Проверки соответствия Nessus

Система аудита конфигураций и содержимого

8 июня 2011 г.

(редакция 54)

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 порядок использования сканера Nessus 4.x для проведения аудита конфигурации ОС Unix, Windows, баз данных, SCADA и Cisco с целью проверки соблюдения политики соответствия, а также выполнения поиска информации, которая может являться конфиденциальной, в содержимом различных систем.

В контексте настоящего документа выражения «соответствие политике» и «проверки соответствия» используются взаимозаменяемо.

Nessus позволяет проводить аудит системы SCADA, однако эта функциональная возможность выходит за рамки настоящего документа. Дополнительные сведения см. на информационной странице Nessus.org по SCADA, размещенной здесь.

Проведение аудита соответствия следует отличать от выполнения сканирования уязвимостей, хотя эти процедуры могут в некоторой степени совпадать. При проведении аудита соответствия определяется, настроена ли система в соответствии с установленной политикой. При сканировании уязвимости определяется, если ли в системе неустраненные известные уязвимости. Читатели узнают типы параметров настройки и конфиденциальных данных, аудит которых возможен, как настроить сканер Nessus для выполнения аудита и как предлагаемое компанией Tenable средство SecurityCenter может быть использовано для управления этим процессом и его автоматизации.

Необходимые условия

Для изучения этого документа предполагается наличие определенного уровня знаний сканера уязвимостей Nessus. Для получения дополнительных сведений о том, как можно настроить Nessus для выполнения аудита исправлений локальных систем Unix и Windows см. документ «Проверки Nessus с использованием учетных данных для Unix и Windows», размещенный по адресу http://www.nessus.org/documentation/.

Клиенты, имеющие подписку Nessus ProfessionalFeed и пользующиеся консолью SecurityCenter

Для выполнения проверок соответствия, описанных в этом документе, пользователи должны иметь подписку Nessus ProfessionalFeed или пользоваться средством SecurityCenter. Оба продукта можно приобрести у компании Tenable Network Security (http://www.tenable.com/). Более подробный список технических требований для проведения аудита приведен в следующих нескольких главах.

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`**.

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
/home/test/
#
```

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.

Стандарты соответствия

Существует множество различных типов требований к соответствию, устанавливаемых государственными и финансовыми организациями. Важно понимать, что эти требования к соответствию являются минимальным базовым уровнем, который в зависимости от коммерческих задач организации можно интерпретировать по-разному. Требования к соответствию должны быть сопоставлены с коммерческими целями для обеспечения надлежащего выявления и снижения рисков. Дополнительные сведения о развитии этого процесса см. в документе компании Tenable «Maximizing ROI on Vulnerability Management» (Достижение максимальной окупаемости инвестиций в управление уязвимостями), размещенном по адресу http://www.tenable.com/whitepapers/.

Например, предприятие может иметь политику, требующую, чтобы на всех серверах с позволяющей установить личность клиентов информацией (PII) была включена регистрация и минимальная длина пароля составляла не менее 10 символов. Эта политика может помочь организации в ее стремлении обеспечить соответствие любым нормам и правилам.

К числу распространенных норм соответствия и руководств по соответствию относятся:

- BASEL II
- Стандарты Центра интернет-безопасности (CIS)
- Задачи контроля, касающиеся связанных с информацией технологий (COBIT)
- Руководства STIG Управления информационного обеспечения Министерства обороны США (DISA)
- Федеральный закон об управлении безопасностью информации (FISMA)
- Базовая конфигурация федеральных настольных компьютеров (FDCC)
- Закон Грэмма-Лича-Блайли (GLBA)
- Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA)
- Стандарты безопасности ISO 27002/17799

- Библиотека информации по информационным технологиям (ITIL)
- Руководства по конфигурации Национального института стандартизации США (NIST)
- Руководства по конфигурации Управления национальной безопасности США (NSA)
- Стандарты безопасности данных в сфере платежных карт (PCI DSS)
- Закон Сарбейнса-Оксли (SOX)
- Защита данных на объектах (SDP)
- Различные законы штатов (например, Закон об уведомлении о нарушении безопасности штата Калифорния; SB 1386)

Эти проверки соответствия также направлены на отслеживание в режиме реального времени, например осуществление выявления проникновений и контроль доступа. Для получения дополнительной информации о том, как предлагаемые компанией Tenable решения для аудита конфигураций, управления уязвимостями, устранения утечек информации, анализа журналов регистрации и наблюдения за сетью могут помочь в выполнении упомянутых норм и правил соответствия требованиям обращайтесь по адресу электронной почты sales@tenable.com, чтобы запросить экземпляр документа «Real-Time Compliance Monitoring» (Наблюдение за соответствием в режиме реального времени).

Аудит конфигураций, утечки информации и соответствие требованиям

Что такое аудит?

Сканер Nessus позволяет проводить аудит системы SCADA, однако эта функциональная возможность выходит за рамки настоящего документа. Дополнительные сведения см. на информационной странице Nessus.org по SCADA, размещенной здесь.

Сканер Nessus может быть использован для входа на серверы под управлением ОС Unix и Windows, в системы устройств Cisco, системы SCADA и базы данных для определения того, настроены ли они в соответствии с локальной политикой безопасности объекта. Сканер Nessus может выполнять поиск по всему жесткому диску систем Windows и Unix с целью поиска неразрешенного содержимого.

Для обеспечения надлежащей защиты активов важно, чтобы организации определяли политику безопасности объектов до проведения аудита. Оценка уязвимостей позволит определить, уязвимы ли системы для известных эксплойтов (средств взлома, использующих уязвимости), но не даст возможности определить, например, хранятся ли регистрационные данные сотрудников на общедоступном сервере.

Абсолютного стандарта безопасности не существует — это вопрос управления рисками, подход к которому зависит от конкретной организации.

Например, представьте такие требования к паролям, как политики в отношении минимального и максимального срока действия паролей и блокировки учетных записей. Возможно существование очень серьезных причин для частой или нечастой смены паролей. Также возможно существование очень серьезных причин блокировки учетной записи в случае более чем пяти неудачных попыток входа в систему, но если данная

система исключительно важна для предприятия в целом, то установка более высокого значения или даже отключение блокировки полностью может оказаться более разумным.

Эти параметры конфигурации являются существенной частью управления системой и политики безопасности, но не относятся к конкретным уязвимостям системы или отсутствующим исправлениям. Сканер Nessus может выполнять проверки соответствия требованиям серверов под управлением ОС Unix и Windows. Политики могут быть очень простыми или очень сложными в зависимости от требований, предъявляемых при каждом конкретном сканировании системы для проверки соответствия.

Аудит в сравнении со сканированием уязвимостей

Сканер Nessus может выполнять сканирование уязвимостей сетевых служб, а также выполнять вход на сервер для выявления любых недостающих исправлений. Однако отсутствие уязвимостей не означает, что серверы настроены правильно или «соответствуют» определенному стандарту.

Преимущество использования сканера Nessus для выполнения сканирования уязвимостей и проведения аудита соответствия требованиям заключается в том, что все данные могут быть получены одновременно. Наличие знаний о том, как настроен сервер, какие исправления применены и какие уязвимости существуют, может помочь определить меры по снижению риска.

На более высоком уровне, если эта информация обобщается для целой сети или класса средств (например, с помощью средства SecurityCenter компании Tenable), безопасность и риски можно анализировать глобально. Это позволяет аудиторам и руководителям сетей выявлять тенденции, касающиеся не отвечающих требованиям систем, и корректировать средства контроля для более масштабного их устранения.

Пример элементов аудита

В последующих разделах описываются аудиты конфигурации ОС Windows, Unix, баз данных и систем Cisco.

Модуль регулярных выражений сканера Nessus 4 основан на диалекте языка Perl и считается «расширенным POSIX» из-за присущей ему гибкости и скорости работы.

Windows

Сканер Nessus может тестировать любые параметры, которые могут быть заданы на платформе Microsoft Windows в виде политики. Существует несколько сотен параметров реестра, которые могут быть проверены, а также могут быть проанализированы разрешения файлов, каталогов и объектов. Неполный перечень примеров аудита включает испытание следующих настроек:

- длительность блокировки учетных записей;
- хранение журнала безопасности;
- возможность локального входа в систему;
- ведение журнала паролей.

Ниже приведен пример элемента аудита для серверов под управлением ОС Windows:

```
<item>
 name: "Minimum password length"
 value: 7
</item>
```

Этот конкретный аудит ищет на сервере Windows параметр «Minimum password length» (минимальная длина пароля) и генерирует сигнал тревоги, если значение этого параметра меньше семи символов.

Сканер Nessus может также производить поиск на компьютерах под управлением ОС Windows конфиденциальных данных. Ниже приведен пример выполнения поиска номеров кредитных карт Visa в файлах различных форматов:

```
<item>
 type: FILE_CONTENT_CHECK
 description: "Determine if a file contains a valid VISA Credit Card
       Number"
 file_extension: "xls" | "pdf" | "txt"
 regex: "([^0-9-]|^)(4[0-9]{3}( |-|)([0-9]{4})( |-|)([0-9]{4})( |-|)([0-
       9]{4}))([^0-9-]|$)"
 expect: "VISA" | "credit" | "Visa" | "CCN"
 max_size: "50K"
 only_show: "4"
</item>
```

Эта проверка ищет по файлам приложений Excel, Adobe и текстовым файлам соответствующие определенным образцам фрагменты текста, свидетельствующие о наличии одного или нескольких действительных номеров кредитных карт Visa.

Unix

Сканер Nessus можно широко использовать для тестирования разрешений файлов, содержимого файлов, выполняющихся процессов и контроля доступа пользователей в различных системах на основе Unix. В настоящее время предлагаются проверки для осуществления аудита таких производных от Unix систем, как Solaris, Red Hat, AIX, HP-UX, SuSE, Gentoo и FreeBSD.

```
<item>
 name: "min_password_length"
 description: "Minimum password length"
 value: "14..MAX"
</item>
```

Этот аудит проверяет, установлена ли в системе Unix минимальная длина пароля 14 символов.

Cisco

Сканер Nessus может испытывать текущую конфигурацию систем, работающих под управлением ОС Cisco IOS, и подтверждать их соответствие стандартам политик безопасности. Проверки можно выполнять, используя какую-либо учетную запись без

дополнительных прав или учетную запись с обеспечивающим дополнительные права паролем enable.

```
<item>
 type: CONFIG_CHECK
 description: "Require AAA service"
 info: "Verify centralized authentication, authorization and accounting"
 info: "(AAA)service (new-model) is enabled."
 item: "aaa new-model"
</item>
```

Базы данных

Сканер Nessus может быть настроен для входа в базы данных следующего типа и определения соответствия требованиям их локальных политик безопасности:

- SQL Server
- Oracle
- MySQL
- PostgreSQL
- DB2
- Informix/DRDA

Аудиты баз данных обычно состоят из ряда операторов, извлекающих из базы данных связанные с безопасностью сведения, например о существовании или статусе небезопасных хранимых процедур. Приведем пример, определяющий, включена ли потенциально опасная хранимая процедура **`xp_cmdshell`**:

```
<custom_item>
 type: SQL_POLICY
 description: "xp_cmdshell option"
 info: "The xp_cmdshell extended stored procedures allows execution of
       host executables outside the controls of database access
       permissions and may be exploited by malicious users."
 info: "Checking that the xp_cmdshell stored procedure is set to '0'"
 sql_request: "select value_in_use from sys.configurations where name =
       'xp_cmdshell'"
 sql_types: POLICY_INTEGER
 sql_expect: "0"
</custom_item>
```

Возможность написать файлы аудита для каждой организации и выполнять поиск конфиденциальных данных очень полезна. В этом документе описывается, как создать пользовательские политики поиска данных различных типов.

Отчеты об аудите

При выполнении аудита сканер Nessus пытается определить, что хост соответствует требованиям, не соответствует требованиям или что результаты являются неокончательными.

Результаты, свидетельствующие о несоответствии требованиям, регистрируются сканером Nessus как «Note» с указанием уровня серьезности, результаты, подтверждающие несоответствие требованиям, регистрируются как «Hole» (брешь), а неокончательные результаты (например, проверка разрешений для файла, который не был найден в системе) регистрируются как «Warning» (предупреждение). Предлагаемое компанией Tenable средство SecurityCenter использует следующую градацию серьезности: «low» (низкая), «medium» (средняя) и «high» (высокая). При этом проверки, которые соответствуют требованиям, получают уровень серьезности «low», не соответствующие — «high», а неокончательные — «medium».

В отличие от проверки уязвимостей, в результате которой сообщается только о фактически существующих уязвимостях, проверка соответствия всегда сообщает те или иные результаты. Таким образом, полученные данные могут использоваться в качестве основы отчета об аудите для демонстрации того, что хост прошел или не прошел конкретное испытание либо не мог быть надлежащим образом испытан.

Необходимые технологии

Подключаемые модули Nessus .nbin для проверки соответствия конфигурации ОС Unix и Windows требованиям

Компания Tenable выпустила два подключаемых модуля Nessus (идентификаторы 21156 и 21157), которые являются реализацией интерфейсов API, используемых для проведения аудита систем Unix и Windows. Эти подключаемые модули были предварительно скомпилированы в формат Nessus «**.nbin**».

Эти подключаемые модули и соответствующие политики аудита доступны клиентам, имеющим подписку на канал ProfessionalFeed, или пользователям консоли SecurityCenter. В данном документе также описываются два средства для ОС Windows, которые помогают создавать пользовательские файлы «**.audit**» для ОС Windows, и одно средство для ОС Unix, предназначенное для создания файлов «**.audit**» для ОС Unix.

Подключаемый модуль .nbin Nessus для проверки соответствия содержимого ОС Windows

Компания Tenable выпустила подключаемый модуль Nessus (идентификатор 24760) под названием «Windows File Contents Check» (проверка содержимого файлов Windows), который является реализацией интерфейсов API, используемых для проверки систем под управлением ОС Windows на наличие не отвечающего требованиям содержимого, например личных сведений (Personally Identifiable Information, PII) или защищаемых медицинских сведений (Protected Health Information, PHI). Эти подключаемые модули предварительно скомпилированы в формат Nessus «**.nbin**». Эти подключаемые модули и соответствующие политики аудита доступны клиентам, имеющим подписку на канал ProfessionalFeed, или пользователям консоли SecurityCenter.

Подключаемый модуль .nbin Nessus для проверки соответствия баз данных

Компания Tenable выпустила подключаемый модуль Nessus (идентификатор 33814) под названием «Database Compliance Checks» (проверки соответствия для баз данных), который является реализацией интерфейсов API, используемых для аудита различных систем баз данных. Этот подключаемый модуль предварительно скомпилирован в

формат Nessus «**.nbin**». Этот подключаемый модуль и соответствующие политики аудита доступны клиентам, имеющим подписку на канал ProfessionalFeed, или пользователям консоли SecurityCenter.

Проверки соответствия баз данных недоступны в Security Center версии 3.4.3 и более ранних версиях.

Подключаемый модуль .nbin Nessus для проверки соответствия содержимого ОС Cisco

Компания Tenable выпустила подключаемый модуль Nessus (идентификатор 46689) под названием «Cisco IOS Compliance Checks» (проверки соответствия ОС Cisco IOS), который является реализацией интерфейсов API, используемых для аудита систем под управлением операционной системы CISCO IOS. Этот подключаемый модуль предварительно скомпилирован в формат Nessus «**.nbin**». Этот подключаемый модуль и соответствующие политики аудита доступны клиентам, имеющим подписку на канал ProfessionalFeed. Эта проверка соответствия может выполняться для сохраненных (Saved), запущенных (Running) и начальных (Startup) конфигураций.

Политики аудита

Компания Tenable разработала ряд политик аудита для платформ Unix, Windows и Cisco. Они поставляются в виде текстовых файлов **.audit** подписчикам ProfessionalFeed и могут быть загружены через портал поддержки Tenable Support Portal, расположенный по адресу https://support.tenable.com/support-center/. Последние сведения о функциональных возможностях проведения аудита продуктов Tenable и всех последних выпусках файлов **.audit** см. на дискуссионных форумах по адресу: https://discussions.nessus.org/.

При написании этих политик аудита были учтены многие аспекты распространенных аудитов соответствия, например требования SOX, FISMA и PCI DSS, но они не являются файлами официального аудита по этим критериям. Пользователям рекомендуется изучить эти политики **.audit** и индивидуально настроить эти проверки под свои локальные среды. Пользователи могут переименовывать эти файлы **.audit** в соответствии с локальными описаниями. Другие политики **.audit** следуют из рекомендованных организациями CERT, CIS, NSA и NIST настроек конфигурации.

Компания Tenable собирается на основе отзывов клиентов и меняющихся рекомендованных методик выпустить несколько файлов **.audit** различного типа. Насколько консалтинговых организаций и клиенты компании Tenable также начали внедрять собственные политики **.audit** и проявили интерес поделиться ими с другими пользователями Nessus ProfessionalFeed. Простым способом распространения политик **.audit** или просто взаимодействия с сообществом Nessus являются дискуссионные форумы Discussion Forum портала Tenable Network Security, расположенные по адресу https://discussions.nessus.org/.

Полезные служебные программы

Компания Tenable разработала средство преобразования файлов **.inf** в файлы **.audit** для Nessus, предназначенные для выполнения аудита ОС Windows. Это средство называется **i2a** и также описывается далее в этом документе.

Существует два средства для ОС Unix, которые можно использовать для создания файлов **.audit** для ОС Unix. Первое средство под названием **c2a** (сокращение от «configuration to audit» — аудит из конфигурации) можно использовать для создания файлов **.audit** для ОС Unix непосредственно из существующих файлов конфигурации. Например, если файл конфигурации программы Sendmail соответствует политике вашего объекта, то средство **c2a** может создать политику аудита на основе контрольной суммы MD5 файла или конкретных пар значений и аргументов, содержащихся в файле **sendmail.cf**. Второе средство, называемое **p2a** (сокращение от «package to audit» — аудит из пакета), можно использоваться для создания файлов **.audit** для ОС Unix из базового пакета, установленного в системе Unix (на основе RPM в Linux или Solaris 10), или из простого текстового файла со списком названий пакетов.

Сканеры Nessus для Unix или Windows

Для выполнения проверок соответствия могут использоваться различные платформы, и обычно лежащая в основе операционная система, на которой устанавливается сканер Nessus, значения не имеет. Аудит соответствия сервера под управлением ОС Windows 2003 можно выполнять с портативного компьютера под управлением ОС OS X, а аудит сервера под управлением ОС Solaris можно проводить с портативного компьютера под управлением ОС Windows.

Учетные данные для подлежащих аудиту устройств

Во всех случаях для входа на целевые серверы сканеру Nessus требуются учетные данные оболочки SSH системы Unix, домена Windows, ОС Cisco IOS или базы данных. В большинстве случаев этот пользователь должен быть супер-пользователем или обычным пользователем с возможностью повышения полномочий (например, **sudo**, **su** или **su+sudo**). Если выполняющий аудит пользователь не имеет прав супер-пользователя, то многие команды удаленной системы невозможно будет выполнить, или возвращаемые результаты будут неправильными.

Учетная запись ОС Windows, используемая в качестве реквизитов для входа, должна иметь право чтения политики локальной машины. Если целевой узел не входит в домен Windows, то учетная запись должна быть членом группы администраторов хоста. Если хост входит в домен, то группа администраторов домена будет входить в группу администраторов хоста и учетная запись будет иметь доступ к политике локальной машины, если она входит в группу администраторов домена.

Для выполнения проверок соответствия содержимого ОС Windows кроме входа в систему с дополнительными правами в отношении домена необходимо также иметь доступ к инструментарию управления Windows (WMI). При отсутствии такого доступа сканер Nessus сообщит, что доступ к WMI для выполнения сканирования отсутствует.

Проверки соответствия баз данных требуют для выполнения полного аудита соответствия базы данных только наличия учетных данных базы данных. Это связано с тем, что выполняется сканирование соответствия требованиям не операционной системы хоста, а базы данных.

Проверки соответствия ОС Cisco IOS для выполнения полного аудита соответствия конфигурации системы обычно требуют наличия пароля enable. Это связано с тем, что сканер Nessus выполняет аудит результата выполнения команды «**show config**», доступной только привилегированному пользователю. Если применяемый для выполнения аудита пользователь сканера Nessus уже имеет права enable, то пароль enable не требуется.

Дополнительные сведения о настройке сканера Nessus или средства SecurityCenter для выполнения проверки уязвимостей с локальными реквизитами входа, см. в документе «Проверки Nessus с использованием учетных данных для Unix и Windows», размещенном по адресу http://www.nessus.org/documentation/.

Использование «su», «sudo» и «su+sudo» для выполнения аудита

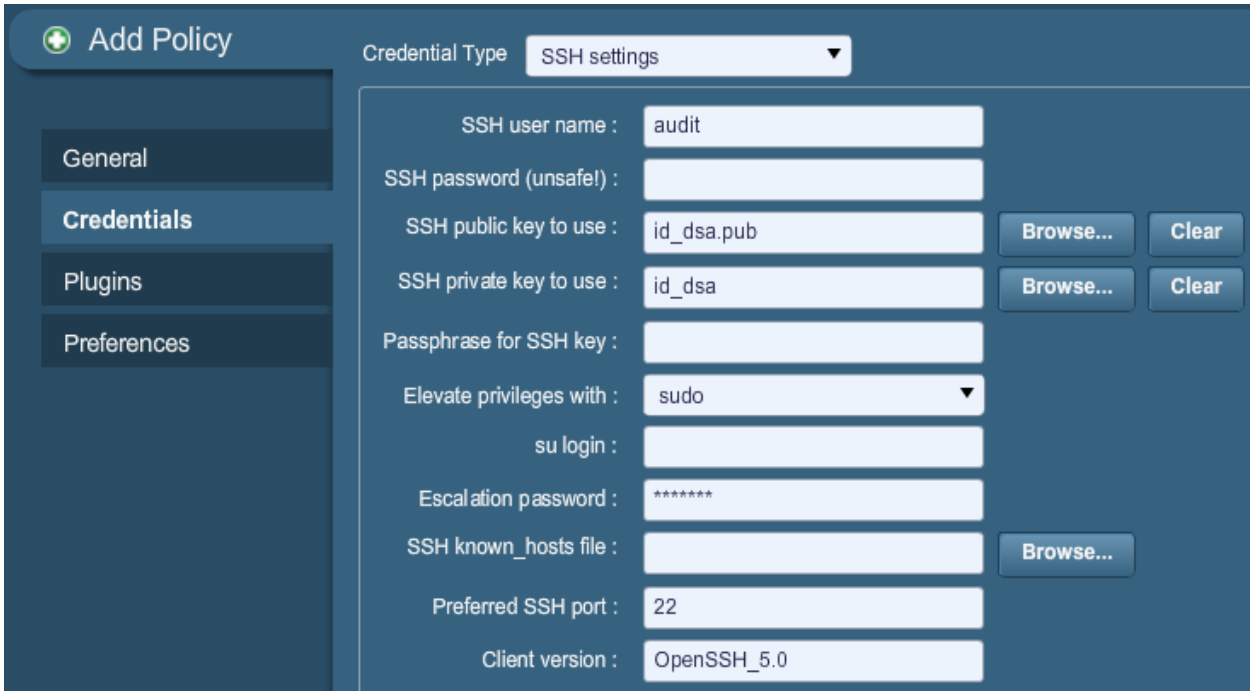
Используйте «**su+sudo**» в случаях, когда политика компании не позволяет сканеру Nessus выполнять вход на удаленный узел в качестве пользователя root и пользователя с правами «**sudo**». При удаленном входе в систему не имеющий дополнительных прав пользователь сканера Nessus может поменять пользователя (с помощью команды «**su**») на имеющего права «**sudo**».

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

Кроме того, если файл SSH **known_hosts** доступен и предоставлен в рамках политики сканирования, Nessus будет пытаться выполнить вход только в хосты, указанные в этом файле. Это гарантирует, что имя пользователя и пароль, используемые вами для аудита известных серверов SSH, не будут использованы для попытки входа в систему, которая может быть вне вашего контроля.

Пример использования команды «sudo»

Ниже приведен пример снимка экрана, показывающий использование команды **sudo** в сочетании с ключами SSH. В этом примере учетная запись пользователя — audit, которая была добавлена в файл **/etc/sudoers** на сканируемой системе. Предоставленный пароль является паролем учетной записи audit, а не паролем root. Ключи SSH соответствуют ключам, сгенерированным для учетной записи audit:

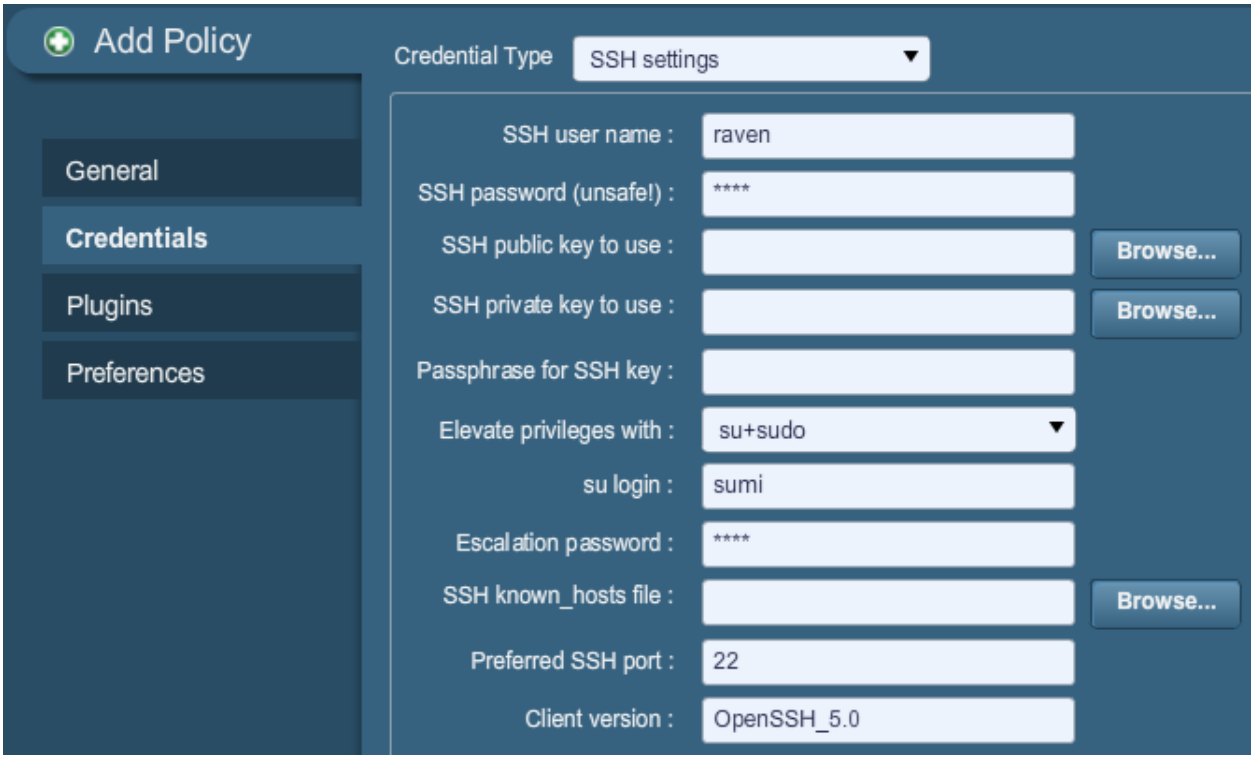


Пример использования команд «su+sudo»

В версии Nessus 4.2.2 был включен новый метод повышения прав для учетных данных узлов под управлением ОС Unix, на которых установлена программа **sudo**: «**su+sudo**». Этот метод позволяет предоставлять реквизиты учетной записи, не имеющей разрешения использовать **sudo**, для этого надо воспользоваться командой **su** для замены пользователя на имеющего такое право и затем воспользоваться командой **sudo**.

Эта конфигурация обеспечивает большую безопасность учетных данных во время сканирования и удовлетворяет требованиям многих организаций.

Чтобы включить эту функцию, просто выберите «su+sudo» в списке «Elevate privileges with» (повысить уровень привилегий с помощью) на вкладке «Credentials high» (учетные данные) раздела «SSH settings» (настройки SSH), как показано на следующем снимке экрана:



В полях «SSH user name» (имя пользователя SSH) и «SSH password» (пароль SSH) введите реквизиты, не обладающие правом пользоваться командой **sudo**. В приведенном выше примере используется учетная запись raven. В раскрывающемся меню «Elevate privileges with» (повысить уровень привилегий с помощью) выберите «su+sudo». Введите в поля «su login» (имя пользователя для команды «su») и «Escalation password» (пароль для повышения уровня привилегий) имя пользователя и пароль, которые *обладают* привилегиями. В данном случае это «sumi». Каких-либо иных изменений в политику сканирования вносить не требуется.

Важные примечания об использовании команды sudo

При выполнении аудита систем под управлением ОС Unix с помощью команд **su**, **sudo** или **su+sudo** помните о следующих моментах:

- Если безопасность системы Unix была повышена путем ограничения перечня команд, которые могут выполняться с помощью команды **sudo**, или файлов, доступ к которым разрешен удаленным пользователям, это может повлиять на аудит. При возникновении подозрений, что аудит ограничивается мерами безопасности, сравните аудиты, выполненные не с учетной записью root с аудитами, с аудитами, выполненными с использованием учетной записи root.
- Команда **sudo** не является встроенной для системы Solaris и требует загрузки и установки, если целевая система работает под управлением ОС Solaris. Убедитесь, что двоичный файл **sudo** доступен как «**/usr/bin/sudo**».
- При сканировании с использованием файла **known_hosts** сканеру Nessus все равно нужно указывать сканируемый хост. Например, в случае сканирования класса C при загруженном файле **known_hosts** со всего 20 отдельными хостами в пределах этого класса C, сканер Nessus выполнит сканирование только хостов, указанных в этом файле.

- Некоторые конфигурации на основе ОС Unix требуют выполнения запускаемых с помощью команды «sudo» команд из сеансов **tty**. Сканирование уязвимостей с помощью Nessus, выполняемое в режиме «su+sudo», не отвечает этому требованию. В случае использования режима «su+sudo» необходимо создать на целевой системе исключение. Чтобы выяснить, необходимо ли это для конкретной версии Unix, введите следующую команду как пользователь root на системе, которую будете сканировать:

  ```
  # grep requiretty `locate sudoers` | grep -v "#" | grep /etc
  ```

  Если строка **requiretty** включена в файл настроек **sudoers**, то в файл **/etc/sudoers** необходимо добавить исключение из этого правила следующим образом:

  ```
  Defaults    requiretty
  Defaults:{userid} !requiretty
  ```

  Обратите внимание, что {userid} — это имя пользователя, которое будет использоваться для выполнения команды «sudo» (поле «su login» (имя пользователя для команды «su») на вкладке «Credentials» (учетные данные) раздела «SSH settings» (настройки SSH) политики). Также убедитесь, что в файл **sudoers** включена следующая строка:

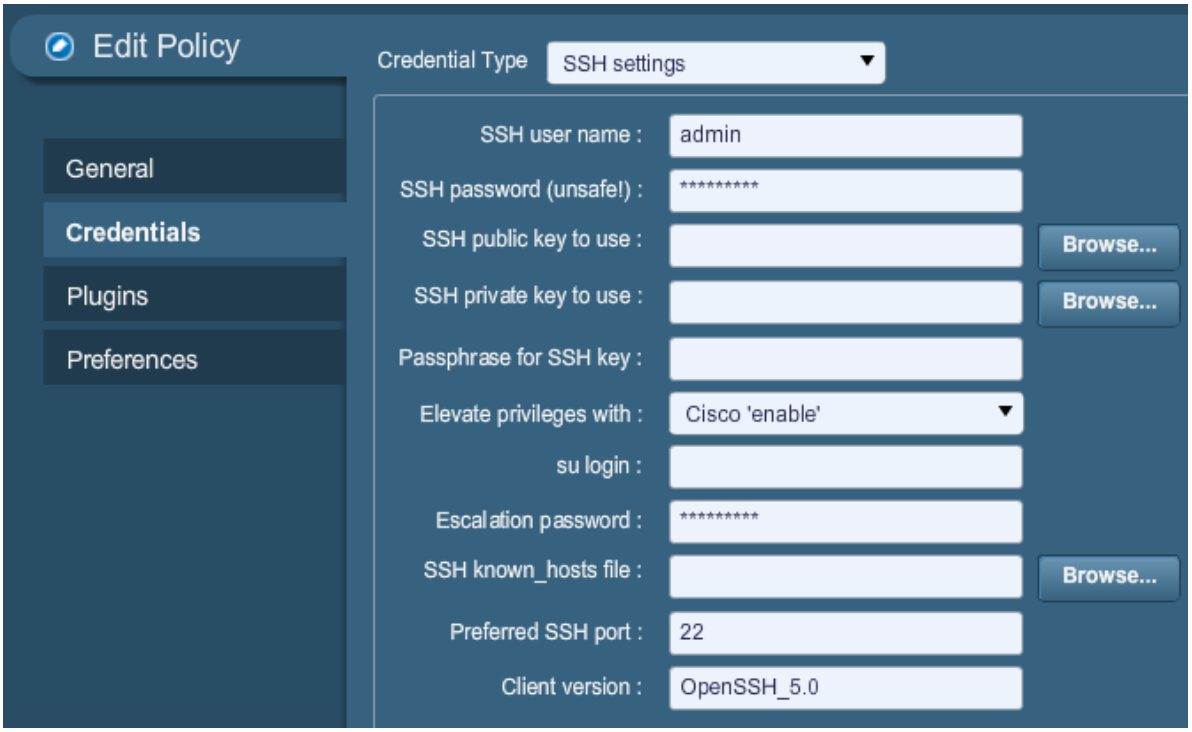
  ```
  {userid}     ALL=(ALL)       ALL
  ```

  Повторимся, {userid} — это имя пользователя, которое будет использоваться для выполнения команды «sudo» (поле «su login» (имя пользователя для команды «su») на вкладке Credentials (учетные данные) раздела SSH settings (настройки SSH) политики).

Пример для ОС Cisco IOS:

Поддерживается только проверка подлинности через SSH. Устаревшие устройства под управлением IOS, которые требовали для проверки подлинности Telnet, не позволяют выполнить сканирование с помощью проверок соответствия Nessus для Cisco.

Реквизиты Cisco IOS настраиваются на странице реквизитов **SSH settings** (настройки SSH) пользовательского интерфейса Nessus. Введите имя пользователя и пароль SSH, необходимые для входа в систему маршрутизатора Cisco. Чтобы указать, что права должны быть расширены, с помощью Enable (разрешить), выберите значение **Cisco enable** (команда enable системы Cisco) в раскрывающемся списке **Elevate privileges with** (повысить уровень привилегий с помощью) и введите пароль для команды enable (разрешить) в поле **Escalation password** (пароль для повышения уровня привилегий).



ПРЕОБРАЗОВАНИЕ ФАЙЛОВ .INF СИСТЕМЫ WINDOWS В ФАЙЛЫ .AUDIT С ПОМОЩЬЮ СЛУЖЕБНОЙ ПРОГРАММЫ I2A

При наличии файлов политик ОС Windows (обычно они имеют расширение **.inf**) их можно преобразовать в файлы **.audit**, чтобы использовать в аудитах Nessus серверов под управлением ОС Windows.

Получение и установка программы

Служебную программу **i2a** можно получить в виде zip-архива через портал поддержки Tenable Support Portal, расположенный по адресу https://support.tenable.com/support-center/. Эта программа не имеет графического интерфейса пользователя и выполняется из командной строки.

Распакуйте содержимое этого файла в каталог по своему выбору и затем переместите файлы ОС Windows **.inf** в этот же каталог.

Преобразование файлов .inf в файлы .audit

Запустите средство преобразования из командной строки, просто введя с клавиатуры:

```
# i2a-x.x.x.exe yourfile.inf file.audit
```

В этом примере файл **yourfile.inf** является исходным файлом **.inf**, а файл **file.audit** — полученным в результате преобразования файлом **.audit**.

Анализ преобразования

Компания Tenable попыталась добиться 100-процентного преобразования информации, которая может быть описана в файле **.inf** и которая может быть использована для аудита в файле **.audit**. Однако современный уровень технологии Nessus 4 не позволяет испытывать некоторые элементы политики.

Файл регистрации процесса преобразования создается для каждого запуска средства **i2a**. В нем содержится построчный аудит всего процесса преобразования. Если какая-то строка файла **.inf** не может быть преобразована, то она будет приведена в этом файле регистрации.

Правильный формат настроек в файле .inf

Проверьте соответствие приведенных в файле регистрации проверок, которые не удалось обработать, описанным ниже допустимым форматам.

Параметры **System Access** (доступ к системе), **System Log** (системный журнал), **Security Log** (журнал безопасности), **Application Log** (журнал приложений) и **Event Audit** (аудит событий) имеют одинаковый формат. Каждая запись описывается как параметр (**Key**), после которого следует значение (**value**).

Синтаксис:

```
Key = value
```

В приведенном выше случае параметр (**Key**) — это проверяемый элемент, а значение (**value**) — это предполагаемое значение данного параметра в удаленной системе.

Пример:

```
MinimumPasswordLength = 8
```

Формат настроек **Privilege Rights** (привилегированные права) аналогичен упомянутому выше, но в данном случае значение может быть пустым.

Синтаксис:

```
PriviledgeRight = User1,User2…UserN
```

Пример:

```
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-544
```

Или:

```
SeTcbPrivilege =
```

Параметр **Registry Key** (раздел реестра) состоит из следующих четырех частей:

- Registry Key (раздел реестра) – это раздел реестра, который необходимо проверить.
- Inheritance Value (значение наследования) – определяет, унаследованы или не унаследованы разрешения для этого раздела реестра. Значение может быть в диапазоне от 0 до 4.
- DACL – список DACL является списком ACL, который контролируется владельцем объекта и определяет права доступа каждого конкретного пользователя и каждой группы к этому объекту.
- SACL – список SACL является списком ACL, который управляет генерированием сообщений аудита в случае попыток получить доступ к защищаемому объекту.

Синтаксис:

```
"Registry Key",Inheritance value,
"D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...
       (string_acen)"
```

Поля DACL и SACL могут быть пустыми, и в этом случае данная проверка будет проигнорирована.

Пример:

```
"MACHINE\SYSTEM\CurrentControlSet\Control\Class",0,"D:PAR(A;CI;KA;;;BA)(A;C
      IIO;KA;;;CO)S:PAR(AU;OICIFA;CC;;;WD)"
```

Формат параметра **File Security** (безопасность файлов) аналогичен формату описанных выше параметров Registry Key (раздел реестра).

Синтаксис:

```
"File Object",Inheritance value,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)
      ... (string_acen)"
```

Пример:

```
"%SystemRoot%\system32\ciadv.msc",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S
      :PAR(AU;OICIFA;CC;;;WD)"
```

Параметр **Service General** (общие параметры служб) состоит из следующих четырех частей:

- Service Name (имя службы) – служба, аудит которой необходимо провести.
- Service start type (тип запуска службы) – Manual (вручную), Automatic (автоматически) или Disabled (отключена). Значение может быть в диапазоне от 2 до 4.

- DACL – список DACL является списком ACL, который контролируется владельцем объекта и определяет права доступа каждого конкретного пользователя и каждой группы к этому объекту.
- SACL – список SACL является списком ACL, который управляет генерированием сообщений аудита в случае попыток получить доступ к защищаемому объекту.

Синтаксис:

```
Service Name,Start type,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1).
      ..(string_acen)"
```

Пример:

```
kdc,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CC
      LCSWRPWPDTLOCRRC;;;SY)"
```

Если проверять параметр «permissions for a service» (права службы) не требуется и достаточно проверить параметр «startup type» (тип запуска), то это можно выполнить следующим образом.

Синтаксис:

```
Service Name,Start type
```

Пример:

```
kdc,3,""
```

Параметр **Registry Value** (значение реестра) состоит из следующих трех частей:

- RegistryKey (раздел реестра) – это раздел реестра, который необходимо проверить.
- RegistryType (тип реестра) – тип реестра: REG_DWORD, REG_SZ и т. д.
- RegistryValue (значение реестра) – значение раздела реестра.

Параметр RegistryValue (значение реестра) может быть определен в двойных, одиночных кавычках или без них.

Синтаксис:

```
RegistryKey,RegistryType,RegistryValue
```

Пример:

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDet
      ect=4,0
```

При желании к любой строке файла **.inf** можно добавить в начале точку с запятой, и скрипт пропустит эту строку как комментарий.

ПРЕОБРАЗОВАНИЕ ФАЙЛОВ КОНФИГУРАЦИИ ОС UNIX В ФАЙЛЫ .AUDIT С ПОМОЩЬЮ ПРОГРАММЫ C2A

Средство **c2a.pl** предназначено для того, чтобы помочь аудиторам создавать файлы **.audit** для аудита конфигураций приложений в определенной сети. Например, если нужно, чтобы все веб-серверы определенной сети были настроены точно так же, как главный хост X, то следует запустить эту программу на сервере X, создать файл **.audit** для **httpd** на этой системе, а затем использовать этот файл в качестве исходного для демона Nessus и запустить сканирование всех других веб-серверов с целью проверки их соответствия.

При желании это средство также может быть использовано для создания файлов аудита кодов MD5 всего узла. В качестве исходного файла ему потребуется список файлов или каталогов, которые нужно проверить, которые будут обработаны данным средством в случае каталогов рекурсивно для создания файла **.audit** для системы. Позднее этот файл можно будет использовать для сканирования изменений в основных файлах и каталогах.

ПОЛУЧЕНИЕ И УСТАНОВКА ПРОГРАММЫ

Служебную программу **c2a** можно получить в виде **tar**-архива через портал поддержки Tenable Support Portal, расположенный по адресу https://support.tenable.com/support-center/.

Разверните содержимое файла **c2a-x.x.x.tar.gz** на локальной машине с помощью следующей команды:

```
# tar xzf c2a-x.x.x.tar.gz
```

При этом в текущем каталоге будет создан каталог **c2a**, в который будут распакованы файлы. При желании распаковать содержимое в какой-то определенный каталог воспользуйтесь следующей командой:

```
# tar xzf c2a.x.x.x.tar.gz -C /path/to/directory
```

После того как архив будет распакован, в каталоге **~/c2a** должны находиться следующие файлы:

- **c2a.pl**
- **c2a.map**
- **c2a_regex.map**
- **cmv.pl**
- **ReadMe.txt**

Создание файла аудита кодов MD5

Запустите средство преобразования с параметром **-md5**, введя команду:

```
# ./c2a.pl -md5 -f /path/to/inputfile.txt -o outputfile.audit
```

Программе требуется исходный файл со списком файлов и каталогов, аудит значений кодов MD5 которых необходимо будет проводить, а также имя файла аудита, который будет в результате получен.

При добавлении файлов в исходный файл обязательно используйте следующий формат:

/path/to/file

Используйте этот формат при добавлении каталогов:

/path/to/file/

При использовании этого формата для файла, а не каталога средство **c2a** сообщит, что такого файла не существует. Для создания каталогов достаточно начального символа наклонной черты (/).

Если записью в исходный файл внесен обычный файл MD5, то только этот файл будет просчитан и записан в формате **.audit**. В случае каталога скрипт рекурсивно проанализирует каждый файл в каталоге. Если результирующий файл не указан, то результат будет записан в файл **~/c2a/op.audit**.

При обработке списка файлов, указанного как inputfile (исходный файл), все встречающиеся символические ссылки будут игнорироваться. Будет выдано сообщение о том, что файла не существует или это символическая ссылка. Начиная с этой версии, средство **c2a** не поддерживает символические ссылки.

Создание файла аудита на основе одного или нескольких файлов конфигурации

Средство **c2a** идеально подходит для обработки файлов конфигурации, имеющих уникальное построчное содержимое. Если файл конфигурации имеет многострочную функциональную структуру, как файлы конфигурации формата XML, то средство **c2a** не очень подходит для них.

Запустите средство преобразования с параметром **-audit**, введя команду:

```
# ./c2a.pl -audit -f /path/to/input.txt -o outputfile.audit
```

Программе требуется исходный файл (**input.txt**) со списком файлов конфигурации, аудит которых необходимо будет проводить, а также имя файла аудита, который будет в результате получен.

В скрипте Perl **c2a.pl** используются два важнейших файла: **c2a.map** и **c2a_regex.map**. Этот скрипт сканирует каждую строку файла конфигурации, аудит которого выполняется, и проверяет, является ли первое слово каждой строки указанным в файле **c2a.map** типом (например, HTTP, SENDMAIL и т. д.), и получает связанное с ним значение. Например, при аудите настроек HTTP программа проверяет, является ли данное слово любым из ключевых слов протокола HTTP, содержащихся в файле **c2a.map**. Если это так, то она применяет к этой строке регулярное выражение из файла **c2a_regex.map** для HTTP и извлекает параметр и значение. Возможен аудит только параметров, включенных в виде записи в файл **c2a.map**.

Файлы конфигурации, которые не должны проверяться в ходе аудита, можно пометить как комментарии с помощью символа «#».

При желании преобразовать параметры, которые были отмечены в файле конфигурации как комментарии, в формат **.audit** внесите изменения в файл **c2a.pl** и установите значение параметра «`$ENFORCE_COMMENT = 1;`».

Как и в предыдущем случае, если результирующий файл не указан, то результат будет записан в файл **~/c2a/op.audit**.

В настоящее время компания Tenable предоставляет параметры MAP для HTTP, SENDMAIL, SYSCTL и NESSUS. Дополнительные настройки приложений несложно добавить, воспользовавшись программой Perl **cmv.pl**. Дополнительную информацию см. в следующем разделе.

Создание файла MAP

Создать файл MAP для какого-либо приложения несложно. Просто запустите скрипт **cmv.pl** следующим образом:

```
# ./cmv.pl -r 'regex' -r tag -f config_file
```

где:

- «**regex**» — это регулярное выражение для извлечения пар параметров конфигурации и их значений. Обычно оно имеет формат «<name> = <value>» (<имя> = <значение>). Но в некоторых случаях формат может быть несколько иным, например символ «=» может быть заменен на пробел, знак табуляции и т. д.
- «**tag**» — это фактически ключевое слово, указывающее на то, что вы хотите разметить приложение, аудит которого осуществляется. Ключевое слово **tag** связывает файл **config_file** с ключевыми словами в файле **c2a.map** и регулярным выражением в **c2a_regex.map**, следовательно, важно, чтобы теги во всех файлах были одинаковыми.
- «**config_file**» — это файл конфигурации, для которого создается файл MAP.

Например, при желании провести аудит настроек конфигурации для VSFTPD, выполните следующие действия:

1. Сначала воспользуйтесь программой **cmv.pl** следующим образом:

```
# ./cmv.pl -r '([A-Za-z0-9_]+)=([A-Za-z0-9]+)' -t VSFTPD -f
/root/vsftpd-0.9.2/vsftpd.conf
```

При этом будет создан файл **tag.map** (например, **VSFTPD.map**). По умолчанию все строки, отмеченные как комментарии, будут пропускаться. Если необходимо учитывать все переменные, то измените значение **$ENFORCE_COMMENT** с «0» на «1» и снова запустите скрипт.

2. Проверьте файл MAP и присоедините его к файлу **c2a.map**.

   Проверьте файл **VSFTPD.map** на наличие ненужных значений, которые могли случайно совпасть с регулярным выражением. После того как убедитесь, что все ключевые слова правильны, добавьте их в файл **c2a.map**.

3. Обновите файл **c2a_regex.map** тем же выражением, которое использовалось программой **cmv.pl**, следующим образом:

   ```
   VSFTPD=([A-Za-z0-9_]+)=([A-Za-z0-9]+)
   ```

   Примечание. Это же регулярное выражение используется в скрипте Perl **cmv.pl**.

4. Обновите файл **input.txt**, указав расположение файла конфигурации VSFTPD:

   ```
   VSFTPD=/root/vsftpd-0.9.2/vsftpd.conf
   ```

5. Запустите скрипт **c2a.pl**:

   ```
   # ./c2a.pl -audit -f input.txt
   ```

6. В итоге проверьте результирующий файл:

   ```
   # vi op.audit
   ```

Иное использование средства c2a

Компания Tenable включила в файлы **c2a.map** и **c2a_regex.map** несколько записей, которые позволят провести аудит приложений Sendmail, Very Secure FTP Daemon (VSFTPD), Apache, файла Red Hat **/etc/sysctl.conf** и Nessus. В ближайшем будущем может быть добавлено другое программное обеспечение. При желании предоставить компании Tenable новые схемы или поделиться ими с другими пользователями Nessus отправляйте их по адресу nessus-support@tenable.com.

Таким образом, скрипт **c2a.pl** можно использовать для создания файлов Nessus **.audit** для нескольких рабочих приложений Unix. Учтите следующее.

- Если у организации много межсетевых экранов на основе ОС Unix, то файл **.audit** может сгенерировать аудит общих и необходимых настроек, которые должны быть установлены в каждой программе межсетевого экрана. Например, если все межсетевые экраны должны включать фильтрацию адресов RFC 1918, то возможно провести соответствующее тестирование фактически используемых межсетевыми экранами правил.

- Если многочисленные пользовательские приложения запускаются из CRON, то можно провести аудит различных CRONTAB, чтобы убедиться, что правильные приложения запускаются в надлежащее время.
- Для централизованного входа можно проверить на удаленных системах Unix их конфигурации SYSLOG, SYSLOG-NG и LOGROTATE.

Ручная подстройка файлов .audit

И, наконец, результат выполнения программы **c2a.pl** также можно редактировать вручную. Например, возможно объединение правил проверки контрольных сумм MD5 с правилами проверки FILE_CONTENT_CHECK (проверка содержимого файлов) в одно правило. Генерируемый программой **c2a.pl** результат также предполагает, что файл конфигурации всегда располагается в одном месте. Можно изменить ключевое слово «**file**» таким образом, чтобы указать другие места, где может находиться файл конфигурации.

При наличии содержимого, которое нежелательно в файлах конфигурации удаленных систем, можно вручную добавить соответствующие проверки с помощью ключевого слова FILE_CONTENT_CHECK_NOT (проверка содержимого файлов на отсутствие). Это позволит выполнить аудит настроек, которые должны быть, а также, которых не должно быть.

Преобразование списков пакетов ОС UNIX в файлы .audit с помощью программы p2a

Средство **p2a.pl** предназначено для того, чтобы помочь аудиторам создавать файлы **.audit** для конфигураций установочных пакетов в системах Linux и Solaris 10 на основе RPM. Например, если нужно, чтобы на всех веб-серверах Linux определенной сети были такие же основные пакеты RPM, как на главном узле X, то необходимо запустить это средство на узле X для создания файла **.audit**, содержащего все пакеты RPM, установленные на этой системе. Затем можно будет использовать этот файл **.audit** со сканером Nessus для сканирования других веб-серверов с целью проверки их соответствия.

Также это средство может быть использовано для создания файла аудита из текстового списка пакетов RPM или пакетов Solaris 10. В исходном файле должен быть список пакетов, перечисленных каждый на отдельной строке, из которого будет надлежащим образом сформирован файл **.audit** для целевой системы. Позднее сгенерированный файл **.audit** можно будет использовать для сканирования изменений в основных установочных пакетах.

Получение и установка программы

Средство **p2a** предоставляется в виде **tar**-архива, включающего один скрипт языка Perl и файл справки **ReadMe.txt**. Его можно получить через портал поддержки Tenable Support Portal, расположенный по адресу https://support.tenable.com/support-center/.

Разверните содержимое файла **p2a-x.x.x.tar.gz** на локальной машине с помощью следующей команды:

```
# tar xzf p2a-x.x.x.tar.gz
```

При этом в текущем каталоге будет создан каталог `p2a`, в который будут распакованы файлы.
При желании распаковать содержимое в какой-то определенный каталог воспользуйтесь следующей командой:

```
# tar xzf p2a.x.x.x.tar.gz -C /path/to/directory
```

После того как архив будет распакован, в каталоге `~/p2a` должны находиться следующие файлы:

- **p2a.pl**
- **ReadMe.txt**

Сделайте этот скрипт исполняемым, запустив:

```
# chmod 750 p2a.pl
```

Использование

Запустите скрипт Perl следующим образом:

```
# ./p2a.pl [-h] -i inputfile.txt -o outputfile.audit
```

«-h»— это дополнительный самостоятельный аргумент, показывающий средство справки.

Создание результирующего файла по всем установленным пакетам

Если скрипт исполняется с одним параметром **-o**, то запускается системная команда извлечения имен всех установленных локально пакетов системы, и затем результирующий файл **.audit** будет записан под именем **/path/to/outputfile.audit**.

```
# ./p2a.pl -o /path/to/outputfile.audit
```

Для выполнения скрипта результирующие файлы должны иметь расширение **.audit**. Иначе будет выдана ошибка в связи с неправильным расширением файла.

Создание результирующего файла по списку пакетов и вывод его на экран

Чтобы отправлять все результаты в окно терминала, запустите **p2a**, используя следующий синтаксис:

```
# ./p2a.pl -i /path/to/inputfile.txt
```

Для этого варианта использования скрипта необходим исходный файл, а результат будет выводиться в окно терминала (**stdout**), и его можно будет скопировать и вставить в файл **.audit**. В исходном файле пакеты должны быть указаны по одному в каждой строке без разделителей.

Пример:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Так как во многих системах на основе Unix установлено свыше тысячи пакетов, объем результата может превысить буфер прокрутки экрана, и просмотр результата полностью может быть непростой задачей.

Создание файла аудита на основе указанного исходного файла

При запуске программы **p2a** с указанными в качестве аргументов исходным и результирующим файлами она генерирует в указанном месте по форматированному списку пакетов файл **.audit**.

```
# ./p2a.pl -i /path/to/input_file.txt -o /path/to/outputfile.audit
```

Исходные файлы должны иметь формат в виде перечня пакетов, каждый из которых приводится в отдельной строке без разделителей.

Пример:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Для выполнения скрипта результирующие файлы должны иметь расширение **.audit**. Иначе будет выдана ошибка в связи с неправильным расширением файла.

Пример использования пользовательского интерфейса Nessus

Получение проверок соответствия стандартам

Клиенты ProfessionalFeed сразу получают проверки соответствия для сканера Nessus, кроме того несколько файлов **.audit** можно загрузить через портал поддержки Tenable

Support Portal, расположенный по адресу https://support.tenable.com/support-center/. Для подтверждения этого запустите пользовательский интерфейс Nessus, пройдите проверку подлинности и управляйте существующей политикой либо редактируйте ее. На вкладке Plugins (подключаемые модули) найдите семейство «Policy Compliance» (соответствие политики), щелкните имя семейства подключаемых модулей и убедитесь в наличии следующих подключаемых модулей:

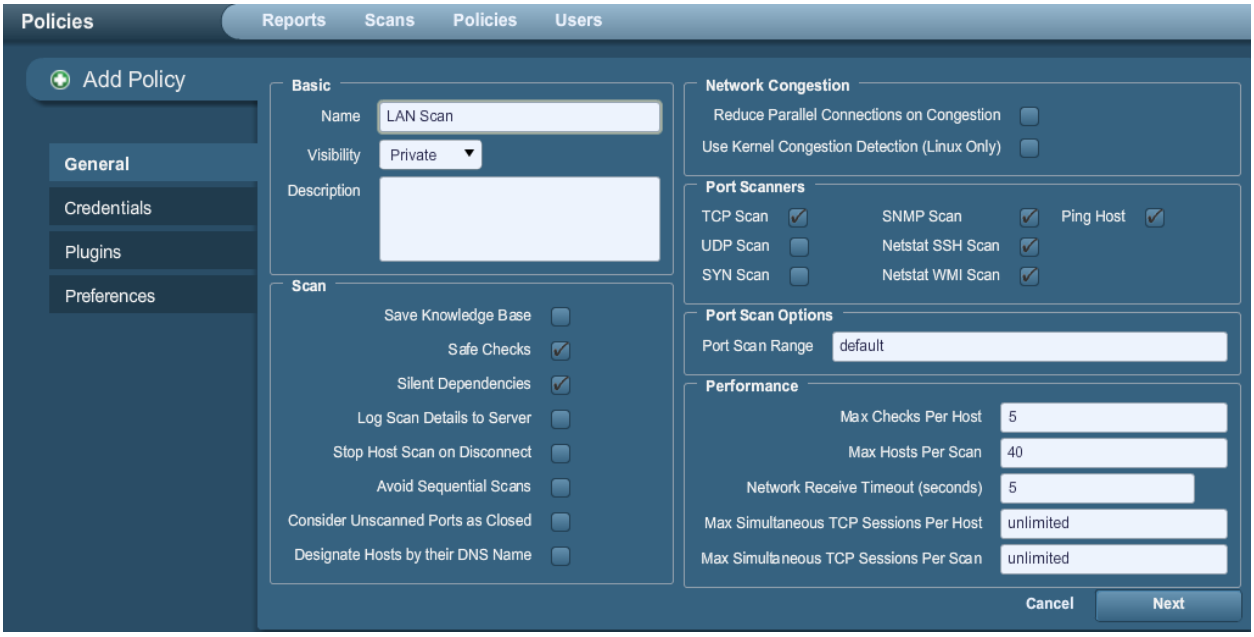
- Cisco IOS Compliance Checks (проверки соответствия для ОС Cisco IOS)
- Database Compliance Checks (проверки соответствия для баз данных)
- PCI DSS compliance (соответствие стандарту PCI DSS)
- PCI DSS Compliance: Passed (соответствие стандарту PCI DSS: подтверждено)
- PCI DSS Compliance: Tests Requirements (соответствие стандарту PCI DSS: требования к тестам)
- Unix Compliance Checks (проверки соответствия для ОС Unix)
- Windows Compliance Checks (проверки соответствия для ОС Windows)
- Windows File Contents Compliance Checks (проверки соответствия содержимого файлов ОС Windows)

Настройка политики сканирования

Чтобы включить проверки соответствия в Nessus, необходимо создать политику сканирования со следующими атрибутами:

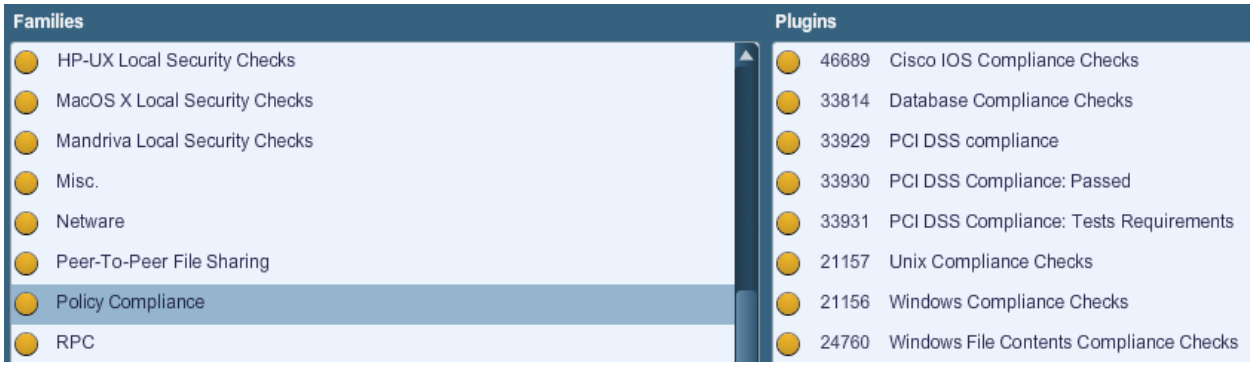
- включите подключаемые модули проверок соответствия, входящие в семейство подключаемых модулей «Policy Compliance» (соответствие политикам);
- укажите одну или несколько политик соответствия **`.audit`** в качестве предпочтительных;
- укажите реквизиты доступа к целевому серверу, включая реквизиты базы данных на вкладке «Preferences» (предпочтения), если это применимо;
- включите зависимости подключаемых модулей.

Важно понимать проверки выбранных файлов **`.audit`**, особенно в случае создания пользовательских файлов. В случае использования двух файлов **`.audit`** для одного сканирования оба файла объединяются с целью получения результатов каждого файла в рамках одного сканирования. В случае противоречий в результатах обработки этих двух файлов, можно получить один результат соответствия, а второй — несоответствия. Всегда проверяйте результаты, приведенные в отчетах.



Чтобы создать политику сканирования, обратитесь к интерфейсу пользователя Nessus, пройдите проверку подлинности и выберите «Policies» (политики). Отредактируйте существующую политику или создайте новую. Можете указать реквизиты доступа к целевому серверу на вкладке **Credentials** (учетные данные), расположенной слева.

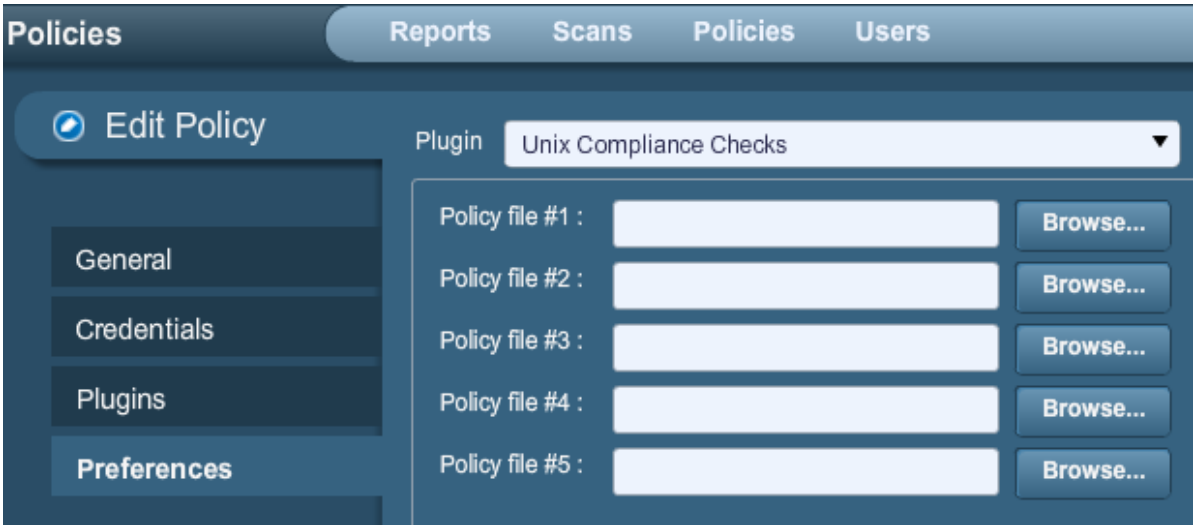
На вкладке **Plugins** (подключаемые модули) включите семейство подключаемых модулей «Policy Compliance» (соответствие политикам) и убедитесь, что параметр **`auto_enable_dependencies`** имеет значение «yes» в файле **`nessusd.conf`** (это значение по умолчанию):



Редактирование политики сканирования для проверки наличия модулей Policy Compliance (соответствие политикам)

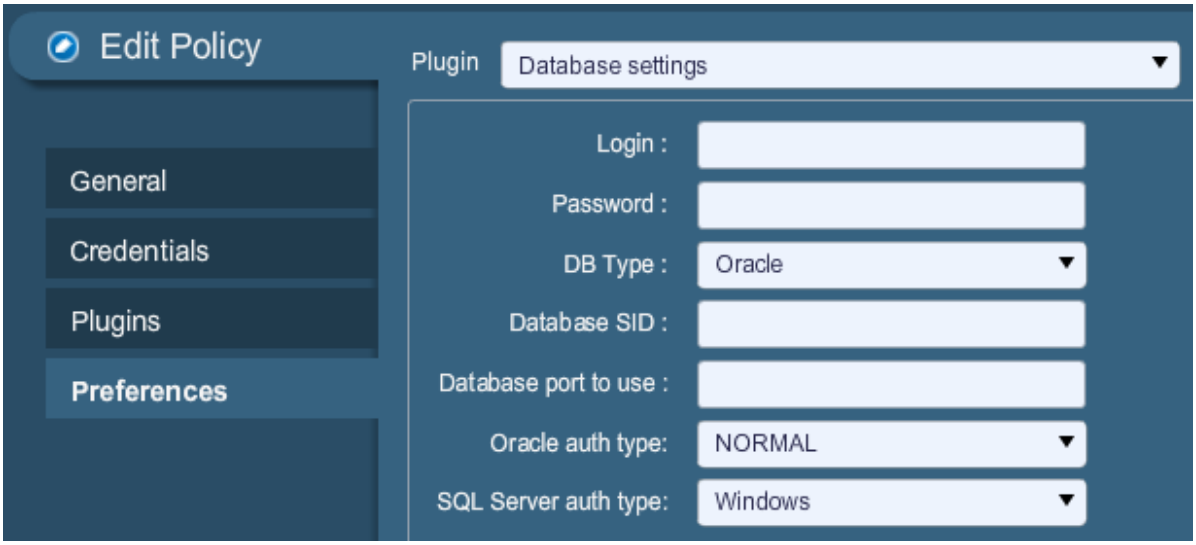
Чтобы включить использование файла **`.audit`** на вкладке **Preferences** (предпочтения) выберите в раскрывающемся меню «Cisco IOS Compliance Checks» (проверки соответствия для ОС Cisco IOS), «Unix Compliance Checks» (проверки соответствия для ОС Unix), «Windows Compliance Checks» (проверки соответствия для ОС Windows), «Windows File Content Compliance Checks» (проверки соответствия содержимого файлов ОС Windows) или «Database Compliance Checks» (проверки соответствия для баз данных). В каждом разделе будет пять полей, в которых можно указать отдельные

файлы `.audit`. Указанные файлы были прежде загружены на локальную клиентскую систему через портал Tenable Support Portal (портал поддержки Tenable).



Пример диалогового окна пользовательского интерфейса Nessus для указания файлов .audit для Unix

Если в предыдущем раскрывающемся меню был выбран вариант «Database Compliance Checks» (проверки соответствия для баз данных), то параметры входа для базы данных необходимо ввести на вкладке **Preferences** -> **Database Settings** (предпочтения -> настройки базы данных):



Доступные на вкладке «Database Settings» (настройки базы данных) параметры включают:

Параметр	Описание
Login (имя входа)	Имя пользователя для базы данных.
Password (пароль)	Пароль, соответствующий указанному имени пользователя.
DB Type (тип базы данных)	Поддерживаются базы данных Oracle, SQL Server, MySQL, DB2, Informix/DRDA и PostgreSQL.
Database SID (SID базы данных)	Системный идентификатор (SID) проверяемой базы данных. Применимы только Oracle, DB2 и Informix.
Oracle auth type (тип проверки подлинности Oracle)	Поддерживаются типы NORMAL, SYSOPER и SYSDBA.
SQL Server auth type (тип проверки подлинности SQL Server)	Поддерживаются типы Windows и SQL Server.

Для получения правильных значений этих полей обратитесь к локальному администратору баз данных.

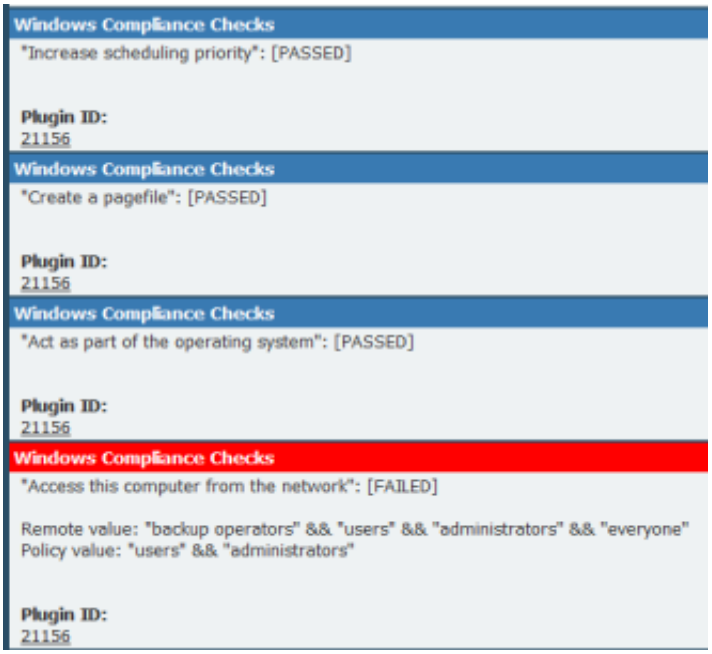
Теперь нажмите кнопку «Save» (сохранить) в нижней части окна, и настройка будет завершена. Новая политика сканирования будет добавлена в список управляемых политик сканирования.

Выполнение сканирования

Запуск сканирования с включенными проверками соответствия совершенно не отличается от запуска других сканирований аудита локальных исправлений или даже обычного сканирования сети. Фактически, все эти проверки при желании можно объединять для запуска одновременно.

Пример результатов

В Nessus 4 все результаты проверки соответствия возвращаются с идентификатором подключаемого модуля, выполнявшего тест. В приведенном ниже примере все данные, полученные в результате сканирования сервера под управлением ОС Windows, будут получены от подключаемого модуля «Windows Compliance» (соответствие ОС Windows) `.nbin` , определяемого как подключаемый модуль 21156.



Пример результатов соответствия, полученных в результате сканирования сервера Windows

Отчет в формате HTML может быть загружен через вкладку «Reports» (отчеты) пользовательского интерфейса Nessus 4, в нем успешно пройденные тесты соответствия отмечаются синим цветом и сопровождаются сообщением PASSED (пройден); не пройденные тесты обозначаются красным цветом и сопровождаются сообщением FAILED (не пройден), а элементы, которые не могут быть проверены, отмечаются желтым цветом и сопровождаются сообщением ERROR (ошибка).

В приведенном выше примере показаны только четыре элемента. Каждый из этих элементов получен из политики контроля доступа и проверяет наличие ненужных и небезопасных служб и протоколов. Некоторые из этих служб не были запущены и отвечают ожиданиям политики `.audit`, в то время как другие (например, служба удаленного реестра) были запущены и поэтому отмечены как «FAILED» (не пройден). Настоятельно рекомендуется настроить все отмеченные как «FAILED» (не пройден) элементы в соответствии со стандартами безопасности.

ПРИМЕР ИСПОЛЬЗОВАНИЯ NESSUS ДЛЯ ОС UNIX ПОСРЕДСТВОМ КОМАНДНОЙ СТРОКИ

Получение проверок соответствия стандартам

Если демон Nessus настроен на получение подключаемых модулей через канал ProfessionalFeed, то в каталоге подключаемых модулей «plugins» будет находиться пять файлов проверки соответствия `.nbin`.

Получите все необходимые файлы `.audit` через портал поддержки Tenable Support Portal по адресу https://support.tenable.com/support-center/ и поместите их в каталог подключаемых модулей plugins своего сканера. В большинстве установочных пакетов по умолчанию это следующий каталог:

/opt/nessus/lib/nessus/plugins

Эти подключаемые модули будут в числе более чем 40 000 файлов подключаемых модулей **.nasl** ,используемых сканером Nessus для сканирования уязвимостей. Их можно найти, выполнив поиск расширения **.nbin**, как показано ниже:

```
# ls compliance*nbin database*nbin unix*nbin cisco_compliance*nbin

cisco_compliance_check.nbin                 database_compliance_check.nbin
compliance_check.nbin                       unix_compliance_check.nbin
compliance_check_windows_file_content.nbin
```

Возможно наличие других файлов **.nbin**, предоставленных компанией Tenable, например подключаемого модуля Skype, который никак не связан с проверками соответствия.

При отсутствии локального доступа к фактическому демону Nessus, но наличии имени пользователя и пароля для входа на сервер, список подключаемых модулей можно запросить с помощью опции **–p** клиента командной строки **nessus**, как показано ниже:

```
# /opt/nessus/bin/nessus -xp 192.168.20.1 1241 username password | grep
      21156
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
21156|Policy Compliance|Checks if the remote system is compliant with the
      policy|infos|This script is Copyright (C) 2006 Tenable Network
      Security|Check compliance policy|$Revision: 1.3
      $|NOCVE|NOBID|NOXREF|\nSynopsis :\n\n Compliance
      checks\n\nDescription :\n\nUsing the supplied credentials this
      script perform a compliance\ncheck against the given
      policy.\n\nRisk factor :\n\nNone
```

Выполнение запроса может занять до пяти минут. Если запрос был выполнен успешно, но никаких данных получено не было, это значит, что проверки соответствия на удаленный сканер Nessus установлены не были.

Некоторые клиенты Nessus для Unix также позволяют загружать файлы. Например, клиент Nessus 4 для Mac OS X можно использовать для загрузки файла `.audit` на удаленную систему.

Использование файлов .nessus

Сканер Nessus может сохранять настроенные политики сканирования, целевые устройства сети и отчеты в файле **.nessus**. В разделе Пример использования пользовательского интерфейса Nessus описывается порядок создания файла **.nessus**, содержащего политику сканирования для проведения проверок соответствия. Инструкции по выполнению сканирования из командной строки с помощью файла **.nessus** см. в «Руководстве пользователя Nessus» по адресу: http://www.tenable.com/documentation/.

Использование файлов .nessusrc

Клиент командной строки Nessus также способен экспортировать настроенные политики сканирования в файлы **.nessusrc**. Это может быть удобно для обеспечения сканирования с помощью командной строки. В разделе Пример использования пользовательского интерфейса Nessus описывается порядок создания политики сканирования для проведения проверок соответствия в Nessus.

Чтобы вызвать сканирование с помощью Nessus посредством командной строки необходимо указать следующее:

- подключаемые модули проверки соответствия для ОС Unix, Windows или баз данных;
- реквизиты целевых хостов, которые будут сканироваться;
- один или несколько файлов **.audit** для работы подключаемых модулей проверки соответствия;
- что зависимости включены.

Соответствующие записи в файле **.nessusrc** имеют следующий формат (часть содержимого пропущена):

```
begin(SERVER_PREFS)
…
auto enable dependencies = yes
…
end(SERVER_PREFS)
begin(PLUGINS_PREFS)
…
Compliance policy file(s) : =
       federal_nsa_microsoft_xp_file_permissions.audit
…
end(PLUGINS_PREFS)
begin(PLUGIN_SET)
 21156 = yes
 21157 = yes
…
End(PLUGIN_SET)
```

В предыдущем примере многие части данных, указывающих, какое сканирование можно выполнить, опущены. Пропущенный текст содержит разрешение использования конкретного файла политики **.audit**, включение зависимостей и сами подключаемые модули проверок соответствия.

Выполнение сканирования

Запуск сканирования с включенными проверками соответствия совершенно не отличается от запуска других сканирований аудита локальных исправлений или даже обычного сканирования сети. Фактически, все эти проверки при желании можно объединять для запуска одновременно.

Пример результатов

Как и в случае клиентов с графическим интерфейсом, все обнаруженные соответствия и несоответствия требованиям отображаются в следующем формате:

```
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Reset lockout account
      counter after" : [FAILED]\n\nRemote value: 30\nPolicy value:
      20\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password
      length" : [FAILED]\n\nRemote value: 0\nPolicy value: 8\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password age" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 1\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Maximum password age" :
      [FAILED]\n\nRemote value: 42\nPolicy value: 182\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Enforce password
      history" : [FAILED]\n\nRemote value: 0\nPolicy value: 5\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout
      threshold" : [FAILED]\n\nRemote value: 0\nPolicy value: 3\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout
      duration" : [FAILED]\n\nRemote value: 30\nPolicy value: 60\n\n\n
```

Эти данные имеют формат отчета **.nsr** сканера Nessus. Это все события несоответствия требованиям.

ИСПОЛЬЗОВАНИЕ КОНСОЛИ SECURITYCENTER

Приведенная ниже информация основана на выполнении сканирований на соответствие стандартам с помощью консоли SecurityCenter 4 или более поздних версий. Пользователям версии Security Center 3.x следует использовать документацию консоли Security Center 3.4, доступную на портале Tenable Support Portal: https://support.tenable.com/support-center/.

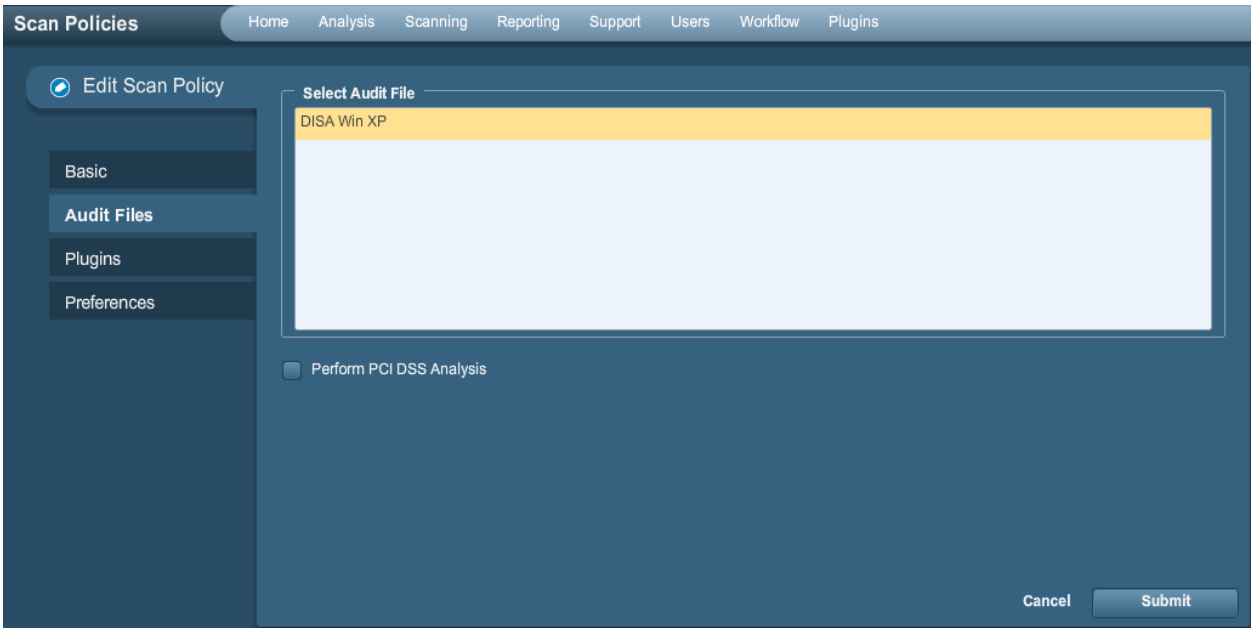
Получение проверок соответствия стандартам

Все клиенты SecurityCenter имеют доступ к подключаемым модулям канала Nessus ProfessionalFeed. Это включает подключаемые модули соответствия Cisco, Unix, Windows, Windows File Contents и Database. Эти подключаемые модули позволяют пользователю загружать на сервер и выполнять сканирования на соответствие стандартам с помощью предварительно созданных и настраиваемых файлов **.audit**, поставляемых компанией Tenable. Любые необходимые файлы **.audit** можно получить на портале Tenable Support Portal по адресу https://support.tenable.com/support-center/**.** Эти файлы **.audit** может загрузить в консоль SecurityCenter любой пользователь, имеющий разрешение Create Audit Files (создание файлов аудита), с помощью средства Add Audit File (добавление файлов аудита) на вкладке Support (поддержка).

Любые файлы **.audit**, загруженные в консоль SecurityCenter, будут доступны любому пользователю SecurityCenter, имеющему разрешение Create Policies (создание политик). Консоль SecurityCenter также выполняет распространение новых и загруженных на сервер файлов **.audit** для сканеров Nessus.

Настройка политики сканирования для выполнения аудита соответствия

Для выполнения сканирования на соответствие стандартам с помощью консоли SecurityCenter пользователи должны настроить политику сканирования с определенными настройками, касающимися соответствия. В этой политике определяются параметры сканирования, файлы аудита, включенные подключаемые модули и дополнительные предпочтения. На второй странице политики сканирования указываются файлы **.audit**, которые будут использоваться для аудита соответствия.



Здесь можно выбрать один или несколько файлов **.audit**, выделив файл **.audit** и нажав кнопку Submit (отправить). Для выбора нескольких файлов **.audit** используйте клавишу «Ctrl». Если требуется базовый анализ PCI DSS, до отправки проверьте, чтобы был установлен флажок Perform PCI DSS Analysis (выполнить анализ PCI DSS).

Стандарты безопасности данных в сфере платежных карт (PCI DSS) представляют собой комплексный набор стандартов безопасности, составленный учредителями совета

PCI Security Standards Council, включая Visa, American Express, Discover Financial Services и MasterCard. Стандарт PCI DSS предназначен для обеспечения общего эталона безопасности конфиденциальных данных держателей платежных карт для всех марок банковских карт. Этот стандарт используется многими представителями электронной коммерции, которые принимают и хранят данные кредитных карт.

Компания Tenable предоставляет три подключаемых модуля всем пользователям консоли SecurityCenter, которые автоматизируют процесс выполнения аудита PCI DSS. Это следующие подключаемые модули:

- PCI DSS compliance: tests requirements (соответствие стандарту PCI DSS: требования к тестам)
- PCI DSS compliance: passed (соответствие стандарту PCI DSS: подтверждено)
- PCI DSS compliance (соответствие стандарту PCI DSS)

Эти подключаемые модули оценивают результаты сканирования и фактическую конфигурацию сканирования для определения того, соответствует ли целевой сервер опубликованным требованиям соответствия PCI. Эти подключаемые модули не выполняют непосредственного сканирования, они проверяют результаты других подключаемых модулей. Чтобы активировать подключаемые модули PCI DSS, просто установите флажок Perform PCI DSS Analysis (выполнить анализ PCI DSS) в окне Compliance (соответствие).

Выбрав нужные файлы **.audit** и настройки PCI DSS, перейдите на вкладку Plugins (подключаемые модули) для подтверждения настроек подключаемых модулей. Для выполнения сканирования на соответствие стандартам в политике должны быть включены элементы семейства подключаемых модулей Policy Compliance (соответствие политике).

При выборе пользователем одного или нескольких файлов аудита на вкладке Audit Files (файлы аудита) политики сканирования необходимые подключаемые модули автоматически включаются на вкладке Plugins (подключаемые модули). Консоль SecurityCenter анализирует выбранные файлы **.audit** и включает на основании указанного в файле типа нужные подключаемые модули.

В семействе Policy Compliance (соответствие политике) есть семь подключаемых модулей для аудита соответствия. Ниже указаны эти подключаемые модули:

Идентификатор подключаемого модуля	Имя подключаемого модуля	Описание подключаемого модуля
21156	Windows Compliance Checks (проверки соответствия для ОС Windows)	Используется для аудита общих настроек Windows.
21157	Unix Compliance Checks (проверки соответствия для ОС Unix)	Используется для аудита общих настроек Unix.

24760	Windows File Contents Compliance Checks (проверки соответствия содержимого файлов ОС Windows)	Используется для аудита конфиденциального содержимого файлов на серверах Windows.
33814	Database Compliance Checks (проверки соответствия для баз данных)	Используется для аудита общих настроек баз данных.
33929	PCI DSS compliance (соответствие стандарту PCI DSS)	Определяет, содержит ли удаленный веб-сервер уязвимости для атак межсайтовыми скриптами (XSS), использует ли старую криптографию SSL2.0, выполняет ли устаревшее программное обеспечение , подвержен ли опасным уязвимостям (балл CVSS >= 4).
33930	PCI DSS Compliance: Passed (соответствие стандарту PCI DSS: подтверждено)	Используя имеющуюся информацию сканирования, сканер Nessus не обнаружил каких-либо не соответствующих стандарту нарушений на этом хосте.
33931	PCI DSS Compliance: Tests Requirements (соответствие стандарту PCI DSS: требования тестов)	Анализ соответствия сканирования Nessus требованиям к тестам PCI. Даже в случае прохождения технических тестов этот отчет может быть недостаточен для сертификации сервера.
46689	Cisco IOS Compliance Checks (проверки соответствия ОС Cisco IOS)	Используется для аудита общих настроек устройств Cisco.

Управление учетными данными

Одно из преимуществ консоли SecurityCenter при выполнении сканирований с использованием учетных данных состоит в том, что она помогает управлять используемыми учетными данными. Учетные данные в консоли SecurityCenter можно создать, перейдя на вкладку Support (поддержка), нажав кнопку Credentials (учетные данные) и кнопку Add (добавить).

Учетные данные Unix, Windows и Cisco хранятся и управляются отдельно от политики сканирования. Учетные данные могут создаваться с видимостью User (пользователь) для текущего пользователя или Organizational (организация). В последнем случае они могут использоваться другими пользователям консоли SecurityCenter. Это позволяет пользователям работать с результатами сканирований и выполнять новые сканирования без необходимости знать фактические учетные данные, используемые в сканировании.

Для сканирования систем баз данных требуются дополнительные учетные данные. Эти учетные данные сохраняются в политике сканирования и настраиваются через Database settings (настройки базы данных) (подключаемый модуль 33815) в предпочтениях политики сканирования. Эти учетные данные настраиваются отдельно от учетных данных, указанных в предыдущем абзаце.

Анализ результатов

Консоль SecurityCenter может использоваться различными методами для анализа и отчетности по данным соответствия, возвращенным сканированиями Nessus. Распространенные отчеты включают следующие.

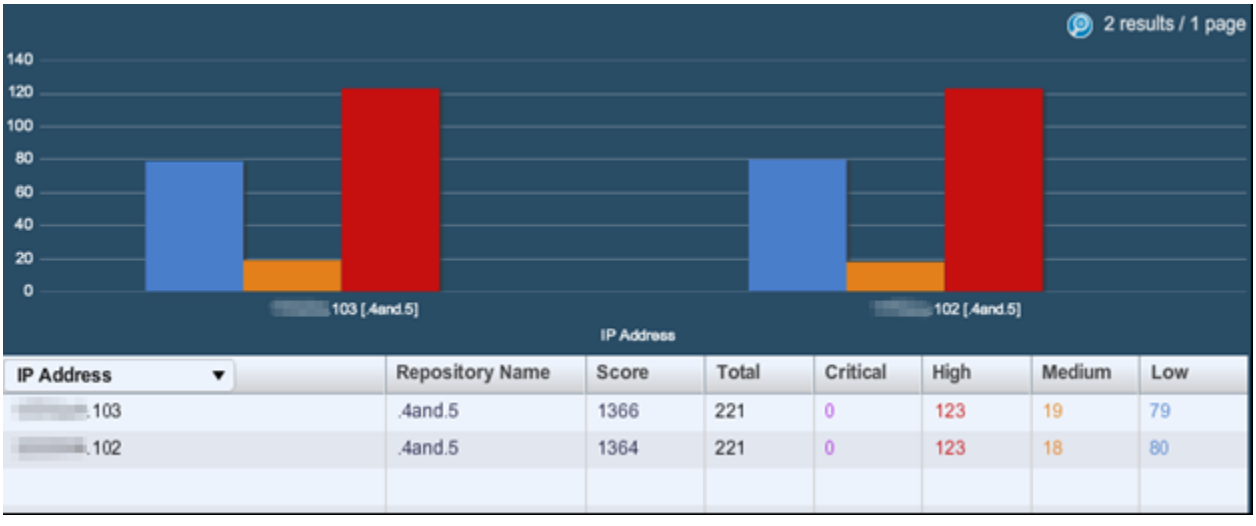
- Список всех соответствующих и не соответствующих стандартам уязвимостей по группам ресурсов.
- Список всех соответствующих и не соответствующих стандартам уязвимостей по хостам или сетям.
- Обзор всех не соответствующих стандартам проблем.
- Аудит настроек базы данных на наличие распространенных ошибок конфигурации.
- Отчетность о статусе пользователей или программного обеспечения на основании ИТ-потребностей.

После получения данных о соответствии стандартам с помощью консоли SecurityCenter можно воспользоваться билетами, отчетностью и аналитическими средствами для определения оптимального порядка действий для изменения конфигурации проверенных аудитом устройств. Эти данные могут быть проанализированы параллельно с другой информацией об уязвимостях, исправлениях безопасности или пассивно обнаруженной информацией.

Ниже приведены примеры снимков экрана консоли SecurityCenter при использовании для анализа информации соответствия стандартам о сканируемых хостах:

Plugin ID	Total	Severity	Name
1000282	4	Low	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\allocatedasd
1000295	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlog\\AutoAdminLogon
1000294	4	Low	HKLM\\System\\CurrentControlSet\\Control\\SecurePipeServers\\Winreg\\AllowedPaths\\Machine
1000293	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionPipes
1000292	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionShares
1000291	4	Medium	HKLM\\Software\\Policies\\Microsoft\\Cryptography\\ForceKeyProtection
1000290	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\ForceGuest
1000289	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\LimitBlankPasswordUse
1000288	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinClientSec
1000287	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinServerSec
1000286	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\NoDefaultAdminOwner
1000285	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LDAP\\LDAPClientIntegrity
1000284	4	Low	HKLM\\Software\\Microsoft\\Driver Signing\\Policy
1000283	4	High	HKLM\\software\\microsoft\\non-driver signing\\policy
1000296	4	Low	HKLM\\System\\CurrentControlSet\\Control\\FileSystem\\NtfsDisable8dot3NameCreation
1000281	4	High	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\scremoveoption
1000280	4	High	HKLM\\system\\currentcontrolset\\control\\lsa\\lmcompatibilitylevel
1000279	4	High	HKLM\\system\\currentcontrolset\\control\\print\\providers\\lanman print services\\servers\\addprinterdrive
1000278	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\AutoAdminLogon
1000277	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkNoDialIn
1000276	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkHideSharePwds
1000275	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDriveTypeAutoRun
1000274	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\PerformRouterDiscovery
1000273	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\SynAttackProtect
1000272	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\DisableIPSourceRouting
1000271	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\KeepAliveTime
1000270	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableDeadGWDetect
1000269	4	High	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableICMPRedirect

Пример списка данных аудита соответствия, просматриваемого с помощью консоли SecurityCenter



IP Address	Repository Name	Score	Total	Critical	High	Medium	Low
.103	.4and.5	1366	221	0	123	19	79
.102	.4and.5	1364	221	0	123	18	80

Пример списка данных аудита соответствия, просматриваемого с помощью консоли SecurityCenter по серверам

Дополнительные сведения об использовании консоли SecurityCenter см. в документации SecurityCenter, доступной по адресу https://support.tenable.com/support-center/.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Компания Tenable подготовила различные документы, содержащие подробные сведения об установке, развертывании, настройке, пользовательской эксплуатации и общем тестировании сканера Nessus:

- **Руководство по установке Nessus** — пошаговое руководство по установке.
- **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.
- **Справочник по проверкам соответствия Nessus** — полное руководство по синтаксису проверок соответствия Nessus.
- **Формат файлов Nessus v2** — содержит описание структуры формата файлов `.nessus`, который был введен с версиями Nessus 3.2 и NessusClient 3.2.
- **Спецификация протокола Nessus XML-RPC** — содержит описание протокола XML-RPC и интерфейса в Nessus.
- **Контроль соответствия в режиме реального времени** — содержит обзор того, как решения компании Tenable могут использоваться для обеспечения выполнения разных типов государственных и финансовых норм.

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

О КОМПАНИИ TENABLE NETWORK SECURITY

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

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