполезно.

### *Автоматическое обновление подключаемых модулей*

Начиная с версии 3.0, сканер Nessus автоматически регулярно получает новейшие подключаемые модули. Это выполняется с помощью параметра **auto_update**, находящегося в файле **nessusd.conf**. Значение этого параметра по умолчанию — «yes» (да). Параметр **auto_update_delay** определяет интервал обновления подключаемых модулей Nessus в часах. По умолчанию используется значение 24. Минимальное допустимое значение — 4 часа. Обновление подключаемых модулей будет выполнено через установленное количество часов после запуска **nessusd** и будет продолжать выполняться каждые N часов после этого.

Чтобы этот параметр работал правильно, должен быть надлежащим образом зарегистрирован код активации канала подключаемых модулей сканера. Для проверки этого условия используйте следующую команду:

**Linux и Solaris:**

```
# /opt/nessus/bin/nessus-fetch --check
```

**FreeBSD:**

```
# /usr/local/nessus/bin/nessus-fetch --check
```

Попытка автоматического обновления подключаемых модулей выполняется, только если:

- Установлено значение параметра **auto_update** «yes» (да) в файле **nessusd.conf**.
- Код активации канала подключаемых модулей зарегистрирован через **nessus-fetch** с этого сканера при наличии прямого подключения к Интернету.
- Сканер не управляется удаленно с помощью Tenable SecurityCenter.

Обратите внимание, что регистрация автономного канала подключаемых модулей не обеспечивает автоматическое получение сканером Nessus новейших подключаемых модулей.

### *Планирование обновлений подключаемых модулей с помощью службы Cron*

Если в вашей организации есть технические или логистические причины, не позволяющие сканеру Nessus выполнять обновление подключаемых модулей автоматически, то можно настроить для этого задачу службы cron.

Чтобы настроить систему для обновления подключаемых модулей каждую ночь через службу cron, выполните следующие действия:

- Станьте пользователем root, введя **su root** (или **sudo bash** при наличии у вас привилегий sudo).
- В качестве пользователя root введите **crontab -e** для правки таблицы crontab пользователя root.
- Добавьте следующую строку в свою таблицу crontab:
  ```
  28 3 * * * /opt/nessus/sbin/nessus-update-plugins
  ```

Приведенная выше конфигурация будет вызывать команду **nessus-update-plugins** каждую ночь в 3:28. Поскольку команда **nessus-update-plugins** автоматически перезапускает службу **nessusd**, не прерывая текущие сканирования, больше ничего делать не требуется.

При настройке службы cron для обновления подключаемых модулей убедитесь в том, что **обновление не инициализируется точно в начале часа.** При настройке расписания выберите случайное количество минут после начала часа, от :05 до :55 для инициализации загрузки в это время.

Начиная с версии 4.4 сканер Nessus может обновлять подключаемые модули в процессе выполнения сканирования. После завершения обновления любые последующие сканирования будут использовать обновленный набор подключаемых модулей. Пользователь не обязан выходить из веб-интерфейса во время этого процесса.

### *Обновление подключаемых модулей через веб-прокси*

Сканер Nessus на ОС Unix поддерживает регистрацию продукта и обновление подключаемых модулей через веб-прокси, требующие обычной проверки подлинности. Настройки прокси находятся в файле **/opt/nessus/etc/nessus/nessus-fetch.rc**. Есть четыре соответствующих строки, управляющих соединениями через прокси. Ниже приведены эти строки с примером синтаксиса:

```
proxy=myproxy.example.com
proxy_port=8080
proxy_username=juser
proxy_password=squirrel
```

Для директивы **proxy** может использоваться имя DNS-узла или IP-адрес. В файле **nessus-fetch.rc** может быть указан только один прокси-сервер. Кроме того, при необходимости может использоваться директива **user_agent**, которая указывает серверу Nessus использовать настраиваемый пользователем агент обработки HTTP.

## Удаление сервера Nessus

В следующей таблице представлены инструкции по удалению сервера Nessus для всех поддерживаемых платформ. За исключением инструкций, относящихся к Mac OS X, выполнение всех приведенных инструкций не приведет к удалению файлов конфигурации или файлов, не входивших в исходную установку. Файлы, которые входили в исходный пакет, но были изменены после установки, также не будут удалены. Для полного удаления остающихся файлов используйте следующую команду:

**Linux и Solaris:**

```
# rm -rf /opt/nessus
```

**FreeBSD:**

```
# rm -rf /usr/local/nessus/bin
```

| Платформа | Инструкции по удалению |
|---|---|
| **Red Hat ES 4 (32-разрядная), ES 5 (32- и 64-разрядная)** | |
| **Команда удаления** | Определение имени пакета:<br><br>`# rpm -qa \| grep Nessus`<br><br>Используйте результат выполнения приведенной выше команды для удаления пакета:<br><br>`# rpm -e <Имя пакета>` |
| **Пример выходных данных** | `# rpm -qa \| grep -i nessus`<br>`Nessus-4.4.0-es5`<br>`# rpm -e Nessus-4.4.0-es5`<br>`#` |

| Fedora Core 12, 13 и 14 (32- и 64-разрядная) | |
|---|---|
| **Команда удаления** | Определение имени пакета:<br><br>`# rpm -qa \| grep Nessus`<br><br>Используйте результат выполнения приведенной выше команды для удаления пакета:<br><br>`# rpm -e <Имя пакета>` |
| **SuSE 9.3 (32-разрядная), 10 (32- и 64-разрядная)** | |
| **Команда удаления** | Определение имени пакета:<br><br>`# rpm -qa \| grep Nessus`<br><br>Используйте результат выполнения приведенной выше команды для удаления пакета:<br><br>`# rpm -e <Имя пакета>` |
| **Debian 5 (32- и 64-разрядная)** | |
| **Команда удаления** | Определение имени пакета:<br><br>`# dpkg -l \| grep -i nessus`<br><br>Используйте результат выполнения приведенной выше команды для удаления пакета:<br><br>`# dpkg -r <Имя пакета>` |
| **Пример выходных данных** | `# dpkg -l \| grep nessus`<br>`ii  nessus  4.4.0  Version 4 of the Nessus Scanner`<br><br>`# dpkg -r nessus`<br>`#` |
| **Ubuntu 8.04, 9.10, 10.04 и 10.10 (32- и 64-разрядная)** | |
| **Команда удаления** | Определение имени пакета:<br><br>`# dpkg -l \| grep -i nessus`<br><br>Используйте результат выполнения приведенной выше команды для удаления пакета:<br><br>`# dpkg -r <Имя пакета>` |
| **Пример выходных** | `# dpkg -l \| grep -i nessus`<br>`ii  nessus  4.4.0  Version 4 of the Nessus` |

| | |
|---|---|
| **данных** | Scanner<br># |
| **Solaris 10 (sparc)** | |
| **Команда удаления** | Остановка службы **nessusd:**<br><br># **/etc/init.d/nessusd stop**<br><br>Определение имени пакета:<br><br># **pkginfo \| grep –i nessus**<br><br>Удаление пакета Nessus:<br><br># **pkgrm <Имя пакета>** |
| **Пример выходных данных** | Следующие выходные данные, получаемые в результате применения предыдущей команды, содержат сведения о пакете Nessus:<br><br># **pkginfo \| grep –i nessus**<br><br>application TNBLnessus The Nessus Network Vulnerability Scanner<br># **pkgrm TNBLnessus**<br># |
| **FreeBSD 8 (32- и 64-разрядная)** | |
| **Команда удаления** | Остановка сервера Nessus:<br><br># **killall nessusd**<br><br>Определение имени пакета:<br><br># **pkg_info \| grep -i nessus**<br><br>Удаление пакета Nessus:<br><br># **pkg_delete <Имя пакета>** |
| **Пример выходных данных** | # **killall nessusd**<br><br># **pkg_info \| grep -i nessus**<br>Nessus-4.4.0 A powerful security scanner<br># **pkg_delete Nessus-4.4.0**<br># |
| **Mac OS X** | |
| **Команда удаления** | Запустите окно терминала. В папке «Applications» (приложения) щелкните «Utilities» (служебные программы), а |

| | |
|---|---|
| | затем «Terminal» (терминал) или «X11». В командной строке с помощью команды sudo запустите оболочку root и удалите каталоги Nessus следующим образом:<br><br>`$ sudo /bin/sh`<br>`Password:`<br>`# ls -ld /Library/Nessus`<br>`# rm -rf /Library/Nessus`<br>`# ls -ld /Library/Nessus`<br>`# ls -ld /Applications/Nessus`<br>`# rm -rf /Applications/Nessus`<br>`# ls -ld /Applications/Nessus`<br>`# ls -ld /Library/Receipts/Nessus*`<br>`# rm -rf /Library/Receipts/Nessus*`<br>`# ls -ld /Library/Receipts/Nessus*`<br>`# exit` |
| **Пример выходных данных** | `$ sudo /bin/sh`<br>`Password:`<br>`# ls -ld /Library/Nessus`<br>`drwxr-xr-x  6 root  admin  204 Apr  6 15:12 /Library/Nessus`<br>`# rm -rf /Library/Nessus`<br>`# ls -ld /Library/Nessus`<br>`ls: /Library/Nessus: No such file or directory`<br>`# ls -ld /Applications/Nessus`<br>`drwxr-xr-x  4 root  admin  136 Apr  6 15:12 /Applications/Nessus`<br>`# rm -rf /Applications/Nessus`<br>`# ls -ld /Applications/Nessus`<br>`# ls -ld /Library/Receipts/Nessus*`<br>`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Client.pkg`<br>`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Server.pkg`<br>`# rm -rf /Library/Receipts/Nessus*`<br>`# ls -ld /Library/Receipts/Nessus*`<br>`ls: /Library/Receipts/Nessus*: No such file or directory`<br>`# exit`<br>`$` |
| **Примечания** | Не пытайтесь выполнить эту процедуру при отсутствии знаний об использовании команд оболочки Unix. Команды **ls** включены для проверки правильности ввода пути и имени. |

# WINDOWS

## Обновление

### *Обновление Nessus версий 4.0 – 4.0.x*

При обновлении сервера Nessus с версии 4.x до более новых версий 4.x пользователю будет задан вопрос о том, необходимо ли удалить все содержимое каталога Nessus. При выборе этого варианта (ответе Yes (да)) будет инициализирован процесс удаления. В

случае выбора этого варианта ранее созданные пользователи, существующие политики и результаты сканирования будут удалены, а регистрация сканера будет отменена.

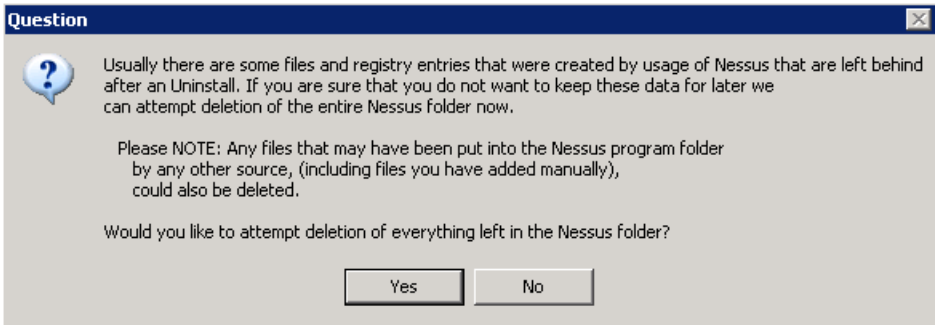
### *Обновление Nessus версий 3.0 – 3.0.x*

Непосредственное обновление сервера Nessus 3.0.x до версии Nessus 4.x не поддерживается. Однако можно использовать обновление до версии 3.2 в качестве промежуточного шага для обеспечения сохранения необходимых настроек и политик сканирования. Если настройки сохранять не требуется, сначала удалите Nessus 3.x, а затем установите новый экземпляр Nessus 4.

В случае выбора обновления до версии 3.2 в качестве промежуточного шага, изучите дополнительную информацию в Руководстве по установке Nessus 3.2.

### *Обновление Nessus версии 3.2 и более поздних версий*

В случае использования Nessus 3.2 или более поздних версий можно загрузить пакет Nessus 4 и установить его без удаления существующей версии. Все предыдущие отчеты о сканировании уязвимостей и политики при необходимости можно сохранить и не удалять. В процессе обновления появится следующий запрос, дающий возможность пользователю сохранить или удалить предыдущую установку:




Щелкните Yes (да), чтобы разрешить серверу Nessus попытаться удалить всю папку Nessus с любыми добавленными вручную файлами, или No (нет), чтобы сохранить папку Nessus со всеми существующими сканированиями, отчетами и т. д. После установки новой версии Nessus они будут доступны для просмотра и экспорта.

Внимание! При выборе ответа Yes (да) будут удалены все файлы, находящиеся в папке Nessus, включая файлы журналов, добавленные вручную пользовательские подключаемые модули и прочее. Будьте внимательны при этом выборе!

## Установка

### *Загрузка Nessus*

Последняя версия сервера Nessus доступна по адресу http://www.nessus.org/download/. Версия Nessus 4.4 доступна для ОС Windows XP, Server 2003, Server 2008, Vista и Windows 7. Проверьте целостность установочного пакета путем сравнения контрольной суммы MD5 загрузки с контрольной суммой, указанной в файле `MD5.asc`, находящемся здесь.

Размеры файлов и имена пакетов Nessus немного отличаются в зависимости от выпуска, но примерно составляют 12 МБ.

### Установка

Сервер Nessus распространяется в виде исполняемого установочного файла. Поместите файл в систему, на которую он устанавливается, или на общий диск, доступный для этой системы.

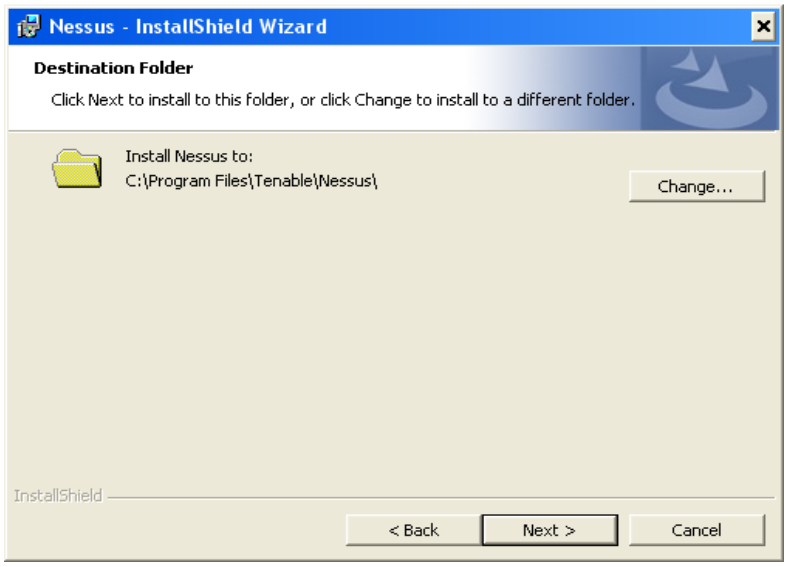
Установку сервера Nessus необходимо выполнять под учетной записью администратора, а не обычного пользователя. В случае получения каких-либо ошибок, связанных с разрешениями пользователя, отказа в доступе или ошибок, предположительно связанных с недостаточными правами, проверьте, используется ли учетная запись с правами администратора. В случае получения этих ошибок при использовании служебных программ командной строки запустите **`cmd.exe`** при помощи команды «Запуск от имени...» с правами администратора.

Некоторые пакеты антивирусного программного обеспечения могут классифицировать сервер Nessus как червь или другую форму вредоносного программного обеспечения. Это происходит из-за большого количества соединений TCP, генерируемых при сканировании. Если появится предупреждение используемого вами антивирусного программного обеспечения, нажмите в окне предупреждения кнопку «разрешить», чтобы сервер Nessus мог продолжить сканирование. Большинство пакетов антивирусного ПО также позволяют добавлять процессы в список исключений. Добавьте **`Nessus.exe`** и **`Nessus-service.exe`** в этот список, чтобы избежать предупреждений.

### Вопросы об установке

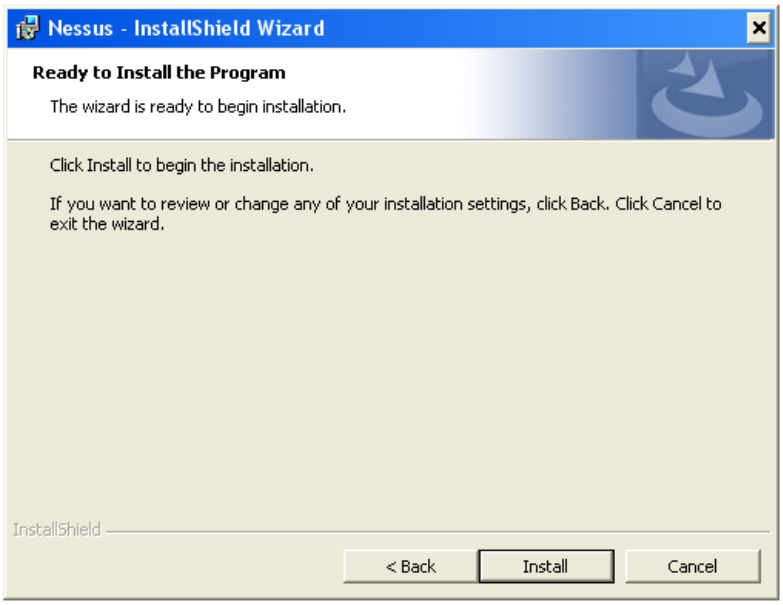

В процессе установки сервер Nessus запрашивает у пользователя некоторую основную информацию. До начала установки необходимо согласиться с условиями лицензионного соглашения:


После дачи согласия можно настроить расположение для установки сервера Nessus:



Когда будет предложено выбрать Setup Type (тип установки), выберите Complete (полный):


Вам будет предложено подтвердить установку:



После завершения установки нажмите кнопку Finish (готово):


### *Основные каталоги сервера Nessus*

| Домашний каталог сервера Nessus | Подкаталоги сервера Nessus | Назначение |
|---|---|---|
| **Windows** | | |
| **\Program Files\Tenable\Nessus** | **\conf** | Файлы конфигурации |
| | **\data** | Шаблоны таблиц стилей |
| | **\nessus\plugins** | Подключаемые модули Nessus |
| | **\nessus\users\<username>\kbs** | Сохраненная на диске пользовательская база знаний |
| | **\nessus\logs** | Файлы журналов Nessus |

Если необходимое дисковое пространство для ведения журналов существует за пределами файловой системы **/opt**, смонтируйте необходимый каталог для установки с помощью команды **mount --bind <olddir> <newdir>** или соответствующего синтаксиса для вашего пакета. Использование для этого символьных ссылок не допускается.

## Конфигурация

В этом разделе описывается порядок конфигурации сервера Nessus 4 на ОС Windows.

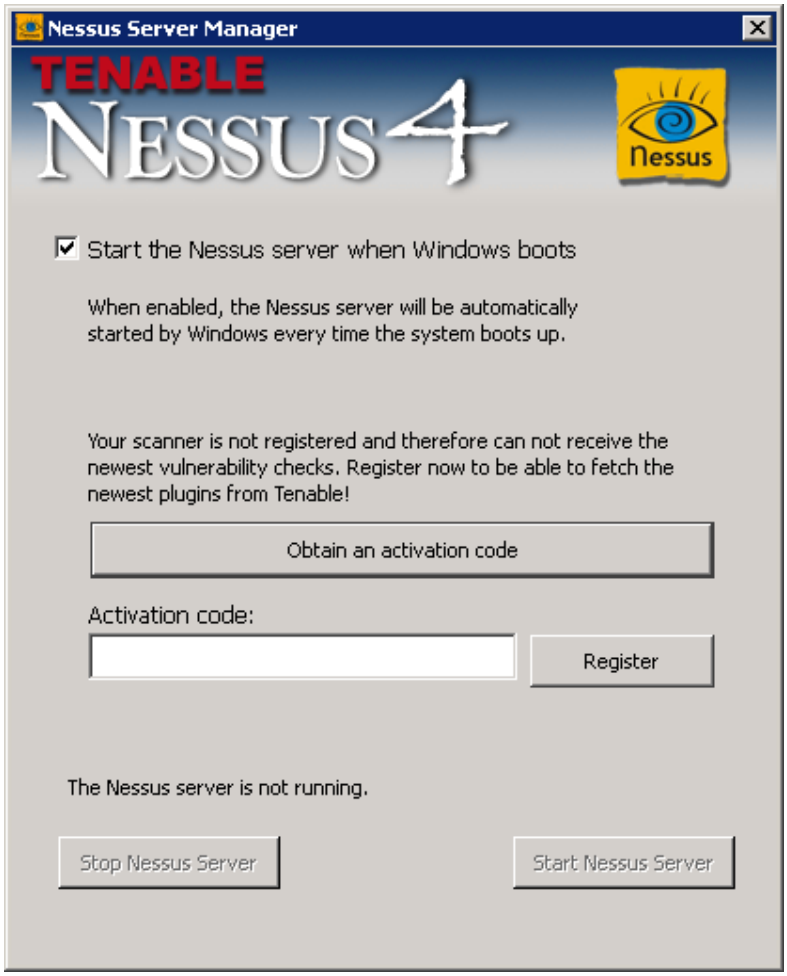
### *Nessus Server Manager*

Для запуска, остановки и настройки сервера Nessus используйте Nessus Server Manager (диспетчер сервера Nessus).

Этот интерфейс позволяет:

- зарегистрировать сервер Nessus на узле nessus.org для получения обновленных подключаемых модулей;
- выполнять обновление подключаемых модулей;
- настроить запуск или отсутствие запуска сервера Nessus при запуске ОС Windows;
- управлять пользователями сервера Nessus;
- запускать и останавливать сервер Nessus.

Запустите диспетчер Nessus Server Manager через меню «Пуск» следующим образом: **Пуск** -> **Программы** -> **Tenable Network Security** -> **Nessus** -> **Nessus Server Manager**. При этом будет загружен диспетчер Nessus Server Manager (**`nessussvrmanager.exe`**), как показано ниже:



Кнопка Start Nessus Server (запустить сервер Nessus) будет недоступна, пока сервер Nessus не будет зарегистрирован.

### *Изменение порта Nessus по умолчанию*

Для изменения порта, который прослушивается сервером Nessus, внесите изменение в файл **nessusd.conf**, расположенный в **C:\Program Files\Tenable\Nessus\conf\.** Для изменения прослушивателя службы Nessus и предпочтений веб-сервера можно внести правки в следующие директивы конфигурации:

```
# Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient
# connections :
listen_port = 1241

# Port for the Nessus Web Server to listen to (new XMLRPC protocol) :
xmlrpc_listen_port = 8834
```

После изменения этих значений остановите службу Nessus с помощью диспетчера Nessus Server Manager и запустите ее снова.

Использование устаревшего клиента через протокол NTP доступно только пользователям канала ProfessionalFeed.

### *Регистрация установки сервера Nessus*

В случае использования диспетчера Tenable SecurityCenter управление кодом активации (Activation Code) и обновлениями подключаемых модулей осуществляется через консоль SecurityCenter. Для связи с SecurityCenter необходимо запустить сканер Nessus, что при нормальном использовании не происходит при отсутствии действительного кода активации и подключаемых модулей. Чтобы сканер Nessus проигнорировал это требование и запустился (чтобы он мог получить информацию от SecurityCenter), выполните следующую команду из командной строки MS-DOS:

```
C:\Program Files\Tenable\Nessus>nessus-fetch --security-center
```

Сразу после выполнения команды **nessus-fetch**, приведенной выше, воспользуйтесь диспетчером служб Windows для запуска Nessus. Сервер Nessus теперь может быть добавлен в консоль SecurityCenter через веб-интерфейс SecurityCenter. Сведения о конфигурации централизованного канала подключаемых модулей для нескольких сканеров Nessus см. в документации SecurityCenter.

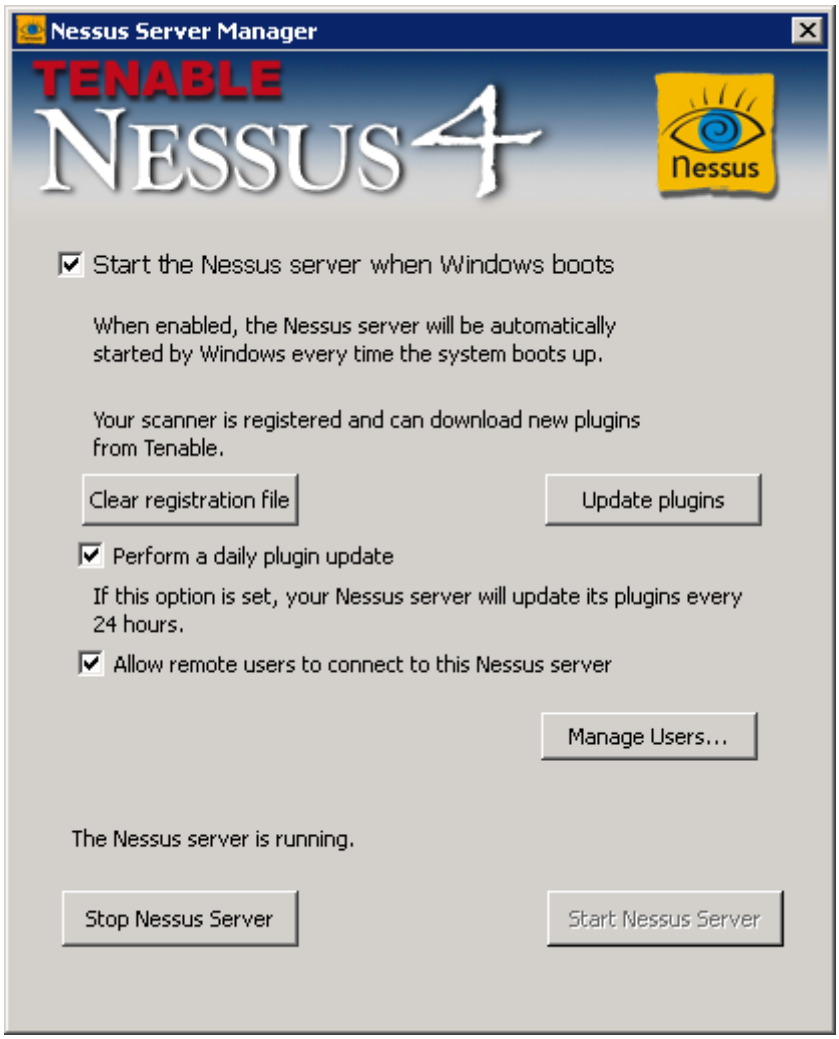
После установки сначала необходимо зарегистрировать сервер Nessus. Регистрация сервера дает доступ к последним подключаемым модулям на узле nessus.org и обеспечивает своевременное обновление аудитов.

После первоначальной регистрации сервер Nessus загрузит и выполнит компиляцию подключаемых модулей, полученных с узла plugins.nessus.org, в фоновом режиме. При первом выполнении это может занять до 10 минут, прежде чем сервер Nessus будет готов. Интерфейс веб-сервера будет недоступен до завершения загрузки и компиляции подключаемых модулей. Код активации **не** учитывает регистр.

Для регистрации сервера Nessus щелкните Obtain an activation code (получить код активации). При этом будет выполнен переход на страницу http://www.nessus.org/plugins/?view=register-info. Здесь можно подписаться на канал ProfessionalFeed или HomeFeed. Подписка на канал ProfessionalFeed необходима для коммерческого использования и предлагает обновление подключаемых модулей, техническую поддержку клиентов, аудиты конфигураций, виртуальную машину и многое другое. Подписка на канал HomeFeed требуется для домашних пользователей, она не предоставляет лицензии на профессиональное или коммерческое использование. После предоставления и обработки необходимой информации вы получите сообщение электронной почты с кодом активации, который дает право на пользование каналом подключаемых модулей ProfessionalFeed или HomeFeed. Введите код активации в соответствующее поле и нажмите кнопку Register (регистрация). Обратите внимание, что вам будет предложено ввести имя пользователя и пароль администратора. После подтверждения подлинности кода активации диспетчером Nessus Server Manager начнется обновление подключаемых модулей Nessus. Этот процесс может занять несколько минут, поскольку начальная загрузка подключаемых модулей представляет собой большой файл.

При отсутствии регистрации сервера Nessus невозможно получать новые подключаемые модули и невозможно запустить сервер Nessus.

После регистрации интерфейс диспетчера Nessus Server Manager отобразит следующее диалоговое окно:




Примечание. Сервер Nessus также можно запускать из командной строки:

```
C:\Windows\system32>net stop "Tenable Nessus"
The Tenable Nessus service is stopping.
The Tenable Nessus service was stopped successfully.


C:\Windows\system32>net start "Tenable Nessus"
The Tenable Nessus service is starting.
The Tenable Nessus service was started successfully.


C:\Windows\system32>
```

### Изменение кодов активации

В какой-то момент вам может потребоваться изменить коды активации (например, при переходе с канала HomeFeed на канал ProfessionalFeed). Это можно выполнить с

помощью кнопки Clear registration file (очистить файл регистрации) в интерфейсе диспетчера Nessus Server Manager. После подтверждения будет выполнена отмена регистрации экземпляра Nessus до получения нового кода активации и повторной регистрации продукта.

## *Создание и управление пользователями Nessus*

### Разрешение удаленных соединений

Если предполагается использовать сканер Nessus удаленно (например, с помощью SecurityCenter), необходимо установить флажок **Allow remote users to connect to this server** (разрешать удаленным пользователям подключение к этому серверу).

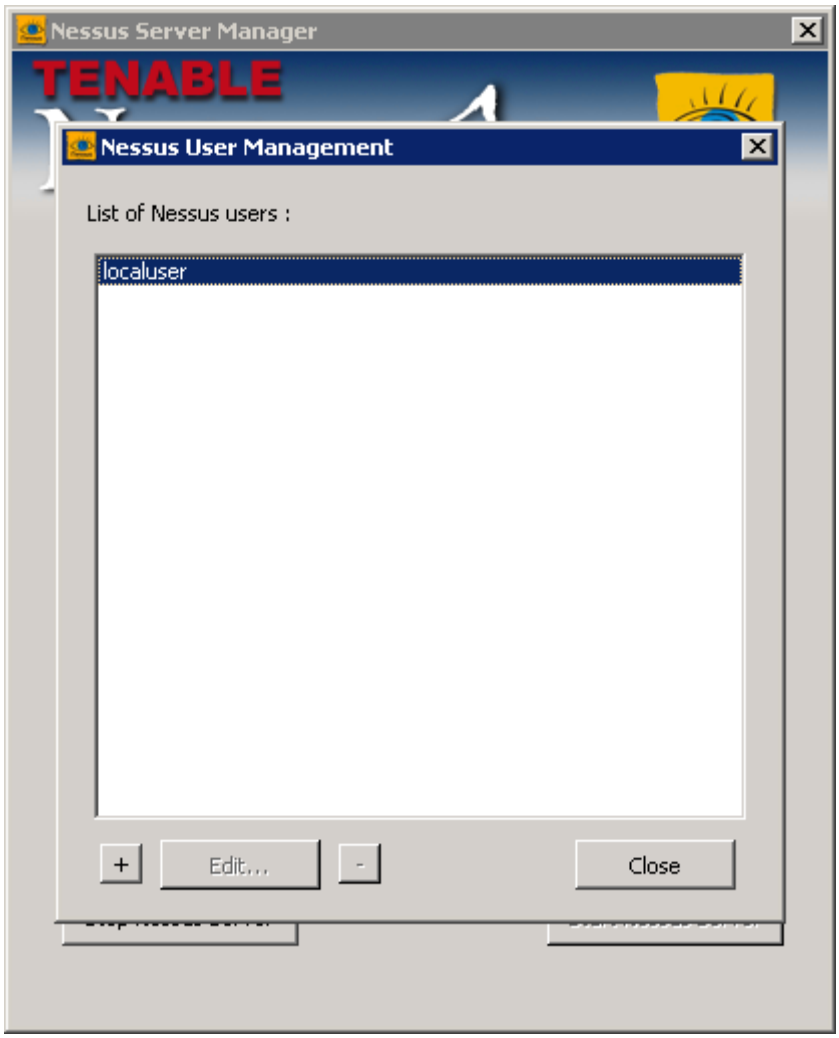
Если этот флажок снят, сервер Nessus будет доступен только для локальных клиентов.

Если этот флажок установлен, доступ к серверу Nessus будет возможен с помощью клиентов, установленных на этом же компьютере, удаленном хосте или с помощью интерфейса SecurityCenter (этот вариант рассматривается ниже в настоящем документе в разделе Работа с SecurityCenter).

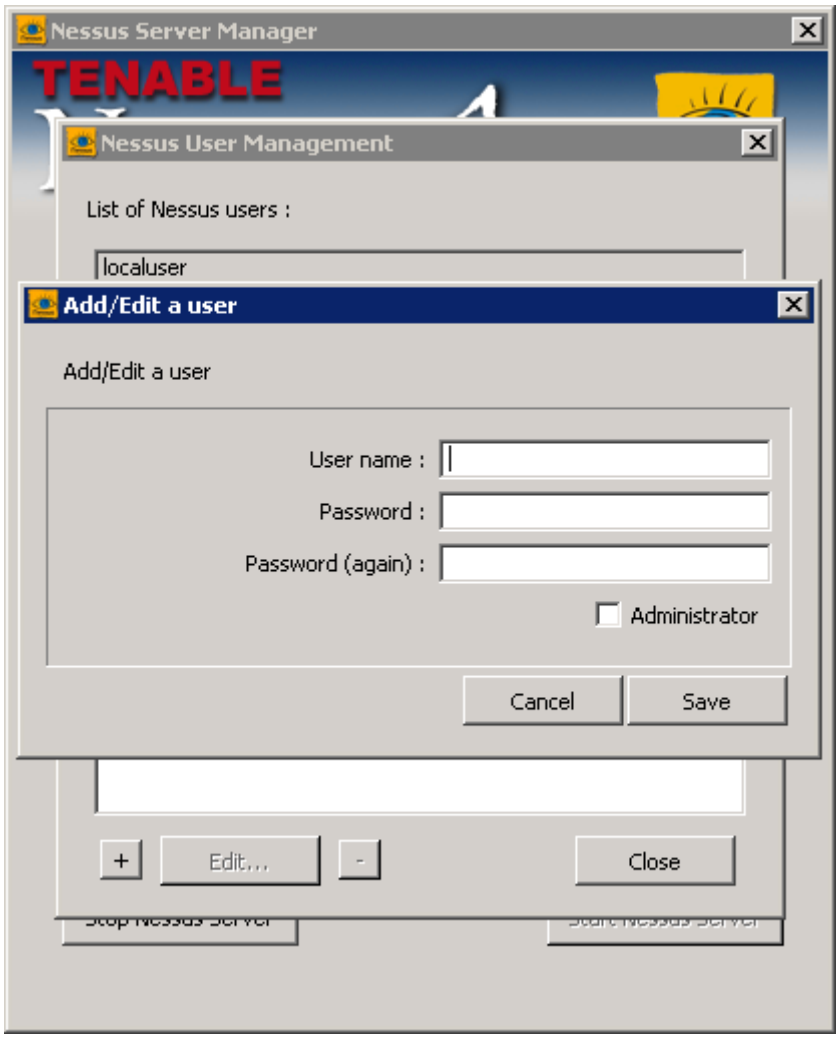
Информация о клиентах Nessus приведена в документе «Руководство пользователя Nessus 4.4».

### Добавление учетных записей пользователей

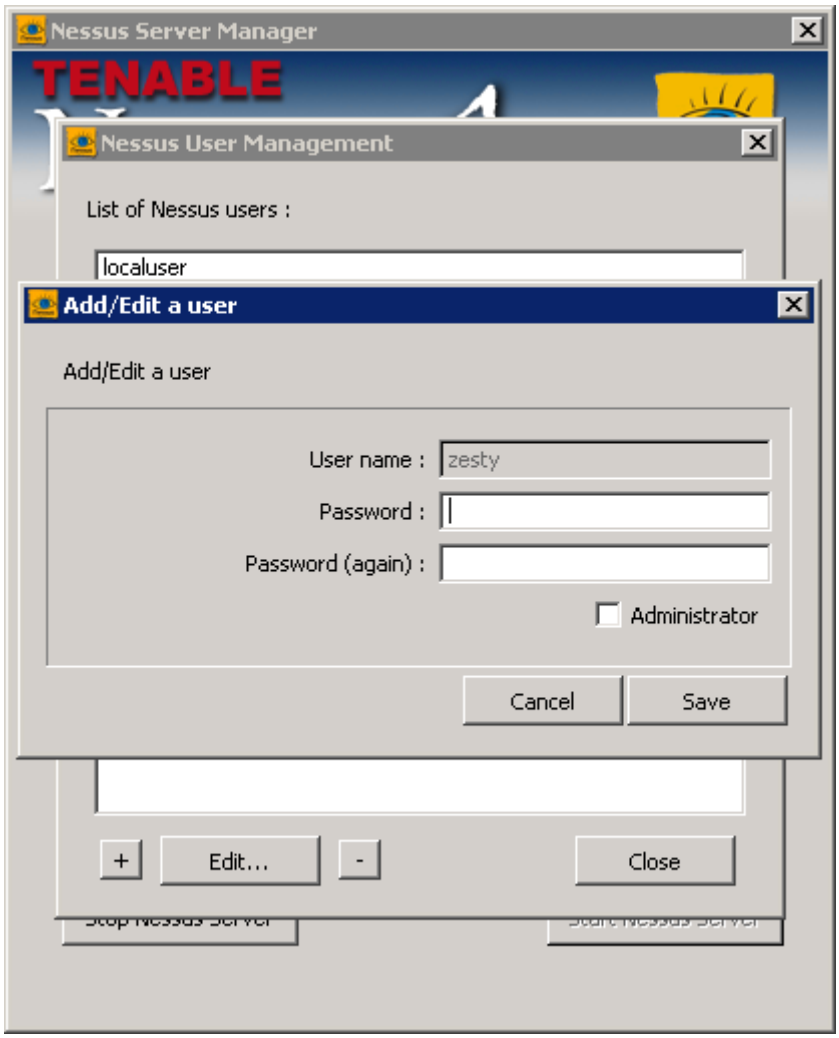
Нажатие кнопки Manage Users… (управление пользователями...) позволяет создавать и управлять учетными записями сервера Nessus:




Для создания пользователя нажмите кнопку «+» и введите новое имя пользователя и пароль. Установите флажок Administrator (администратор), если пользователь будет администратором:




Выбрав имя из списка и нажав кнопку Edit… (правка...), можно изменить пароль соответствующего пользователя (см. приведенный ниже снимок экрана). При выборе пользователя и нажатии кнопки «-» соответствующий пользователь будет удален после подтверждения.




Изменить имя пользователя невозможно. При необходимости изменить имя пользователя удалите существующего пользователя и создайте нового с нужным именем.

Обратите внимание, что сервер Nessus использует внутреннюю административную учетную запись для локальной связи графического интерфейса пользователя Nessus со службой Tenable Nessus Service. Эта учетная запись не может использоваться для удаленного соединения клиента Nessus.

### Установленные на хосте брандмауэры

Если сервер Nessus установлен на хосте с «личным» брандмауэром, например Zone Alarm, Sygate, брандмауэр ОС Windows XP или иное аналогичное ПО, необходимо разрешить подключения к нему с IP-адреса клиента Nessus.

По умолчанию для веб-сервера Nessus Web Server (интерфейс пользователя) используется порт 8834. В ОС Microsoft XP с пакетом обновлений 2 (SP2) и более поздних версиях щелчок по значку **Security Center** (центр обеспечения безопасности),

находящемуся на **панели управления**, дает возможность управления настройками Брандмауэра Windows. Чтобы открыть порт 8834, выберите вкладку **Exceptions** (исключения) и добавьте в список порт 8834.

В случае использования другого личного брандмауэра инструкции по настройке см. в соответствующей документации.

### *Запуск демона Nessus*

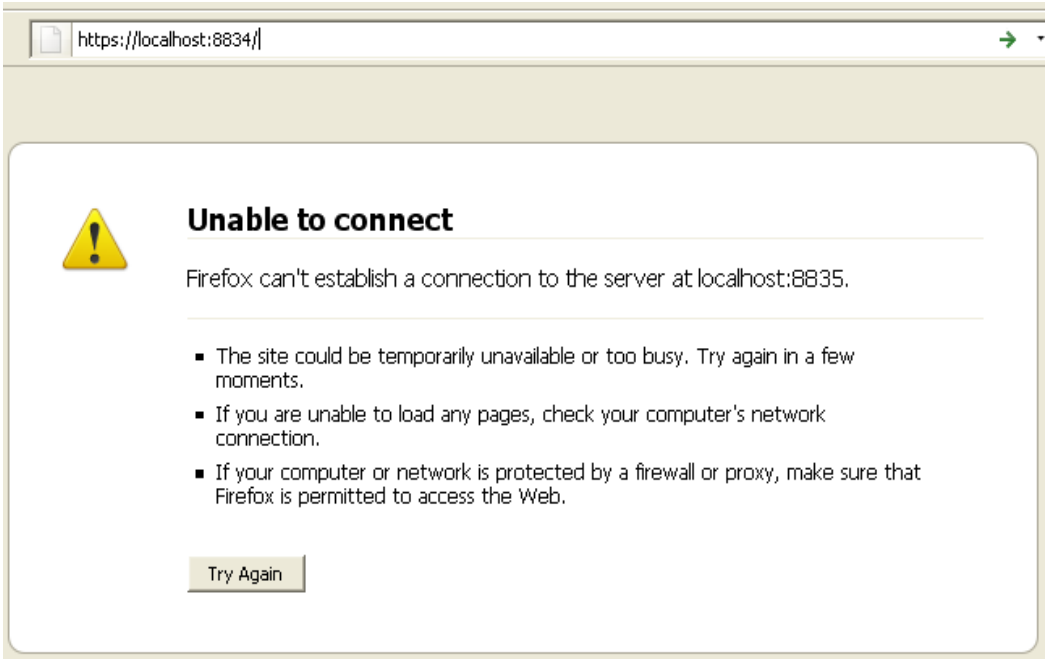
Для запуска демона Nessus нажмите кнопку **Start Nessus Server** (запустить сервер Nessus) в диспетчере Nessus Server Manager.

Для автоматического запуска сервера Nessus установите флажок **Start the Nessus Server when Windows boots** (запускать сервер Nessus при загрузке Windows).

Сервер Nessus под ОС Windows устанавливается как служба Tenable Nessus, и настраивается ее автоматический запуск при перезагрузке системы. Эта настройка выполняется с помощью флажка Start the Nessus Server when Windows boots (запускать сервер Nessus при загрузке Windows).

После запуска службы `nessusd` для пользователей консоли SecurityCenter начальная установка и конфигурация сканера Nessus 4 будет завершена. Они могут перейти к разделу Работа с SecurityCenter.

Если демон Nessus не запущен или интерфейс пользователя недоступен, веб-браузер выдаст сообщение об ошибке при установлении соединения:



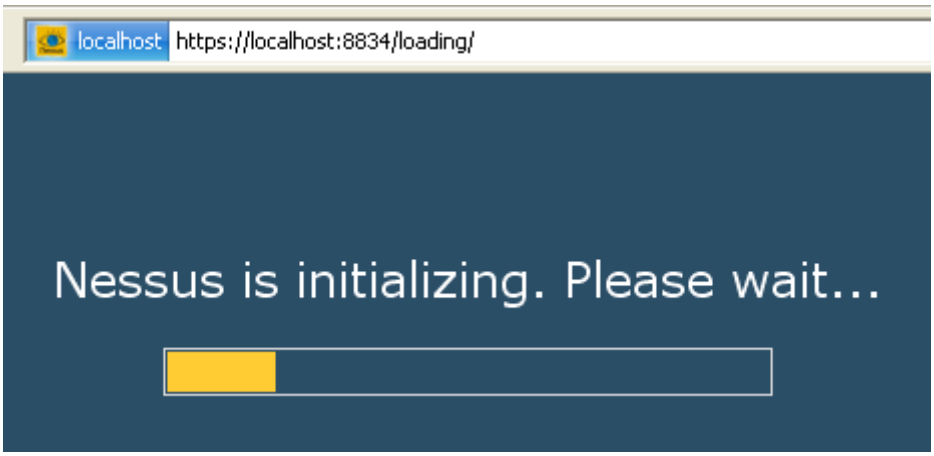

Сервер Nessus будет выполняться на localhost (127.0.0.1) и по умолчанию прослушивать устаревшие клиенты на порту 1241. Для проверки того, прослушивает ли сканер Nessus порт 1241, из командной строки Windows выполните команду **`netstat -an | findstr 1241`**, как показано ниже:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Обратите внимание, что выходные данные содержат адрес «0.0.0.0:1241». Это означает, что сервер прослушивает данный порт. Эта же команда может использоваться для проверки доступности веб-сервера (интерфейса пользователя), если заменить в ней 1241 на 8834.

Обратите внимание на то, что служба Nessus Service запускается автоматически только после установки **и** обновления подключаемых модулей.

При первом обновлении сканера Nessus и обработке подключаемых модулей это может занять несколько минут. Веб-сервер отобразит сообщение «Nessus is initializing...» (выполняется инициализация Nessus) и выполнит перезагрузку, когда будет готов.

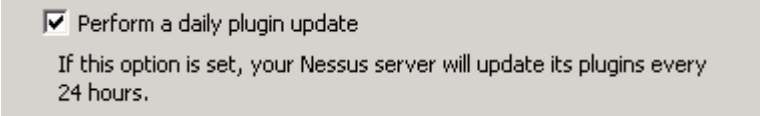



При первом подключении к веб-интерфейсу браузер может выдать предупреждение о ненадежном соединении. Это объясняется тем, что сервер Nessus поставляется с сертификатом SSL по умолчанию. Дополнительные сведения об этом приведены в Руководстве пользователя Nessus.

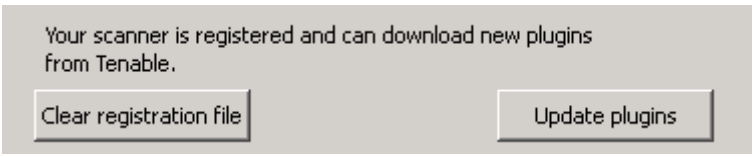
## Обновление подключаемых модулей

Сервер Nessus включает тысячи подключаемых модулей (или скриптов), которые выполняют тестирование уязвимостей сети и хостов. Новые уязвимости обнаруживаются постоянно, и для обнаружения этих уязвимостей разрабатываются новые подключаемые модули. Чтобы сканер Nessus пополнялся новейшими подключаемыми модулями, обеспечивая максимальную точность сканирования, вам необходимо ежедневно выполнять обновление подключаемых модулей.

Флажок **Perform a daily plugin update** (выполнять ежедневное обновление подключаемых модулей) настраивает сервер Nessus для автоматического обновления подключаемых модулей с узла Tenable каждые 24 часа. Это происходит примерно в то время суток, когда был запущен сервер Nessus.




Запустить обновление подключаемых модулей можно нажатием кнопки **Update Plugins** (обновить подключаемые модули), как показано ниже:




### *Как часто необходимо обновлять подключаемые модули?*

В общем случае, для большинства организаций достаточно обновлять подключаемые модули Nessus один раз в день. В случае совершенной необходимости использования самых новых подключаемых модулей и постоянного обновления в течение дня, достаточно выполнять обновление не чаще одного раза в четыре часа, поскольку более частое обновление практически бесполезно.

### *Обновление подключаемых модулей через веб-прокси*

Сканер Nessus на ОС Windows поддерживает регистрацию продукта и обновление подключаемых модулей через веб-прокси, требующие обычной проверки подлинности. Настройки прокси находятся в **файле** **`C:\Program Files\Tenable\Nessus\conf\nessus-fetch.rc`**. Есть четыре соответствующих строки, управляющих соединениями через прокси. Ниже приведены эти строки с примером синтаксиса:

```
proxy=myproxy.example.com
proxy_port=8080
proxy_username=juser
proxy_password=guineapig
```

Для директивы **`proxy`** может использоваться имя DNS-узла или IP-адрес. В файле **`nessus-fetch.rc`** может быть указан только один прокси-сервер. Кроме того, при необходимости может использоваться директива **`user_agent`**, которая указывает серверу Nessus использовать настраиваемый пользователем агент обработки HTTP.

Начиная с версии Nessus 4.2, сканеры под ОС Microsoft Windows поддерживают проверку подлинности прокси, включая NTLM.

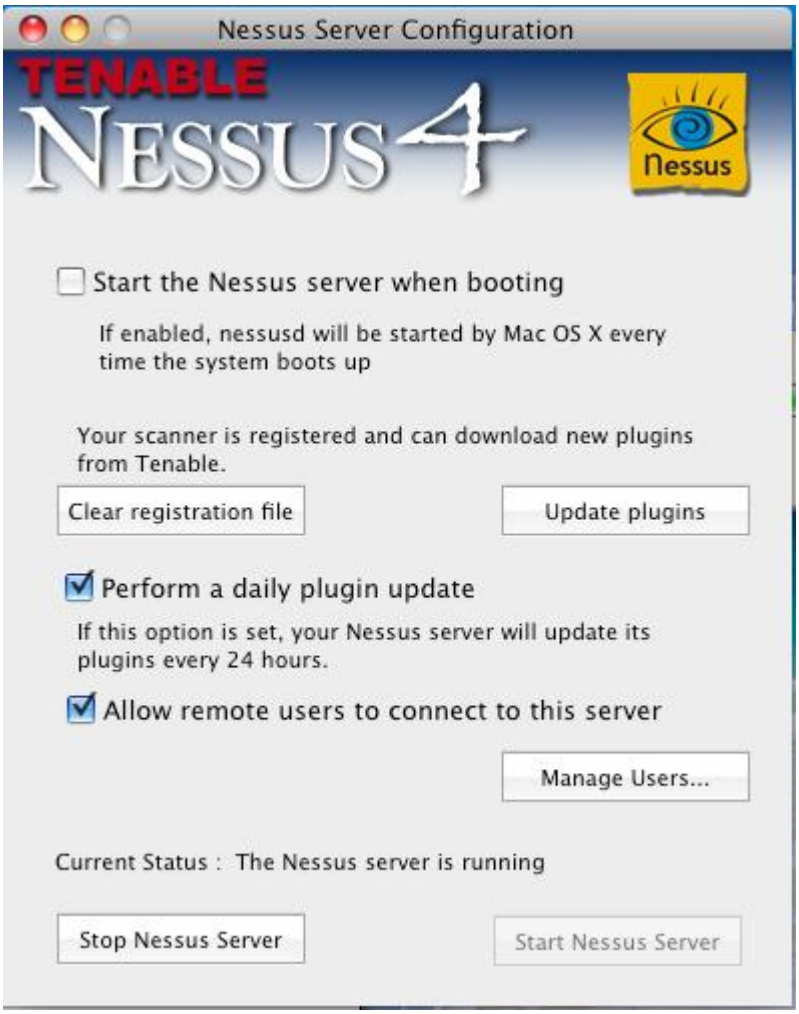
## Удаление сервера Nessus

Для удаления сервера Nessus на панели управления щелкните **Add or Remove Programs** (установка и удаление программ). Выберите **Tenable Nessus** и нажмите кнопку **Change/Remove** (изменить/удалить). При этом откроется мастер InstallShield Wizard. Выполните указания этого мастера для полного удаления Nessus. Вам будет задан вопрос, хотите ли вы удалить всю папку Nessus. Ответьте Yes (да), только если не хотите сохранять какие-либо результаты сканирования и политики, которые были созданы.

# MAC OS X

## Обновление

Обновление более старых версий Nessus выполняется аналогично новой установке. Однако в конце установки необходимо будет остановить и перезапустить сервер Nessus. Загрузите файл **`Nessus-4.x.x.dmg.gz`** и щелкните его двойным щелчком мыши для развертывания архива. Щелкните двойным щелчком файл **`Nessus-4.x.x.dmg`**, в результате чего будет смонтирован образ диска, который появится в списке Devices (устройства) в обозревателе Finder. После появления тома Nessus 4 в обозревателе Finder щелкните двойным щелчком файл `Nessus 4`. После завершения установки перейдите в каталог **`/Applications/Nessus/`** и запустите диспетчер Nessus Server Manager. Для завершения обновления необходимо нажать кнопку Update Plugins" (обновить подключаемые модули):



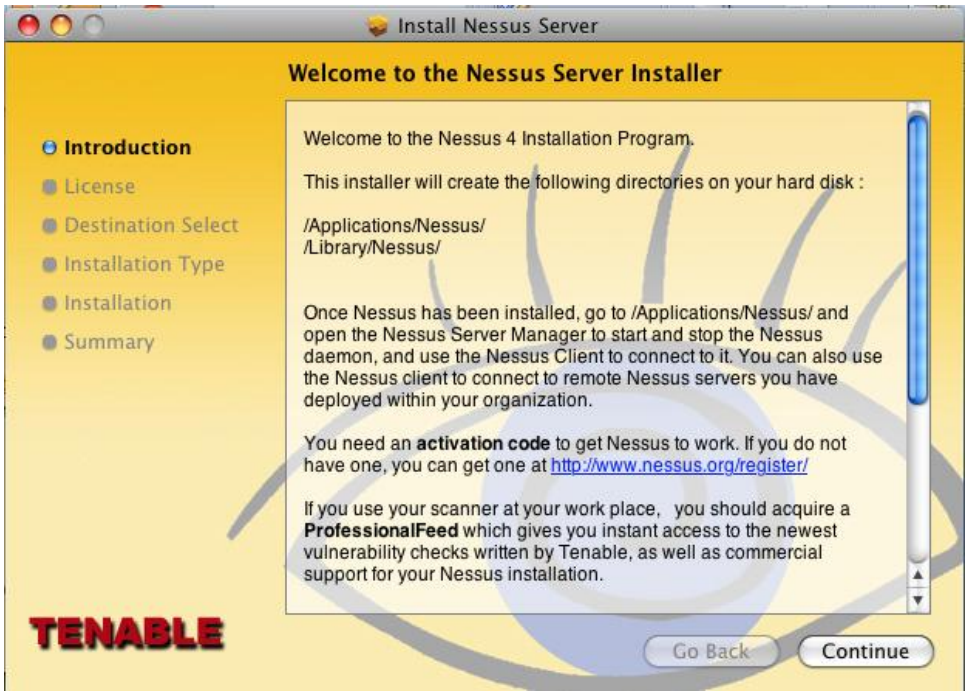

## Установка

Последняя версия сервера Nessus доступна по адресу http://www.nessus.org/download/. Сервер Nessus доступен для Mac OS X 10.4 и 10.5. Проверьте целостность установочного пакета путем сравнения контрольной суммы MD5 загрузки с контрольной суммой, указанной в файле **`MD5.asc`**, находящемся здесь.

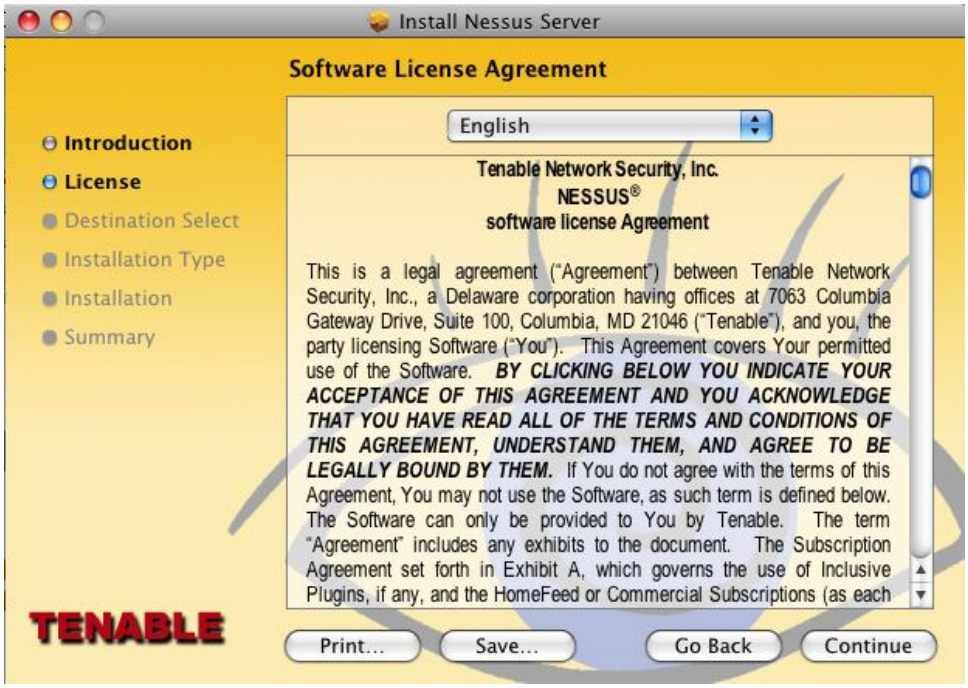
Для установки сервера Nessus на Mac OS X необходимо загрузить файл **`Nessus-4.x.x.dmg.gz`**, а затем двойным щелчком мыши развернуть архив. Щелкните двойным щелчком файл **`Nessus-4.x.x.dmg`**, в результате чего будет смонтирован образ диска, который появится в списке Devices (устройства) в обозревателе Finder. После появления тома Nessus 4 в обозревателе Finder щелкните двойным щелчком файл **`Nessus 4`**, как показано ниже.


Обратите внимание, что несколько раз в процессе установки будет появляться запрос имени пользователя и пароля администратора.

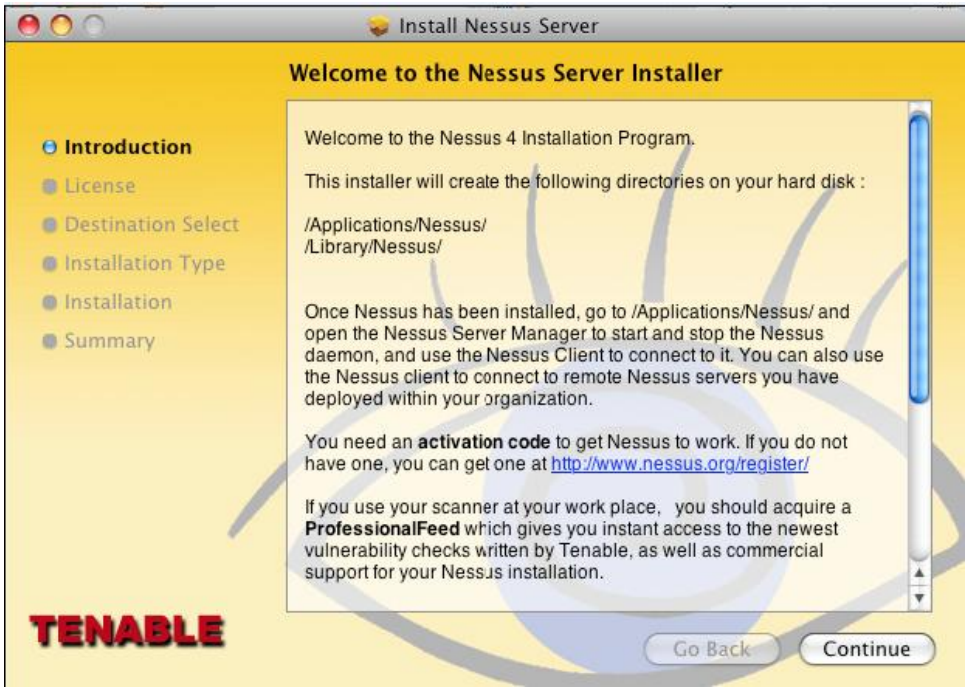
Отобразится следующее окно установки:



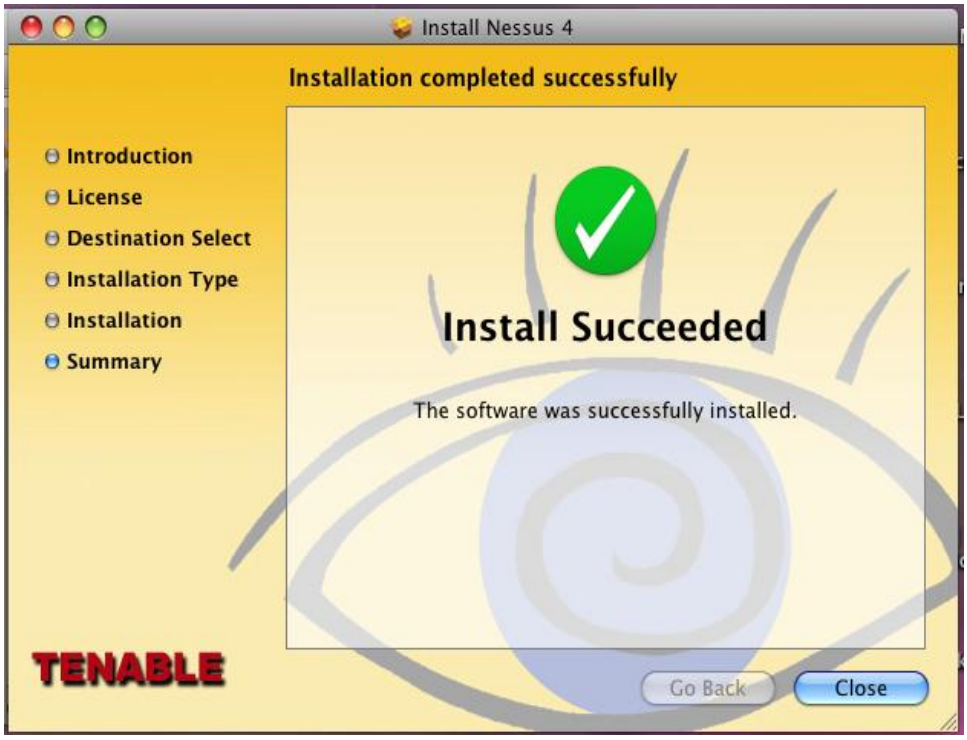

Нажмите кнопку Continue (продолжить), при этом откроется диалоговое окно с предложением принять условия лицензионного соглашения, прежде чем будет продолжена установка:




После принятия условий лицензионного соглашения откроется следующее диалоговое окно, в котором можно изменить расположение установки по умолчанию, как показано ниже:




Нажмите кнопку Install (установить) для продолжения установки. На этом этапе потребуется ввести имя пользователя и пароль администратора. Когда установка будет успешно завершена, появится следующее окно:

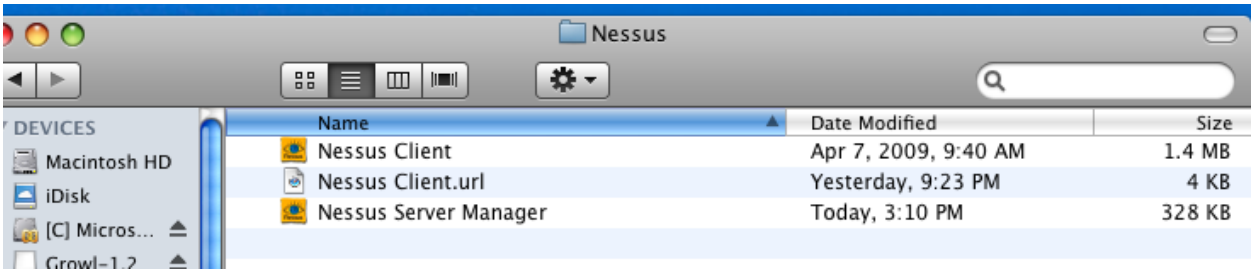



## Конфигурация

В этом разделе описывается порядок конфигурации сервера Nessus 4 на ОС Mac OS X.

### *Nessus Server Manager*

Для запуска, остановки и настройки сервера Nessus используйте программу Nessus Server Manager (диспетчер сервера Nessus), находящуюся в каталоге **`/Applications/Nessus/`**:



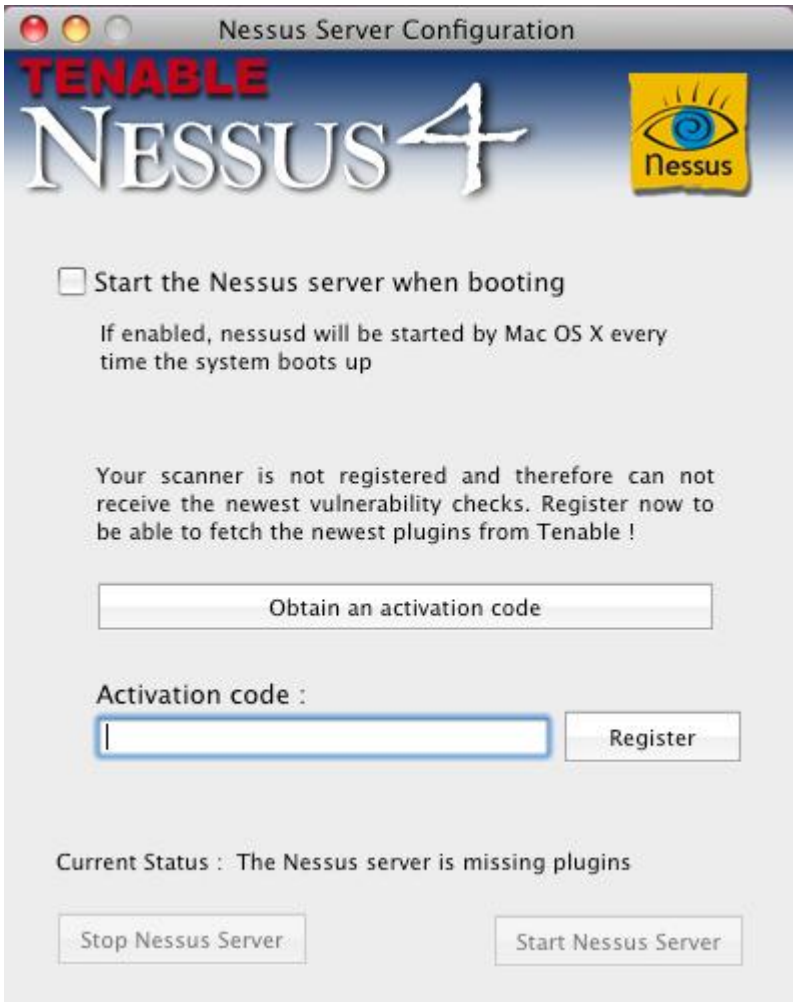

Обратите внимание, что в случае обновления сервера Nessus клиент Nessus Client все еще будет находиться в папке Nessus. Клиент Nessus Client больше не требуется использовать для управления сканированиями Nessus, и при желании его можно удалить. Nessus Client.url — это ссылка для управления Nessus через веб-браузер. Новые установки не включают клиент Nessus Client.

Интерфейс диспетчера Nessus Server Manager позволяет:

- зарегистрировать сервер Nessus на узле nessus.org для получения обновленных подключаемых модулей;
- выполнять обновление подключаемых модулей;
- настроить запуск или отсутствие запуска сервера Nessus при запуске Mac OS X;
- управлять пользователями сервера Nessus;
- запускать и останавливать сервер Nessus.

При каждом запуске диспетчера Nessus Server Manager будет появляться запрос имени пользователя и пароля администратора, потому что для взаимодействия с сервером Nessus требуются привилегии пользователя root.

Чтобы запустить диспетчер Nessus Server Manager, щелкните двойным щелчком значок, при этом откроется следующее начальное окно:



Кнопка Start Nessus Server (запустить сервер Nessus) будет недоступна, пока сервер Nessus не будет зарегистрирован.

### *Регистрация установки сервера Nessus*

В случае использования диспетчера Tenable SecurityCenter управление кодом активации (Activation Code) и обновлениями подключаемых модулей осуществляется через консоль SecurityCenter. Для связи с SecurityCenter необходимо запустить сканер Nessus, что при нормальном использовании не происходит при отсутствии действительного кода активации и подключаемых модулей. Чтобы сканер Nessus проигнорировал это требование и запустился (чтобы он мог получить информацию от SecurityCenter), выполните следующую команду из командной строки оболочки root:

```
# /Library/Nessus/run/bin/nessus-fetch --security-center
```

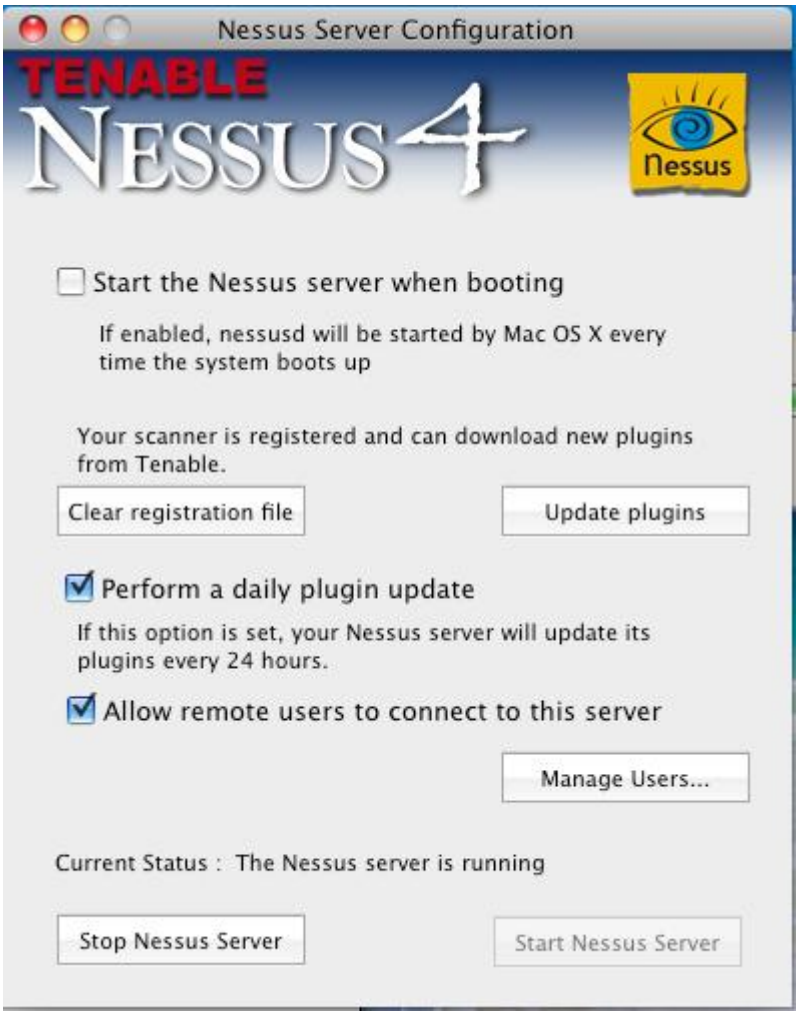
Сразу после выполнения команды **nessus-fetch**, приведенной выше, воспользуйтесь соответствующей командой для запуска сервера Nessus. Сервер Nessus теперь может быть добавлен в консоль SecurityCenter через веб-интерфейс SecurityCenter. Сведения о конфигурации централизованного канала подключаемых модулей для нескольких сканеров Nessus см. в документации SecurityCenter.

После установки сначала необходимо зарегистрировать сервер Nessus. Регистрация сервера дает доступ к последним подключаемым модулям на узле nessus.org и обеспечивает своевременное обновление аудитов.

Для регистрации сервера Nessus щелкните Obtain an activation code (получить код активации). При этом будет выполнен переход на старицу http://www.nessus.org/plugins/?view=register-info. Здесь можно подписаться на канал ProfessionalFeed или HomeFeed. Подписка на канал ProfessionalFeed необходима для коммерческого использования и предлагает обновление подключаемых модулей, техническую поддержку клиентов, аудиты конфигураций, виртуальную машину и многое другое. Подписка на канал HomeFeed требуется для домашних пользователей, она не предоставляет лицензии на профессиональное или коммерческое использование. После предоставления и обработки необходимой информации вы получите сообщение электронной почты с кодом активации, который дает право на пользование каналом подключаемых модулей ProfessionalFeed или HomeFeed. Введите код активации в соответствующее поле и нажмите кнопку Register (регистрация). Обратите внимание, что вам будет предложено ввести имя пользователя и пароль администратора. После подтверждения подлинности кода активации диспетчером Nessus Server Manager начнется обновление подключаемых модулей Nessus. Этот процесс может занять несколько минут, поскольку начальная загрузка подключаемых модулей представляет собой большой файл.

При отсутствии регистрации сервера Nessus невозможно получать новые подключаемые модули и невозможно запустить сервер Nessus.

После регистрации интерфейс диспетчера Nessus Server Manager отобразит следующее диалоговое окно:




### Изменение кодов активации

В какой-то момент вам может потребоваться изменить коды активации (например, при переходе с канала HomeFeed на канал ProfessionalFeed). Это можно выполнить с помощью кнопки Clear registration file (очистить файл регистрации) в интерфейсе диспетчера Nessus Server Manager. После подтверждения будет выполнена отмена регистрации экземпляра Nessus до получения нового кода активации и повторной регистрации продукта.

## *Создание и управление пользователями Nessus*

### Разрешение удаленных соединений

Если предполагается использовать сканер Nessus удаленно (например, с помощью SecurityCenter), необходимо установить флажок **Allow remote users to connect to this server** (разрешать удаленным пользователям подключение к этому серверу).

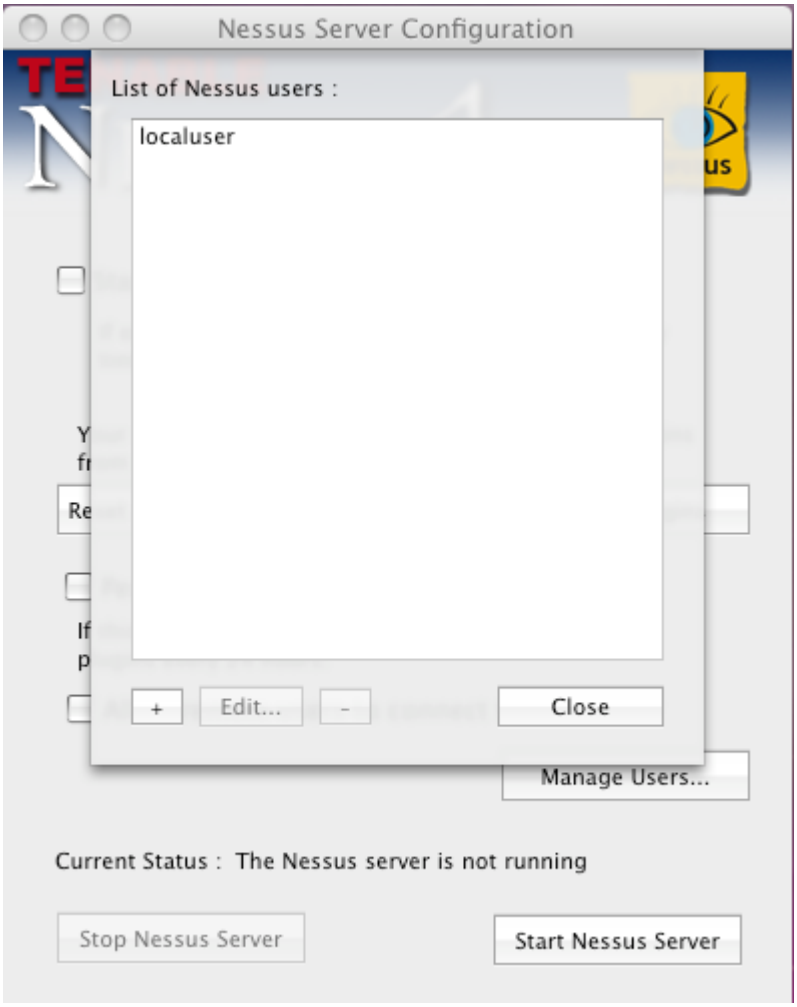
Если этот флажок снят, сервер Nessus будет доступен только для локального клиента Nessus.

Если этот флажок установлен, доступ к серверу Nessus будет возможен с помощью клиентов, установленных на этом же компьютере, удаленном хосте или с помощью интерфейса SecurityCenter (этот вариант рассматривается ниже в настоящем документе в разделе Работа с SecurityCenter).

Информация о клиентах Nessus приведена в документе «Руководство пользователя Nessus 4.4».

### Добавление учетных записей пользователей

Нажатие кнопки Manage Users… (управление пользователями...) позволяет создавать и управлять учетными записями сервера Nessus:




Если вы не обладаете достаточным опытом, не удаляйте пользователя localuser, так как при этом будет отключен сервер `Local Connection` для Nessus.

Для создания пользователя нажмите кнопку «+» и введите новое имя пользователя и пароль. Установите флажок Administrator (администратор), если пользователь будет администратором. Выбрав имя из списка и нажав кнопку Edit… (правка...), можно изменить пароль соответствующего пользователя (см. приведенный ниже снимок

экрана). При выборе пользователя и нажатии кнопки «-» соответствующий пользователь будет удален после подтверждения.

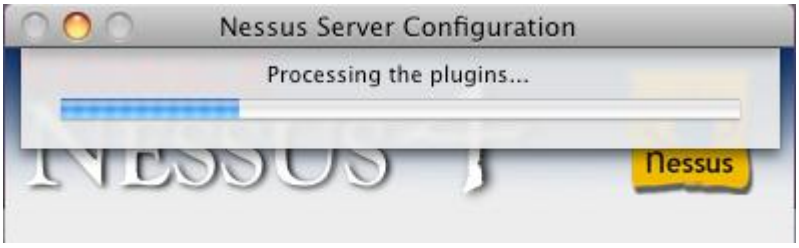
Изменить имя пользователя невозможно. При необходимости изменить имя пользователя удалите существующего пользователя и создайте нового с нужным именем.

### *Запуск демона Nessus*

Для запуска демона Nessus нажмите кнопку **Start Nessus Server** (запустить сервер Nessus) в диспетчере Nessus Server Manager.

Для автоматического запуска сервера Nessus установите флажок **Start the Nessus Server at bootup** (запускать сервер Nessus при загрузке ОС).

После запуска службы **`nessusd`** потребуется несколько минут для обработки подключаемых модулей, как показано ниже:

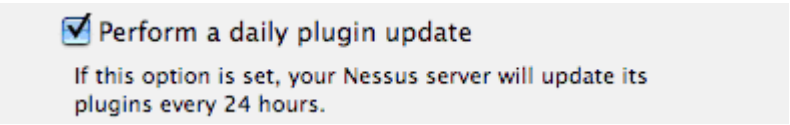



После запуска службы `nessusd` для пользователей SecurityCenter начальная установка и конфигурация сканера Nessus 4 будет завершена. Они могут перейти к разделу Работа с SecurityCenter.

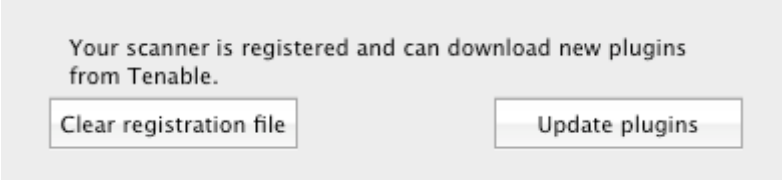
## Обновление подключаемых модулей

Сервер Nessus включает тысячи подключаемых модулей (или скриптов), которые выполняют тестирование уязвимостей сети и хостов. Новые уязвимости обнаруживаются постоянно, и для обнаружения этих уязвимостей разрабатываются новые подключаемые модули. Чтобы сканер Nessus пополнялся новейшими подключаемыми модулями, обеспечивая максимальную точность сканирования, необходимо ежедневно выполнять обновление подключаемых модулей.

Флажок **Perform a daily plugin update** (выполнять ежедневное обновление подключаемых модулей) настраивает сервер Nessus для автоматического обновления подключаемых модулей с узла Tenable каждые 24 часа. Это происходит примерно в то время суток, когда был запущен сервер Nessus.




Запустить обновление подключаемых модулей можно нажатием кнопки Update Plugins (обновить подключаемые модули), как показано ниже:




### *Как часто необходимо обновлять подключаемые модули?*

В общем случае, для большинства организаций достаточно обновлять подключаемые модули Nessus один раз в день. В случае совершенной необходимости использования самых новых подключаемых модулей и постоянного обновления в течение дня, достаточно выполнять обновление не чаще одного раза в четыре часа, поскольку более частое обновление практически бесполезно.

При установленном флажке Start the Nessus server when booting (запускать сервер Nessus при загрузке системы) разрешается удаленный доступ пользователей и ежедневно выполняется обновление подключаемых модулей.

## Удаление сервера Nessus

Для удаления Nessus остановите службу Nessus и удалите следующие каталоги:

```
/Library/Nessus
/Applications/Nessus
/Library/Receipts/Nessus*
```

Если вы не знакомы с использованием командной строки Unix в системе Mac OS X, обратитесь за помощью в службу технической поддержки Tenable.

Существуют бесплатные программные средства, такие как DesInstaller.app (http://www.macupdate.com/info.php/id/7511) и CleanApp (http://www.macupdate.com/info.php/id/21453/cleanapp), которые также можно использовать для удаления сервера Nessus. Компания Tenable не имеет отношения к этим программным средствам, и они не проходили специального тестирования для удаления сервера Nessus.

# НАСТРОЙКА ДЕМОНА NESSUS (ДЛЯ ОПЫТНЫХ ПОЛЬЗОВАТЕЛЕЙ)

Файл **`/opt/nessus/etc/nessus/nessusd.conf`** содержит несколько настраиваемых параметров. Например, настраивается максимальное количество проверок и одновременно сканируемых хостов; ресурсы, которые должен использовать `nessusd`; а также скорость чтения данных и многие другие параметры. Этот файл создается автоматически с настройками по умолчанию, но их рекомендуется проверять и изменять в соответствии с используемой средой сканирования. Полный список параметров конфигурации с пояснениями приведен в конце этого раздела.

В частности, значения **`max_hosts`** и **`max_checks`** могут оказывать большое влияние на возможности системы Nessus выполнять сканирование, а также на сканируемые в плане уязвимостей системы в вашей сети. Уделите особое внимание этим двум настройкам.

Ниже приведены эти две настройки со значениями по умолчанию из файла **nessusd.conf**:

```
# Maximum number of simultaneous hosts tested:
max_hosts = 40

# Maximum number of simultaneous checks against each host tested:
max_checks = 5
```

Обратите внимание, что эти настройки переопределяются для каждого сканирования при использовании консоли Tenable SecurityCenter или интерфейса пользователя Nessus. Для просмотра или изменения этих параметров в шаблоне сканирования в консоли SecurityCenter измените в Scan Template (шаблоне сканирования) Scan Options (параметры сканирования). В интерфейсе пользователя Nessus измените политику сканирования и перейдите на вкладку Options (параметры).

Помните, что настройки в файле `nessusd.conf` всегда переопределяются значениями из SecurityCenter Scan Template (шаблон сканирования SecurityCenter) или параметрами политик веб-клиента Nessus при выполнении сканирования с помощью этих средств.

Обратите внимание, что параметр **max_checks** имеет неизменяемый предел 15. Любое значение больше 5 часто приводит к нежелательному результату, поскольку большинство серверов не могут обрабатывать такое большое количество принудительных запросов.

**Примечания о параметре max_hosts**

Как очевидно из названия (макс_хостов), это максимальное количество целевых систем, которые будут сканироваться одновременно. Чем больше количество систем, одновременно сканируемых сканером Nessus, тем больше расходуется ресурсов ОЗУ, процессора и пропускной способности сети в системе этого сканера. При установке значения **max_hosts** следует учитывать конфигурацию оборудования сканирующей системы и другие приложения, выполняемые на ней.

Поскольку несколько других факторов, уникальных для вашей среды сканирования, также будут влиять на сканирование Nessus (например, политика вашей организации в отношении сканирования, прочий трафик сети, влияние определенных типов сканирования на сканируемые хосты), оптимальное значение параметра `max_hosts` можно установить только экспериментально.

Консервативное начальное значение для определения оптимальной настройки `max_hosts` в корпоративной среде — 20 для систем Nessus на базе ОС Unix и 10 для сканера Windows Nessus.

**Примечания о параметре max_checks**

Это количество проверок или подключаемых модулей, которые будут одновременно выполняться в отношении одного сканируемого хоста. Обратите внимание, что установка слишком большого числа потенциально может перегрузить сканируемые системы, в зависимости от используемых в ходе сканирования подключаемых модулей.

Чтобы определить общее количество одновременно выполняемых проверок, которые потенциально могут производиться в любой момент сканирования, умножьте **max_checks** на **max_hosts**. Поскольку **max_checks** и **max_hosts** используются в комбинации, установка слишком большого значения **max_checks** также может привести к превышению ограничений ресурсов системы сканера Nessus. Как и в случае с параметром **max_hosts**, оптимальное значение параметра **max_checks** можно установить экспериментально, но рекомендуется всегда устанавливать относительно низкое значение.

В случае внесения изменений в файл **nessusd.conf** сервер Nessus необходимо перезагрузить, чтобы они вступили в действие.

В процессе обновления до версии 4.4 сервер Nessus не перезапишет текущий файл **nessusd.conf**. В результате несколько параметров не будут включены в файл конфигурации. Для не включенных в файл параметров сканер Nessus будет использовать значения по умолчанию из новой установки версии 4.4.

В следующей таблице приведено краткое объяснение каждого параметра конфигурации, который доступен в файле **nessusd.conf**. Многие из этих параметров можно настраивать через интерфейс пользователя при создании политики сканирования. Новые параметры, появившиеся в версии 4.4.1, выделены жирным шрифтом.

| Параметр | Описание |
|---|---|
| auto_update | Автоматическое обновление подключаемых модулей. В случае включения этого параметра и при наличии регистрации сервера Nessus, получение последних подключаемых модулей с узла plugins.nessus.org будет выполняться автоматически. Отключите этот параметр, если сканер установлен в изолированной сети, не имеющей подключения к Интернету. |
| auto_update_delay | Время интервала между обновлениями. Минимальный допустимый интервал составляет 4 (четыре) часа. |
| purge_plugin_db | Очистка сканером Nessus базы данных подключаемых модулей при каждом обновлении. При выборе значения yes (да) каждое обновление будет выполняться значительно медленнее. |
| throttle_scan | Снижение производительности сканирования при перегрузке ЦП. |
| logfile | Расположение файла журнала Nessus. |
| www_logfile | Расположение журнала веб-сервера Nessus Web Server (интерфейс пользователя). |
| log_whole_attack | Регистрировать в журнале сведения об атаке? Полезно для отладки неполадок при сканировании, но может занимать значительное дисковое пространство. |

| | |
|---|---|
| dumpfile | Расположение файла дампа для отладки выходных данных, если такой файл генерируется. |
| rules | Расположение файла правил Nessus Rules. |
| cgi_path | При тестировании веб-серверов используется этот разделенный двоеточиями список путей CGI. |
| port_range | Диапазон портов, которые будут сканировать сканеры портов. Можно использовать ключевые слова default (по умолчанию) или all (все), а также разделенный запятыми список портов или диапазонов портов. |
| optimize_test | Оптимизация процедуры тестирования. При изменении значения этого параметра на no (нет) сканирование будет выполняться дольше и обычно будет выдавать больше ложных результатов. |
| checks_read_timeout | Таймаут чтения для сокетов тестов. |
| non_simult_ports | Порты, в отношении которых два подключаемых модуля не должны выполняться одновременно. |
| plugins_timeout | Максимальное время действия подключаемого модуля (в секундах). |
| safe_checks | Безопасные проверки собирают данные из заголовков, а не получают их в результате активного сканирования уязвимости. |
| auto_enable_dependencies | Автоматическая активация зависимых подключаемых модулей. В случае отключения этого параметра могут быть выполнены не все подключаемые модули, несмотря на то, что они выбраны в политике сканирования. |
| silent_dependencies | В случае включения этого параметра список зависимых подключаемых модулей и их выходные данные не включаются в отчет. |
| use_mac_addr | Обозначать хосты MAC-адресами, а не IP-адресами (полезно для сетей DHCP). |
| save_knowledge_base | Сохранять базу знаний на диск для дальнейшего использования. |
| plugin_upload | Определяет, могут ли пользователи с правами администратора загружать подключаемые модули. |
| plugin_upload_suffixes | Суффиксы подключаемых модулей, которые может загружать пользователь с правами администратора. |
| slice_network_addresses | При установке этого параметра сканер Nessus не будет сканировать сеть последовательно (10.0.0.1, затем 10.0.0.2, затем 10.0.0.3 и т. д.), а будет пытаться распределить нагрузку на всю сеть (например, выполнит сканирование |

| | |
|---|---|
| | 10.0.0.1, затем 10.0.0.127, затем 10.0.0.2, затем 10.0.0.128 и т. д.). |
| listen_address | Адрес IPv4 для прослушивания входящих соединений. |
| listen_port | Порт для прослушивания (старый протокол NTP). Используется для соединений NessusClient в версиях до 4.2. |
| xmlrpc_listen_port | Порт прослушивания веб-сервера Nessus Web Server (новый протокол XMLRPC). |
| xmlrpc_idle_session_timeout | Таймаут бездействия сеанса XMLRPC (в минутах). |
| xmlrpc_min_password_len | Указывает сканеру Nessus применить политику в отношении длины паролей для пользователей сканера. |
| enable_listen_ipv4 | Указывает сканеру Nessus прослушивать IPv4. |
| enable_listen_ipv6 | Указывает сканеру Nessus прослушивать IPv6, если система поддерживает адресацию IPv6. |
| source_ip | В случае многосетевой системы с разными IP-адресами в одной подсети, этот параметр указывает сканеру Nessus, какой NIC/IP использовать для тестирования. В случае указания нескольких IP-адресов, сканер Nessus будет перебирать их при выполнении соединений. |
| ssl_cipher_list | Использование только надежных шифров SSL при подключении к порту 1241. Поддерживает ключевое слово strong (надежный) для общих назначений OpenSSL, как указано в документе http://www.openssl.org/docs/apps/ciphers.html. |
| disable_ntp | Отключение старого протокола NTP. |
| disable_xmlrpc | Отключение нового интерфейса XMLRPC (веб-сервер). |
| nasl_no_signature_check | Должен ли сканер Nessus считать все скрипты NASL подписанными? Выбор значения yes (да) небезопасен и не рекомендуется. |
| nasl_log_type | Указывать тип выходных данных обработчика NASL в файле **`nessusd.dump`**. |
| use_kernel_congestion_detection | Использовать сообщения о перегрузке TCP операционной системы Linux для масштабирования активности сканера. |
| global.max_scans | При установке ненулевого значения этот параметр определяет максимальное количество сканирований, которые могут выполняться параллельно. **Примечание**: если этот параметр не используется, то никакое ограничение не применяется. |

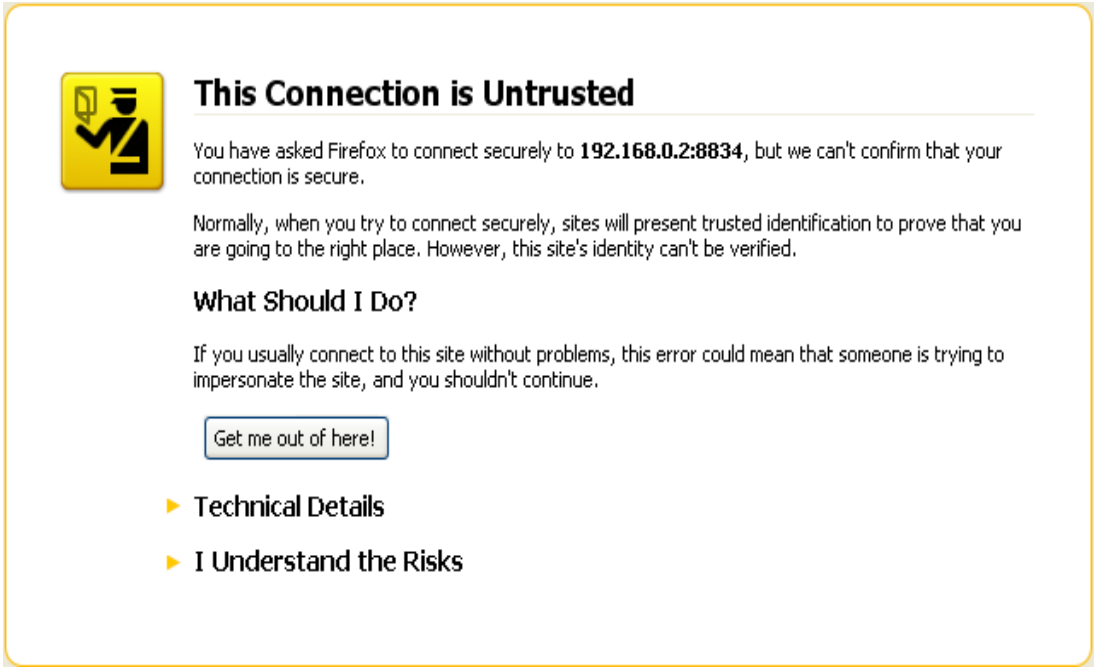
| | |
|---|---|
| global.max_web_users | При установке ненулевого значения этот параметр определяет максимальное количество сканирований, которые могут выполняться параллельно.<br>**Примечание**: если этот параметр не используется, то никакое ограничение не применяется. |
| global.max_simult_tcp_sessions | Максимальное количество одновременных сеансов TCP между всеми сканированиями.<br>**Примечание**: если этот параметр не используется, то никакое ограничение не применяется. |
| max_simult_tcp_sessions | Максимальное количество одновременных сеансов TCP на одно сканирование. |
| host.max_simult_tcp_sessions | Максимальное количество одновременных сеансов TCP на один сканируемый хост. |
| reduce_connections_on_congestion | Уменьшение количества одновременных сеансов TCP при перегрузке сети. |
| stop_scan_on_disconnect | Остановка сканирования хоста, который, по признакам, был отключен во время сканирования. |
| stop_scan_on_hang | Остановка сканирования, которое, по-видимому, зависло. |
| paused_scan_timeout | Время в минутах, по истечении которого будет удалено приостановленное сканирование (0 при отсутствии таймаута). |
| report_crashes | Сообщать анонимно о сбоях компании Tenable? |
| **nessus_syn_scanner.global_throughput.max** | Устанавливает максимальное количество пакетов syn, которые сканер Nessus будет отправлять в секунду во время сканирования портов (независимо от количества одновременно сканируемых хостов). Установите эту настройку в зависимости от чувствительности удаленного устройства к большому количеству пакетов syn. |
| qdb_mem_usage | Указывает сканеру Nessus использовать больше или меньше памяти в состоянии бездействия. Если сканер Nessus работает на выделенном сервере, при установке значения high (высокое) для этого параметра будет использоваться больше памяти для повышения производительности. Если сканер Nessus работает на общей машине, при установке значения low (низкое) для этого параметра будет использоваться значительно меньше памяти за счет умеренного снижения производительности. |
| **xmlrpc_import_feed_policies** | При установке значения no (нет) сканер Nessus будет включать политики сканирования по умолчанию, предоставленные компанией Tenable. |

Настройки в файле **nessusd.conf** могут переопределяться настройками пользователя в файле **.nessusrc**.

По умолчанию при подписке HomeFeed параметру **report_crashes** будет присвоено значение yes (да), а при подписке ProfessionalFeed параметру **report_crashes** будет присвоено значение no (нет). Связанная с неполадками Nessus информация будет отправляться компании Tenable для помощи в отладке и предоставлении программного обеспечения самого высокого качества. При этом никакая личная или позволяющая идентифицировать систему информация не отправляется.

## НАСТРОЙКА СЕРВЕРА NESSUS С ПОЛЬЗОВАТЕЛЬСКИМ СЕРТИФИКАТОМ SSL

В установке Nessus по умолчанию используется сертификат SSL с самозаверением. При первом использовании веб-интерфейса для доступа к сканеру Nessus веб-браузер выдаст ошибку, указывающую на то, что сертификат не является надежным:




Чтобы избежать предупреждений браузера, можно использовать собственный сертификат SSL вашей компании. При установке сервер Nessus создает два файла, которые составляют сертификат: **servercert.pem** и **serverkey.pem.** Эти файлы необходимо заменить файлами сертификата, сгенерированными вашей организацией или надежным центром сертификации (Certificate Authority, CA).

Прежде чем заменять файлы сертификата, остановите сервер Nessus. Замените указанные два файла и снова запустите сервер Nessus. При последующих соединениях со сканером сообщение об ошибке отображаться не будет, если сертификат сгенерирован надежным центром сертификации.

В следующей таблице указано расположение файлов сертификата для разных систем:

| Операционная система | Расположение файла сертификата |
|---|---|
| **Linux и Solaris** | `/opt/nessus/com/nessus/CA/servercert.pem`<br>`/opt/nessus/var/nessus/CA/serverkey.pem` |
| **FreeBSD** | `/usr/local/nessus/com/nessus/CA/servercert.pem`<br>`/usr/local/nessus/var/nessus/CA/serverkey.pem` |
| **Windows** | `C:\Program Files\Tenable\Nessus\nessus\CA\` |
| **Mac OS X** | `/Library/Nessus/run/com/nessus/CA/servercert.pem`<br>`/Library/Nessus/run/var/nessus/CA/serverkey.pem` |

Начиная с версии 4.4 сервер Nessus поддерживает цепочки сертификатов SSL.

Также можно посетить `https://[IP-адрес]:8834/getcert` для установки корневого центра сертификации в вашем браузере, что позволит устранить появление предупреждения.

## NESSUS БЕЗ ДОСТУПА К ИНТЕРНЕТУ

В этом разделе описаны действия для регистрации сканера Nessus, установки ключа активации и получения последних подключаемых модулей, если ваша система Nessus не имеет прямого доступа к Интернету.

Коды активации, получаемые с помощью описанной ниже автономной процедуры, привязаны к определенному сканеру Nessus, который использовался при начальной процедуре. Загруженный пакет подключаемых модулей нельзя использовать для другого сканера Nessus.

### РЕГИСТРАЦИЯ СКАНЕРА NESSUS

Код активации для подписки Nessus необходимо получить из своей учетной записи на портале Tenable Support Portal в случае использования канала ProfessionalFeed или из регистрационного сообщения электронной почты в случае использования канала HomeFeed. Для использования сканера Nessus в профессиональной среде требуется подписка на канал ProfessionalFeed, даже если он не используется непосредственно для коммерческих целей. К такому использованию относится сканирование рабочего или домашнего компьютера, используемого для коммерческих целей. Дополнительные сведения о том, на какой тип подписки вы имеете право, см. в документе Subscription Agreement (соглашение о подписке). Пользователи, имеющие право на подписку HomeFeed, могут зарегистрировать сканер на веб-сайте http://www.nessus.org/register/, введя адрес электронной почты регистрируемого пользователя. Для приобретения подписки ProfessionalFeed обращайтесь в компанию Tenable по адресу электронной почты sales@tenable.com или посетите интернет-магазин по адресу https://store.tenable.com/. Компания Tenable затем отправит вам код активации для канала ProfessionalFeed.

Обратите внимание, что вы можете использовать только один код активации для каждого сканера, если сканеры не управляются при помощи SecurityCenter.

Получив код активации, выполните следующую команду на системе, в которой запущен сервер Nessus:

**Windows:**

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --challenge
```

**Linux и Solaris:**

```
# /opt/nessus/bin/nessus-fetch --challenge
```

**FreeBSD:**

```
# /usr/local/nessus/bin/nessus-fetch --challenge
```

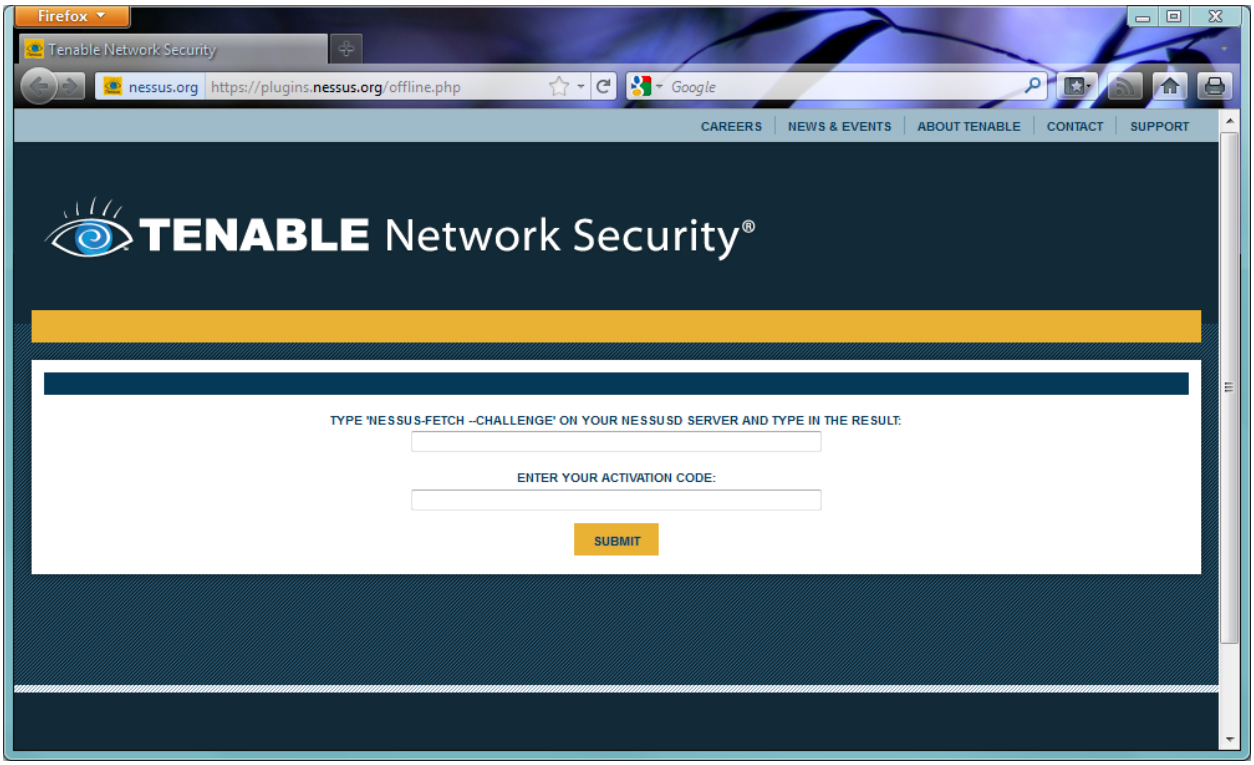
**Mac OS X:**

```
# /Library/Nessus/run/bin/nessus-fetch --challenge
```

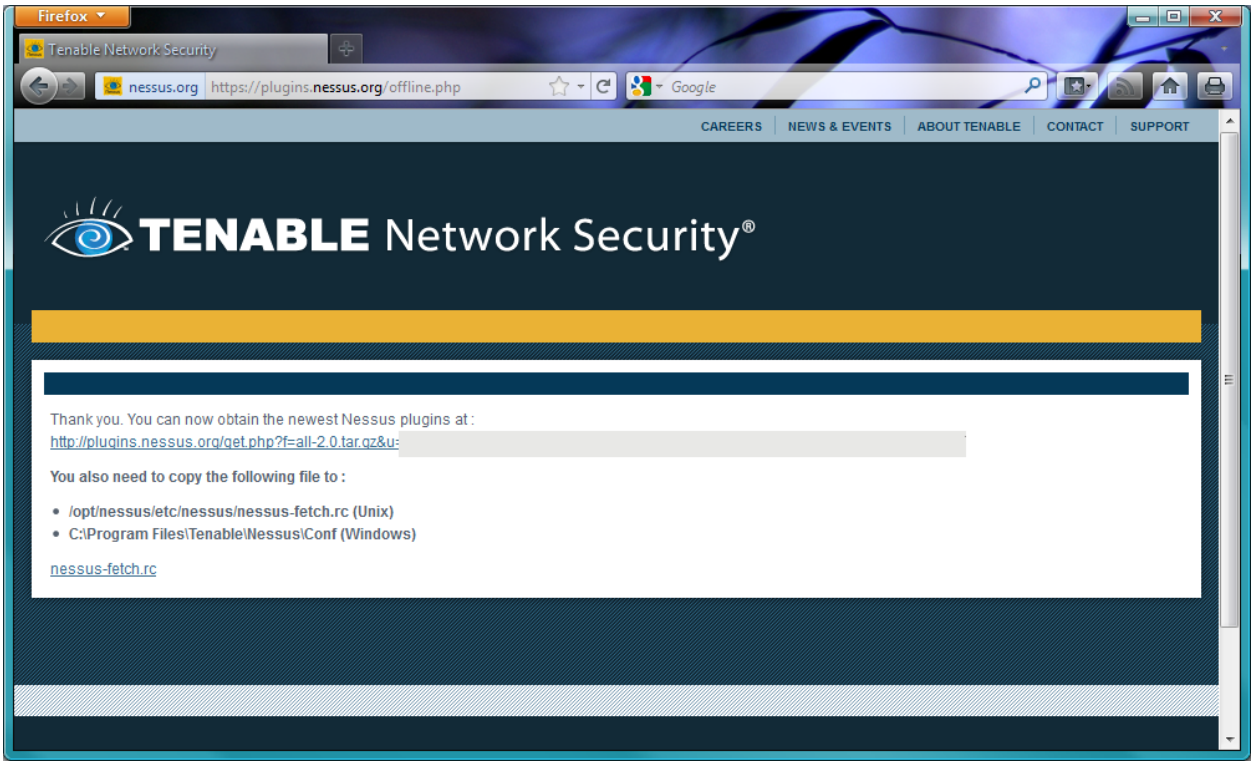
При этом будет сгенерирована строка, называемая challenge (запрос проверки подлинности), которая выглядит следующим образом:

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Затем перейдите на страницу https://plugins.nessus.org/offline.php, скопируйте в буфер обмена и вставьте строку challenge, а также ранее полученный код активации в соответствующие текстовые поля:



В результате на экране появится URL-адрес, аналогичный показанному ниже:




Этот экран дает доступ к загрузке канала самых новых подключаемых модулей Nessus (**`all-2.0.tar.gz`**) и ссылку на файл **`nessus-fetch.rc`** в нижней части экрана.

Сохраните этот URL-адрес, потому что он будет требоваться при каждом следующем обновлении подключаемых модулей, как описано в следующем разделе.

Код регистрации, используемый для автономного обновления, затем нельзя использовать для того же сервера Nessus через диспетчер Nessus Server Manager.

Если в какой-то момент вам потребуется проверить код регистрации определенного сканера, можно воспользоваться параметром **`--code-in-use`** программы **`nessus-fetch`**.

Скопируйте файл **`nessus-fetch.rc`** на хост, на котором установлен сервер Nessus, в следующий каталог:

**Windows:**

**`C:\Program Files\Tenable\Nessus\conf`**

**Linux и Solaris:**

**`/opt/nessus/etc/nessus/`**

**FreeBSD:**

**/usr/local/nessus/etc/nessus/**

**Mac OS X:**

**/Library/Nessus/run/etc/nessus/**

Файл **nessus-fetch.rc** требуется скопировать только один раз. Последующие загрузки подключаемых модулей Nessus необходимо копировать в соответствующий каталог каждый раз, как описано в следующем разделе.

Обратите внимание, что по умолчанию сканер Nessus выполняет попытку обновления подключаемых модулей каждые 24 часа после регистрации. Если вы не хотите, чтобы выполнялись попытки обновления через Интернет, просто внесите изменения в файл **nessusd.conf** и установите для параметра **auto_update** значение no.

## Получите и установите обновленные подключаемые модули

Выполняйте это действие каждый раз при автономном обновлении подключаемых модулей.

### *Windows*

Для получения новых подключаемых модулей перейдите по URL-адресу, показанному на предыдущем этапе, загрузите файл **all-2.0.tar.gz** и сохраните его в каталоге **C:\Program Files\Tenable\Nessus\.** Для установки подключаемых модулей выполните следующую команду:

```
C:\Program Files\Tenable\Nessus>nessus-update-plugins.exe all-2.0.tar.gz
Expanding all-2.0.tar.gz
Done. You need to restart the Nessus server for the changes to take effect

C:\Program Files\Tenable\Nessus>
```

Затем с помощью диспетчера Nessus Server Manager остановите и перезапустите сервер Nessus.

После установки подключаемых модулей файл **all-2.0.tar.gz** хранить не обязательно. Но компания Tenable рекомендует хранить последнюю версию загруженного файла подключаемых модулей на случай, если он потребуется снова.

Теперь вам доступны новые подключаемые модули. Каждый раз, когда потребуется обновить подключаемые модули, необходимо перейти по указанному URL-адресу, получить tar-архив, скопировать его на систему, на которой установлен сервер Nessus, и выполнить рассмотренную выше команду.

### *Linux, Solaris и FreeBSD*

Для получения новых подключаемых модулей перейдите по URL-адресу, показанному на предыдущем этапе, загрузите файл **all-2.0.tar.gz** и сохраните его в каталоге

**/opt/nessus/sbin/** (или **/usr/local/nessus/sbin/** для ОС FreeBSD). Для установки подключаемых модулей выполните следующую команду:

**Linux и Solaris:**

```
# /opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

**FreeBSD:**

```
# /usr/local/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

Далее перезапустите процесс Nessus из командной строки, чтобы сканер Nessus начал использовать новые подключаемые модули. Инструкции по перезагрузке демона Nessus см. в разделах: Остановка демона Nessus и Запуск демона Nessus.

После установки подключаемых модулей файл **all-2.0.tar.gz** хранить не обязательно. Но компания Tenable рекомендует хранить последнюю версию загруженного файла подключаемых модулей на случай, если он потребуется снова.

Теперь вам доступны новые подключаемые модули. Каждый раз, когда потребуется обновить подключаемые модули, необходимо перейти по указанному URL-адресу, получить tar-архив, скопировать его на систему, на которой установлен сервер Nessus, и выполнить рассмотренную выше команду.

### *Mac OS X*

Для получения новых подключаемых модулей перейдите по URL-адресу, показанному на предыдущем этапе, загрузите файл **all-2.0.tar.gz** и сохраните его в каталоге **/Library/Nessus/run/sbin/**. Для установки подключаемых модулей выполните следующую команду:

```
# /Library/Nessus/run/sbin/nessus-update-plugins all-2.0.tar.gz
```

Затем с помощью диспетчера Nessus Server Manager остановите и перезапустите сервер Nessus.

После установки подключаемых модулей файл **all-2.0.tar.gz** хранить не обязательно. Но компания Tenable рекомендует хранить последнюю версию загруженного файла подключаемых модулей на случай, если он потребуется снова.

Теперь вам доступны новые подключаемые модули. Каждый раз, когда потребуется обновить подключаемые модули, необходимо перейти по указанному URL-адресу, получить tar-архив, скопировать его на систему, на которой установлен сервер Nessus, и выполнить рассмотренную выше команду.

# РАБОТА С SECURITYCENTER

## Обзор SecurityCenter

Tenable SecurityCenter — это основанная на веб-технологиях консоль управления, которая объединяет процесс обнаружения и управления уязвимостями, управления событиями и журналами, мониторинга соответствия стандартам и отчетности по всем

этим элементам. Консоль SecurityCenter обеспечивает эффективное предоставление данных о событиях безопасности IT-отделу, руководству и группе аудита.

SecurityCenter поддерживает одновременное использование нескольких сканеров Nessus для периодического сканирования сетей практически любого размера. С помощью Nessus API (специализированной реализации протокола XML-RPC) консоль SecurityCenter обменивается данными со связанными с ней сканерами Nessus для отправки инструкций сканирования и получения результатов.

Консоль SecurityCenter позволяет нескольким пользователям и администраторам с разными уровнями прав: обмениваться информацией об уязвимостях; определять приоритетность уязвимостей; показывать, какие ресурсы сети содержат критические проблемы безопасности; давать рекомендации системным администраторам по их устранению; а также отслеживать устранение уязвимостей. Консоль SecurityCenter также получает данные от многих ведущих систем обнаружения атак, таких как Snort и ISS, через Log Correlation Engine (обработчик корреляции журналов).

Консоль SecurityCenter также может получать информацию о пассивных уязвимостях от сканера Tenable Passive Vulnerability Scanner (сканер пассивных уязвимостей Tenable), позволяющую конечным пользователям обнаруживать новые хосты, приложения, уязвимости и атаки без необходимости выполнения активного сканирования с помощью сканера Nessus.

## Настройка сервера Nessus для работы с консолью SecurityCenter

Чтобы включить управление любым сканером Nessus с помощью консоли SecurityCenter, должны быть доступны специальное имя пользователя и пароль для загрузки на сервер подключаемых модулей и выполнения сканирования. Этот пользователь должен иметь права администратора, предоставленные в ходе выполнения процесса `nessus-adduser` (добавление пользователя), чтобы обеспечить наличие прав, необходимых для загрузки на сервер подключаемых модулей и выполнения прочих административных функций.

Если сканер Nessus настроен для сканирования только определенных диапазонов IP-адресов, он все равно может использоваться консолью SecurityCenter. Однако если консоль SecurityCenter попытается просканировать адреса за пределами установленных диапазонов, данные об уязвимостях не будут получены.

### *Unix/Mac OS X*

Для систем командной строки Unix пользуйтесь инструкциями по добавлению пользователей, приведенными в разделе Создание пользователя Nessus Созданный пользователь должен быть администратором (admin).

Для систем Mac OS X пользуйтесь инструкциями по добавлению пользователей, приведенными в разделе Создание и управление пользователями Nessus. По умолчанию пользователи сканера Nessus на системах Mac создаются с правами администратора.

### *Windows*

#### Настройка сервера Nessus для прослушивания в режиме демона сети

Сервер Nessus можно настроить для обмена данными с консолью SecurityCenter. Для этого необходимо выполнить две задачи. Необходимо добавить учетную запись, с помощью которой консоль SecurityCenter будет входить на сервер Nessus, а затем настроить прослушивание службой Nessus входящих сетевых соединений от консоли SecurityCenter.

#### Добавление учетных записей пользователя в ОС Windows

В случае использования сервера Nessus для Windows и консоли SecurityCenter необходимо создать одного пользователя из командной строки и зарегистрировать его. Это позволит администратору запускать службу `nessusd` и консоль SecurityCenter для загрузки подключаемых модулей. Для выполнения этой задачи откройте оболочку командной строки DOS (Пуск -> Выполнить -> cmd) и перейдите в папку **`C:\Program Files\Tenable\Nessus`**. Введите следующие команды, чтобы добавить пользователя и настроить сервер Nessus для получения подключаемых модулей от консоли SecurityCenter:

```
C:\Program Files\Tenable\Nessus>nessus-adduser.exe
Login : admin
Authentication (pass/cert) : [pass]
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins,
       etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that admin has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)


Login             : admin
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
#
```

Пользователи консоли SecurityCenter всегда должны быть администраторами.

### Включение службы Nessus в ОС Windows

После добавления пользователя Nessus сервер Nessus необходимо настроить для включения службы Nessus. Это позволит консоли SecurityCenter фактически добавить сервер Nessus. Используйте следующую команду:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --security-center
nessusd can now be started, SecurityCenter will upload the plugins

C:\Program Files\Tenable\Nessus>
```

С помощью диспетчера служб Windows запустите службу Tenable Nessus. Для проверки того, прослушивает ли сканер Nessus порт 1241, из командной строки Windows выполните команду `netstat -an | findstr 1241`, как показано ниже:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Обратите внимание, что выходные данные содержат адрес «0.0.0.0:1241». Это означает, что сервер прослушивает данный порт. Сервер Nessus теперь может быть добавлен в SecurityCenter через веб-интерфейс SecurityCenter.

### Установленные на хосте брандмауэры

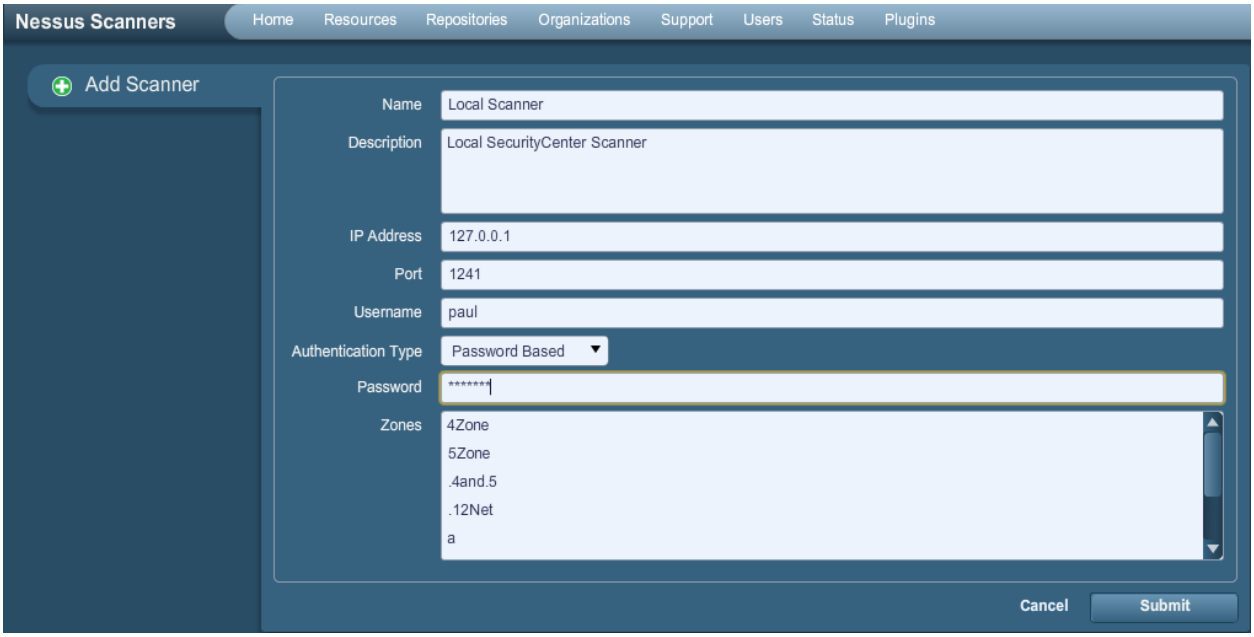
Если сервер Nessus сконфигурирован с локальным брандмауэром, например Zone Alarm, Sygate, BlackICE, брандмауэр ОС Windows XP или иное аналогичное ПО, необходимо открыть подключения к нему с IP-адреса консоли SecurityCenter.

По умолчанию используется порт 1241. В ОС Microsoft XP service pack 2 (SP2) и более поздних версиях щелчок по значку **Security Center** (центр обеспечения безопасности), находящемуся на **панели управления**, дает возможность управления настройками Брандмауэра Windows. Чтобы открыть порт 1241, выберите вкладку **Exceptions** (исключения) и добавьте в список порт 1241.

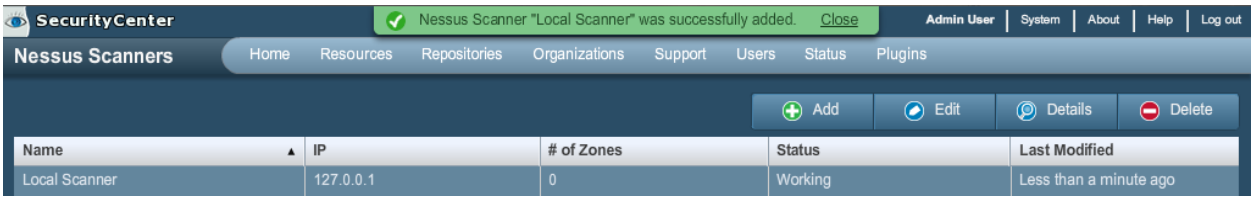
## Настройка консоли SecurityCenter для работы с сервером Nessus

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) консоли SecurityCenter:




После успешного добавления сканера и выбора сканера отобразится следующая страница:




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

# УСТРАНЕНИЕ НЕПОЛАДОК NESSUS WINDOWS

## Проблемы установки и обновления

**Проблема. В журнале nessusd.messages указывается, что сервер nessusd запущен, но он не запущен.**

**Решение.** Сообщение «nesssud <version> started» (nesssud <версия> запущен) лишь указывает, что программа `nessusd` была выполнена. Сообщение «nessusd is ready» (nessusd готов) указывает, что сервер Nessus работает и готов принимать соединения.

**Проблема. При попытке установить Nessus Windows** отображается следующее сообщение об ошибке**:**

**“1607: Unable to install InstallShield Scripting Runtime” (1607: невозможно установить библиотеку выполнения сценариев InstallShield)**

**Решение.** Этот код ошибки может появляться, если служба Windows Management Instrumentation (WMI) по какой-то причине отключена. Проверьте, запущена ли эта служба.

Если служба WMI запущена, то проблема могла возникнуть между настройками ОС Microsoft Windows и продуктом InstallShield, который используется для установки и удаления сервера Nessus Windows. Есть статьи в базах знаний Microsoft и InstallShield, в которых подробно рассматриваются возможные причины и пути решения этой проблемы.

- Статья базы знаний Microsoft ID 910816: http://support.microsoft.com/?scid=kb;en-us;910816
- Статья базы знаний InstallShield ID Q108340: http://consumer.installshield.com/kb.asp?id=Q108340

## Проблемы сканирования

**Проблема. Невозможно выполнить сканирование через соединение PPP или PPTP.**

**Решение.** В настоящее время эта возможность не поддерживается. Соответствующая функция будет включена в следующие версии Nessus Windows.

**Проблема. В отчетах о сканировании моей системы с помощью антивирусного ПО сообщается о большом количестве вирусов в Nessus Windows.**

**Решение.** Определенные антивирусные программы могут определять некоторые подключаемые модули Nessus как вирусы. Исключите каталог plugins (подключаемые модули) из сканирования антивирусной программы, поскольку этот каталог не содержит исполняемых программ.

**Проблема. При сканировании необычного устройства, например контроллера RAID, процесс прерывается, потому что сканер Nessus определяет устройство как принтер.**

**Решение.** Отключите настройку Safe Checks (безопасные проверки) в политике сканирования, прежде чем сканировать это устройство. При сканировании принтеров они обычно требуют перезапуска, поэтому в случае включения настройки Safe Checks (безопасные проверки) устройства, определяемые как принтеры, не сканируются.

**Проблема. Сканирования SYN, по-видимому, не дожидаются установления соединения в Nessus Windows.**

**Решение.** Правильно, сканирование SYN не устанавливает полное соединение TCP, но это не влияет на результаты сканирования.

**Проблема. Какие факторы при выполнении сканирования влияют на производительность Nessus Windows под ОС Windows XP?**

**Решение.** Корпорация Microsoft внесла изменения в ОС Windows XP Service Pack 2 и 3 (выпуски Home и Pro), которые могут влиять на производительность сканера Nessus Windows и давать ложные отрицательные результаты. Стек TCP/IP теперь ограничивает

количество одновременных незавершенных попыток исходящего соединения TCP. При достижении предельного значения последующие попытки соединения ставятся в очередь и разрешаются с фиксированной скоростью (10 попыток в секунду). В случае переполнения очереди попытки могут теряться. Дополнительные сведения приведены на следующей странице Microsoft TechNet:

http://technet.microsoft.com/en-us/library/bb457156.aspx

Это приводит к тому, что при сканировании Nessus под ОС Windows XP потенциально могут появляться ложные отрицательные результаты, поскольку ОС XP допускает только 10 новых незавершенных соединений в секунду (в состоянии SYN). Для большей точности рекомендуется настроить сканер Nessus под ОС Windows XP таким образом, чтобы ограничить количество сканируемых портов следующими значениями (устанавливаются в индивидуальной конфигурации сканирования для каждой политики сканирования):

Max number of hosts (максимальное количество хостов): 10
Max number of security checks (максимальной количество проверок безопасности): 4

Для повышения производительности и надежности сканирования настоятельно рекомендуется устанавливать Nessus Windows на серверные версии семейства ОС Microsoft Windows, например Windows Server 2003 или Windows Server 2008.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

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

- **Руководство пользователя Nessus** — настройка и работа с интерфейсом пользователя Nessus.
- **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/.

# ЛИЦЕНЗИОННЫЕ ЗАЯВЛЕНИЯ, НЕ ПРИНАДЛЕЖАЩИЕ КОМПАНИИ TENABLE

Ниже приведены программные пакеты сторонних производителей, которые компания Tenable поставляет для использования со сканером Nessus. На любой компонент стороннего производителя, не помеченный авторским правом компании Tenable, распространяется действие других лицензионных условий, которые приведены в документации.

Подключаемые модули сторонних производителей считаются «подключаемыми модулями для обнаружения уязвимостей» и охватываются следующими условиями.

Раздел 1 (a) Лицензионного соглашения Nessus содержит следующий текст:

Любые подключаемые модули или компоненты, не помеченные авторским правом компании Tenable, не являются «Подключаемыми модулями» согласно определению настоящего Соглашения о подписке, и на них распространяется действие других лицензионных условий.

Раздел 1 (b) (i) Лицензионного соглашения Nessus содержит следующий текст:

Подписка включает программы обнаружения уязвимостей, разработанные не компанией Tenable или ее лицензиарами, лицензия на которые предоставляется Вам на условиях отдельных соглашений. Условия настоящего Соглашения о подписке не распространяются на указанные программы обнаружения уязвимостей.

Элементы этого Программного обеспечения компании Tenable для обеспечения безопасности сетей (Tenable Network Security Software) могут использовать следующие защищенные авторским правом материалы, использование которых признается настоящим документом.

Авторское право на элементы программного обеспечения (c) 1997 – 2008 гг. University of Cambridge (libpcre)

Дальнейшее распространение и использование исходного и двоичного кода (с изменениями или без изменений) разрешается при соблюдении следующих условий.

- Используемые для дальнейшего распространения копии исходного кода должны содержать приведенное выше уведомление об авторских правах, этот список условий и следующее заявление об отказе от ответственности.

- Используемые для дальнейшего распространения копии двоичного кода должны содержать приведенное выше уведомление об авторских правах, этот список условий и следующее заявление об отказе от ответственности в документации и/или материалах, предоставляемых с распространяемой копией.

- Наименования University of Cambridge и Google Inc., также как и наименования участников их разработок не могут использоваться для подписи или рекламы продуктов, созданных на основе этого программного обеспечения, без предварительного письменного разрешения.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО ВЛАДЕЛЬЦАМИ АВТОРСКИХ ПРАВ И УЧАСТНИКАМИ РАЗРАБОТКИ НА УСЛОВИЯХ «КАК ЕСТЬ», И КАКИЕ-ЛИБО ЯВНЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, ОТКЛОНЯЮТСЯ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ВЛАДЕЛЕЦ АВТОРСКИХ ПРАВ ИЛИ УЧАСТНИКИ РАЗРАБОТКИ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПРЕДОСТАВЛЕНИЕ ЗАМЕНЯЮЩИХ ТОВАРОВ ИЛИ УСЛУГ; ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ; ЛИБО НАРУШЕНИЕ РАБОТЫ ПРЕДПРИЯТИЯ), НЕЗАВИСИМО ОТ ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО КОНТРАКТ, АБСОЛЮТНАЯ ОТВЕТСТВЕННОСТЬ, ОТВЕТСТВЕННОСТЬ ИЗ ПРАВОНАРУШЕНИЯ (ВКЛЮЧАЯ НЕОСТОРОЖНОСТЬ И ПРОЧЕЕ), ВОЗНИКШИХ КАКИМ-ЛИБО ОБРАЗОМ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ УВЕДОМЛЕНИЯ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право на элементы программного обеспечения (c) 2000 г. The NetBSD Foundation, Inc. Все права защищены.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО КОМПАНИЕЙ NETBSD FOUNDATION, INC. И УЧАСТНИКАМИ РАЗРАБОТКИ НА УСЛОВИЯХ «КАК ЕСТЬ», И КАКИЕ-ЛИБО ЯВНЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, ОТКЛОНЯЮТСЯ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ NETBSD FOUNDATION, INC. ИЛИ УЧАСТНИКИ РАЗРАБОТКИ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПРЕДОСТАВЛЕНИЕ ЗАМЕНЯЮЩИХ ТОВАРОВ ИЛИ УСЛУГ; ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ; ЛИБО НАРУШЕНИЕ РАБОТЫ ПРЕДПРИЯТИЯ), НЕЗАВИСИМО ОТ ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО КОНТРАКТ, АБСОЛЮТНАЯ ОТВЕТСТВЕННОСТЬ, ОТВЕТСТВЕННОСТЬ ИЗ ПРАВОНАРУШЕНИЯ (ВКЛЮЧАЯ НЕОСТОРОЖНОСТЬ И ПРОЧЕЕ), ВОЗНИКШИХ КАКИМ-ЛИБО ОБРАЗОМ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ УВЕДОМЛЕНИЯ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право на элементы программного обеспечения (c) 1995 – 1999 гг. Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). Все права защищены.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО УКАЗАННЫМ ИНСТИТУТОМ И УЧАСТНИКАМИ РАЗРАБОТКИ НА УСЛОВИЯХ «КАК ЕСТЬ», И КАКИЕ-ЛИБО ЯВНЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, ОТКЛОНЯЮТСЯ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ УКАЗАННЫЙ ИНСТИТУТ ИЛИ УЧАСТНИКИ РАЗРАБОТКИ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПРЕДОСТАВЛЕНИЕ ЗАМЕНЯЮЩИХ ТОВАРОВ ИЛИ УСЛУГ; ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ; ЛИБО НАРУШЕНИЕ РАБОТЫ ПРЕДПРИЯТИЯ), НЕЗАВИСИМО ОТ ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО КОНТРАКТ, АБСОЛЮТНАЯ ОТВЕТСТВЕННОСТЬ, ОТВЕТСТВЕННОСТЬ ИЗ ПРАВОНАРУШЕНИЯ

(ВКЛЮЧАЯ НЕОСТОРОЖНОСТЬ И ПРОЧЕЕ), ВОЗНИКШИХ КАКИМ-ЛИБО ОБРАЗОМ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ УВЕДОМЛЕНИЯ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право на элементы программного обеспечения (c) 1998, 1999, 2000 гг. Thai Open Source Software Center Ltd и Clark Cooper
Авторское право на элементы программного обеспечения (c) 2001, 2002, 2003, 2004, 2005, 2006 гг. Expat maintainers.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И НЕНАРУШЕНИЯ ПАТЕНТНЫХ ПРАВ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ АВТОРЫ ИЛИ ВЛАДЕЛЬЦЫ АВТОРСКИХ ПРАВ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЕТЕНЗИИ, УЩЕРБ ИЛИ ИНУЮ ОТВЕТСТВЕННОСТЬ, ВЫТЕКАЮЩИЕ ИЗ ДЕЙСТВИЯ КОНТРАКТА, ПРАВОНАРУШЕНИЯ ИЛИ ИНЫХ ОСНОВАНИЙ И ВОЗНИКШИЕ ИЗ-ЗА ИЛИ В СВЯЗИ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ЛИБО ИСПОЛЬЗОВАНИЕМ ИЛИ ИНЫМ ВЗАИМОДЕЙСТВИЕМ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

Настоящий продукт включает программное обеспечение, разработанное проектом OpenSSL Project для использования в рамках набора программ OpenSSL Toolkit. (http://www.openssl.org/) Авторское право (c) 1998 – 2007 гг. The OpenSSL Project. Все права защищены.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО ПРОЕКТОМ OpenSSL PROJECT НА УСЛОВИЯХ «КАК ЕСТЬ», И КАКИЕ-ЛИБО ЯВНЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, ОТКЛОНЯЮТСЯ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПРОЕКТ OpenSSL PROJECT ИЛИ УЧАСТНИКИ ЕГО РАЗРАБОТОК НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПРЕДОСТАВЛЕНИЕ ЗАМЕНЯЮЩИХ ТОВАРОВ ИЛИ УСЛУГ; ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ; ЛИБО НАРУШЕНИЕ РАБОТЫ ПРЕДПРИЯТИЯ), НЕЗАВИСИМО ОТ ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО КОНТРАКТ, АБСОЛЮТНАЯ ОТВЕТСТВЕННОСТЬ, ОТВЕТСТВЕННОСТЬ ИЗ ПРАВОНАРУШЕНИЯ (ВКЛЮЧАЯ НЕОСТОРОЖНОСТЬ И ПРОЧЕЕ), ВОЗНИКШИХ КАКИМ-ЛИБО ОБРАЗОМ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ УВЕДОМЛЕНИЯ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право на элементы программного обеспечения (C) 1998 – 2003 гг. Daniel Veillard. Все права защищены.

Настоящим любому лицу, приобретающему копию этого программного обеспечения и файлы сопроводительной документации (далее «Программное обеспечение»), бесплатно предоставляется разрешение использовать это Программное обеспечение без ограничений, включая (не ограничиваясь этим) права на использование, копирование, изменение, объединение, публикацию, распространение, сублицензирование и/или продажу копий этого Программного обеспечения, а также

возможность предоставления лицам, которым поставляется это Программное обеспечение, таких же прав, при соблюдении следующих условий:

Приведенное выше уведомление об авторских правах и настоящее уведомление о предоставлении разрешений должно включаться во все копии или существенные части Программного обеспечения.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И НЕНАРУШЕНИЯ ПАТЕНТНЫХ ПРАВ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ DANIEL VEILLARD НЕ БУДЕТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЕТЕНЗИИ, УЩЕРБ ИЛИ ИНУЮ ОТВЕТСТВЕННОСТЬ, ВЫТЕКАЮЩИЕ ИЗ ДЕЙСТВИЯ КОНТРАКТА, ПРАВОНАРУШЕНИЯ ИЛИ ИНЫХ ОСНОВАНИЙ И ВОЗНИКШИЕ ИЗ-ЗА ИЛИ В СВЯЗИ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ЛИБО ИСПОЛЬЗОВАНИЕМ ИЛИ ИНЫМ ВЗАИМОДЕЙСТВИЕМ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

Авторское право на элементы программного обеспечения (C) 2001 – 2002 гг. Thomas Broyer, Charlie Bozeman и Daniel Veillard.
Все права защищены.

Настоящим любому лицу, приобретающему копию этого программного обеспечения и файлы сопроводительной документации (далее «Программное обеспечение»), бесплатно предоставляется разрешение использовать это Программное обеспечение без ограничений, включая (не ограничиваясь этим) права на использование, копирование, изменение, объединение, публикацию, распространение, сублицензирование и/или продажу копий этого Программного обеспечения, а также возможность предоставления лицам, которым поставляется это Программное обеспечение, таких же прав, при соблюдении следующих условий:

Приведенное выше уведомление об авторских правах и настоящее уведомление о предоставлении разрешений должно включаться во все копии или существенные части Программного обеспечения.

НАСТОЯЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ) ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И НЕНАРУШЕНИЯ ПАТЕНТНЫХ ПРАВ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ АВТОРЫ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КАКИЕ-ЛИБО ПРЕТЕНЗИИ, УЩЕРБ ИЛИ ИНУЮ ОТВЕТСТВЕННОСТЬ, ВЫТЕКАЮЩИЕ ИЗ ДЕЙСТВИЯ КОНТРАКТА, ПРАВОНАРУШЕНИЯ ИЛИ ИНЫХ ОСНОВАНИЙ И ВОЗНИКШИЕ ИЗ-ЗА ИЛИ В СВЯЗИ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ЛИБО ИСПОЛЬЗОВАНИЕМ ИЛИ ИНЫМ ВЗАИМОДЕЙСТВИЕМ С ЭТИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

## 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