Проверки Nessus с использованием учетных данных для ОС Unix и Windows

15 июня 2011 г.

(редакция 25)

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 выполнения сканирования сетей с проверкой подлинности при помощи сканера уязвимостей **Nessus** компании Tenable Network Security. Сканирование сетей с проверкой подлинности позволяет осуществлять удаленный аудит сетей для получения данных о хостах, таких как не установленные исправления и настройки операционной системы. Мы будем рады получить ваши комментарии и предложения по адресу электронной почты support@tenable.com.

Сканер Nessus использует возможность входа в систему удаленных хостов Unix через протокол Secure Shell (SSH). Для хостов Windows сканер Nessus использует различные технологии проверки подлинности Microsoft.

Обратите внимание, что сканер Nessus также использует протокол SNMP для выполнения запросов о версии и информационных запросов к удаленным маршрутизаторам и коммутаторам. Хотя это также явдяется разновидностью «локальных проверок», данный вопрос не рассматривается в настоящем документе.

В этом документе большинство ссылок делается на сканер Nessus, но основные концепции также верны для консоли SecurityCenter компании Tenable.

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
/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.

ОБЗОР ПРОВЕРОК NESSUS С ИСПОЛЬЗОВАНИЕМ УЧЕТНЫХ ДАННЫХ

Сканер Nessus компании Tenable – очень эффективный сканер уязвимостей сети, оснащенный обширной базой подключаемых модулей, которые проверяют широкий спектр уязвимостей с возможностью удаленного взлома системы. Помимо удаленного

сканирования, сканер Nessus также может использоваться для сканирования локальных уязвимостей.

Назначение

Внешнее сканирование уязвимостей сети используется для получения моментальных сведений о работающих в системе службах и уязвимостях, которые они могут содержать. Однако, это лишь внешний взгляд на ситуацию. Важно определить, какие работают локальные службы, для выявления уязвимостей безопасности от локальных атак или настроек конфигурации, которые могут подвергнуть систему внешним атакам, что невозможно выполнить с помощью внешнего сканирования.

При типовой оценке уязвимостей сети удаленное сканирование выполняется в отношении внешних точек, а локальное сканирование выполняется из самой сети. Ни один из этих видов сканирования не позволяет определить локальные уязвимости сканируемой системы. Некоторая полученная информация основывается на данных заголовков, которые могут быть неоднозначными или неверными. С помощью защищенных учетных данных сканер Nessus может получить локальный доступ для сканирования целевой системы без использования агента. Это может быть полезно для сканирования очень больших сетей с целью определения локальных уязвимостей или нарушений стандартов.

Наиболее распространенной проблемой безопасности в организациях является несвоевременное применение исправлений безопасности. Сканирование Nessus с использованием учетных данных позволяет быстро определить, на каких системах своевременно не установлены исправления. Это особенно важно, когда публикуются новые уязвимости и руководство организации хочет быстро получить ответ в отношении их влияния на организацию.

Еще одной крупной заботой для организаций является определение соответствия принятой в организации политике, отраслевым стандартам (например, стандартам центра Center for Internet Security (CIS)) или законодательным нормам (например, законам Сарбейнса-Оксли (SOX), Грэмма-Лича-Блайли (GLBA) или HIPAA). Организации, принимающие данные кредитных карт, должны демонстрировать соответствие стандартам безопасности Payment Card Industry Data Security Standards (PCI DSS). Было значительное количество широко опубликованных случаев, когда конфиденциальность данных кредитных карт миллионов клиентов была нарушена. Это представляет существенные финансовые потери для банков, несущих ответственность за покрытие платежей, уплату крупных штрафов или потерю возможностей принимать кредитные карты нарушившим конфиденциальность торговцем или платежной системой.

Уровень доступа

При сканировании с использованием учетных данных могут выполняться любые операции, доступные локальным пользователям. Уровень сканирования зависит от прав, предоставленных учетной записи пользователя, которая используется сканером Nessus.

Обычные пользователи с локальным доступом на системах Unix могут определять основные проблемы безопасности, например уровни исправлений или записи файла **`/etc/passwd`**. Для получения более полной информации, например данных о конфигурации системы или файла разрешений, действующего в рамках всей системы, необходима учетная запись с правами уровня root.

Для сканирования с использованием учетных данных систем Windows требуется учетная запись уровня администратора. Несколько бюллетеней и обновлений программного обеспечения, выпущенных корпорацией Microsoft, сделали чтение реестра для определения уровня программных исправлений ненадежным без прав администратора. Для выполнения непосредственного чтения файловой системы требуется доступ администратора. Это позволяет сканеру Nessus подключиться к компьютеру и выполнить непосредственный анализ для определения истинного уровня исправлений, установленных на оцениваемых системах. В операционной системе Windows XP Pro такой доступ к файлам действует только при использовании локальной учетной записи администратора, если политика «Network access: Sharing and security model for local accounts» (сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей) изменена на «Classic – local users authenticate as themselves» (обычная - локальные пользователи удостоверяются как они сами).

Используемые технологии

Особой проблемой при выполнении сканирования с использованием учетных данных является автоматическое предоставление наделенных привилегиями учетных данных сканеру с соблюдением безопасности. Очевидно, цель сканирования уязвимостей безопасности не будет достигнута, если при этом откроется еще более значительная уязвимость! Сканер Nessus поддерживает использование нескольких защищенных методов решения этой проблемы на обеих платформах, Unix и Windows.

Системы Unix

На системах Unix сканер Nessus использует программы на основе протокола Secure Shell (SSH) версии 2 (например, OpenSSH, Solaris SSH и т. д.) для проверок на базе хоста. Этот механизм шифрует передаваемые данные для защиты этих данных от просмотра программами-анализаторами сетевых пакетов. Сканер Nessus поддерживает три типа методов проверки подлинности для использования с SSH: имя пользователя и пароль, открытые и закрытые ключи, а также система Kerberos.

Имя пользователя и пароль

Несмотря на поддержку этого метода, компания Tenable не рекомендует использовать имя пользователя и пароль для проверки подлинности с помощью SSH. Статические пароли подвержены атакам типа «злоумышленник в середине» и атакам методом подбора, когда они используются в течение продолжительного времени.

Открытые и закрытые ключи

Шифрование с открытым ключом, также называемое шифрованием с ассиметричными ключами, является более надежным механизмом проверки подлинности с использованием пары ключей, открытого и закрытого. В ассиметричной криптографии открытый ключ используется для шифрования данных, а закрытый ключ — для дешифровки. Использование открытого и закрытого ключа представляет собой более безопасный и гибкий метод для проверки подлинности SSH. Сканер Nessus поддерживает оба формата ключей, DSA и RSA.

Kerberos

Система Kerberos, разработанная проектом MIT Project Athena, является приложением клиент/сервер, которое использует протокол шифрования с симметричными ключами. При симметричном шифровании ключ, используемый для шифрования данных, совпадает с ключом, используем для дешифровки. Организации развертывают центр KDC (центр распространения ключей), содержащий данные всех пользователей и служб, которым требуется проверка подлинности Kerberos. Пользователи проходят

проверку подлинности Kerberos, запрашивая билет предоставления билета (TGT). После получения пользователем билета TGT он может использоваться для запроса билетов служб из центра KDC для использования других служб на основе Kerberos. Kerberos использует для шифрования всех обменов данными протокол шифрования CBC (Cipher Block Chain) DES.

Используемая в сканере Nessus реализация проверки подлинности Kerberos для SSH поддерживает алгоритмы шифрования aes-cbc и aes-ctr. Ниже приведен обзор взаимодействия сканера Nessus с системой Kerberos.

- Конечный пользователь предоставляет IP-адрес центра KDC.
- **nessusd** запрашивает **sshd**, поддерживается ли проверка подлинности Kerberos.
- **sshd** отвечает «да».
- **nessusd** запрашивает билет Kerberos TGT, а также имя для входа и пароль.
- Kerberos отправляет билет **nessusd**.
- **nessusd** предоставляет билет **sshd**.
- **nessusd** выполняет вход.

Системы Windows

Сканер Nessus поддерживает несколько разных типов методов проверки подлинности для систем на основе Windows. В каждом из этих методов используется имя пользователя, пароль и имя домена (иногда используется как дополнительный элемент проверки подлинности).

LanMan

Метод проверки подлинности LanMan имел наибольшее распространение на серверных установках ОС Windows NT и первых выпусков Windows 2000. Он практически не используется на более новых выпусках ОС Windows, но сохраняется для обратной совместимости.

NTLM и NTLMv2

Метод проверки подлинности NTLM, введенный в ОС Windows NT, обеспечил повышенную безопасность по сравнению с проверкой подлинности LanMan. Однако расширенная версия NTLMv2 криптографически более надежна, чем NTLM, и используется сканером Nessus при попытке входа в сервер Windows как метод проверки подлинности по умолчанию.

Подписывание SMB-пакетов

Подписывание SMB-пакетов включает вычисление криптографической контрольной суммы, применяемое ко всему входящему и исходящему трафику сервера Windows. Многие системные администраторы включают эту функцию на своих серверах для обеспечения 100 % проверки подлинности пользователей и их принадлежности домену. Эта функция используется сканером Nessus автоматически, если требуется удаленным сервером Windows.

SPNEGO

Протокол SPNEGO (Simple and Protected Negotiate) обеспечивает возможность единого входа (SSO) с клиента Windows во многие защищенные ресурсы с помощью учетных данных для входа пользователя Windows. Сканер Nessus поддерживает использование

протокола SPNEGO с проверкой подлинности NTLMSSP с LMv2 или Kerberos и шифрованием RC4.

Kerberos

Сканер Nessus также поддерживает использование проверки подлинности Kerberos в домене Windows. Для настройки этой возможности должен быть предоставлен IP-адрес контроллера домена Kerberos Domain Controller (фактически, IP-адрес сервера Windows Active Directory Server).

NTLMSSP (NT Lan Manager Security Support Provider) и LMv2

Если расширенная схема безопасности (например, Kerberos или SPNEGO) не поддерживается или выдает ошибку, сканер Nessus выполнит попытку входа через проверку подлинности NTLMSSP/LMv2. Если и это не получится, сканер Nessus выполнит попытку входа с использованием проверки подлинности NTLM.

Имена пользователей, пароли и домены Windows

Поле домена SMB является необязательным, и сканер Nessus сможет выполнить вход с учетными данными домена без этого поля. Имя пользователя, пароль и необязательное поле домена ссылаются на учетную запись, которая известна целевой машине. Например, при наличии имени пользователя joesmith и пароля **`my4x4mpl3`** сервер Windows сначала ищет это имя пользователя в списке пользователей локальной системы, а затем проверяет, принадлежит ли оно какому-либо домену этой системы.

Фактическое имя домена требуется, только если имя учетной записи домена отличается от имени учетной записи компьютера. Вполне допускается наличие учетной записи Administrator (администратор) на сервере Windows и в домене. В этом случае для входа в локальный сервер имя пользователя Administrator используется с паролем соответствующей учетной записи. Для входа в домен также используется имя пользователя Administrator, но с паролем домена и именем домена.

Независимо от используемых учетных данных, сканер Nessus всегда пытается войти в сервер Windows со следующими комбинациями.

- Administrator с паролем.
- Случайное имя пользователя и пароль для тестирования гостевых учетных записей (Guest).
- Без имени пользователя или пароля для тестирования пустых сеансов.

ПРОВЕРКИ С ИСПОЛЬЗОВАНИЕМ УЧЕТНЫХ ДАННЫХ НА ПЛАТФОРМАХ UNIX

Описанный в этом разделе процесс позволяет выполнять локальные проверки безопасности на системах на базе ОС Unix. В этом примере используется демон SSH OpenSSH. В случае использования коммерческого варианта SSH эта процедура может немного отличаться.

Есть два основных метода, которые могут использоваться для включения локальных проверок безопасности.

1. Использование пары открытого и закрытого ключей SSH.
2. Учетные данные пользователя и доступ `sudo` или учетные данные для доступа `su`.

Необходимые условия

Требования к конфигурации для SSH

Сканер Nessus 4.x поддерживает алгоритмы blowfish-cbc, aesXXX-cbc (aes128, aes192 и aes256), 3des-cbc и aes-ctr.

Некоторые коммерческие варианты сервера SSH не поддерживают алгоритм blowfish, вероятно, по причинам экспорта. Также можно настроить сервер SSH, чтобы он принимал только определенные типы шифрования. Проверьте свой сервер SSH, чтобы убедиться в поддержке нужного алгоритма.

Привилегии пользователя

Для обеспечения максимальной эффективности пользователь SSH должен иметь возможность выполнять любые команды в системе. В системах Unix такие права называются привилегиями **root**. Хотя некоторые проверки (например, проверки уровней исправлений) можно выполнять с обычным доступом, полные проверки соответствия стандартам, которые выполняют аудит конфигурации системы и разрешений для файлов, требуют доступа уровня root. По этой причине при наличии возможности настоятельно рекомендуется использовать ключи SSH вместо учетных данных.

Требования к конфигурации для Kerberos

При использовании Kerberos необходимо настроить **sshd** с поддержкой Kerberos для проверки билета с помощью центра KDC. Для этого должен быть надлежащим образом настроен обратный просмотр DNS. Должен быть установлен метод взаимодействия Kerberos **gssapi-with-mic**.

Включение локальных проверок безопасности SSH на ОС Unix

В этом разделе приведена процедура высокого уровня, предназначенная для включения протокола SSH между системами, участвующими в проверках Nessus с использованием учетных данных. Этот раздел не предназначен для углубленного изучения SSH. Предполагается, что читатель обладает необходимыми знаниями о командах системы Unix.

Генерирование открытых и закрытых ключей SSH

Первым шагом является генерирование пары открытого и закрытого ключей для использования сканером Nessus. Эту пару ключей можно сгенерировать с любой системы Unix с использованием любой учетной записи пользователя. Однако важно, чтобы ключи принадлежали определенному пользователю сервера Nessus.

Чтобы сгенерировать пару ключей, воспользуйтесь служебной программой **ssh-keygen** и сохраните ключ в надежном месте. В следующем примере ключи генерируются на системе Red Hat ES 3.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
       /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Не передавайте закрытый ключ на какую-либо систему, кроме той, на которой работает сервер Nessus. Когда служебная программа **ssh-keygen** запросит парольную фразу, введите надежную парольную фразу или нажмите клавишу Enter дважды (т. е. не устанавливайте никакой парольной фразы). В случае установки парольной фразы это должно быть указано в параметрах Policies -> Credentials -> SSH settings (политики -> учетные данные -> настройки SSH), чтобы сканер Nessus использовал проверку подлинности на основе ключей.

Пользователи Nessus Windows могут скопировать оба ключа в основной каталог приложения Nessus на системе, на которой работает сервер Nessus (по умолчанию **C:\Program Files\Tenable\Nessus**), а затем копировать открытый ключ на нужные целевые системы. Так проще управлять файлами открытого и закрытого ключей.

Создание учетной записи пользователя и настройка ключа SSH

На каждой целевой системе, которая будет сканироваться с помощью локальных проверок безопасности, создайте новую учетную запись, предназначенную специально для сканера Nessus. Эта учетная запись пользователя должна иметь точно одинаковое имя на всех системах. В этом документе использовано имя пользователя nessus, но можно использовать любое имя.

После создания учетной записи для этого пользователя проверьте, что этой учетной записи не присвоен действительный пароль. На системах Linux новые учетные записи пользователей по умолчанию заблокированы, если в явной форме не установлен начальный пароль. В случае использования учетной записи, для которой установлен пароль, воспользуйтесь командой **passwd –l** для блокировки учетной записи.

Необходимо также создать каталог в домашнем каталоге этой новой учетной записи для хранения открытого ключа. В этом примере каталог имеет имя **/home/nessus/.ssh**. Ниже приведен пример для систем Linux:

```
# passwd –l nessus
# cd /home/nessus
# mkdir .ssh
#
```

Для систем Solaris 10 компания Sun расширила команду **passwd(1)**, обеспечив различие между заблокированными и не дающими возможности входа учетными записями (non-login account). Эта функция предназначена для того, чтобы заблокированная учетная запись пользователя не могла использоваться для выполнения команд (например, задач службы cron). Не дающие возможности входа учетные записи используются только для выполнения команд и не поддерживают интерактивных сеансов входа. Эти учетные записи имеют маркер NP в поле пароля **/etc/shadow**. Для настройки не

дающей возможности входа учетной записи и создания каталога с открытым ключом SSH в ОС Solaris 10 выполните следующие команды:

```
# passwd -N nessus

# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

После создания учетной записи пользователя необходимо передать ключ в нужную систему, поместить его в соответствующий каталог и установить правильные разрешения.

Пример

Из системы, в которой находятся ключи, скопируйте безопасным методом открытый ключ в систему, которая будет сканироваться проверками хоста, как показано ниже. 192.1.1.44 — пример удаленной системы, которая будет тестироваться с помощью проверок на базе хоста.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

Скопировать файл с системы, на которой установлен сканер Nessus, также можно с помощью команды защищенного протокола FTP, **sftp**. Обратите внимание, что файл на целевой системе должен иметь имя authorized_keys.

Вернитесь к системе, в которой располагается открытый ключ

Установите разрешения для каталога **/home/nessus/.ssh** и файла **authorized_keys**.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Повторите этот процесс на всех системах, которые будут тестироваться проверками SSH (начиная с пункта «Создание учетной записи пользователя и настройка ключа SSH» выше).

Выполните тест, чтобы определить правильность конфигурации учетных записей и сетей. С помощью простой команды ОС Unix **id** со сканера Nessus выполните следующую команду:

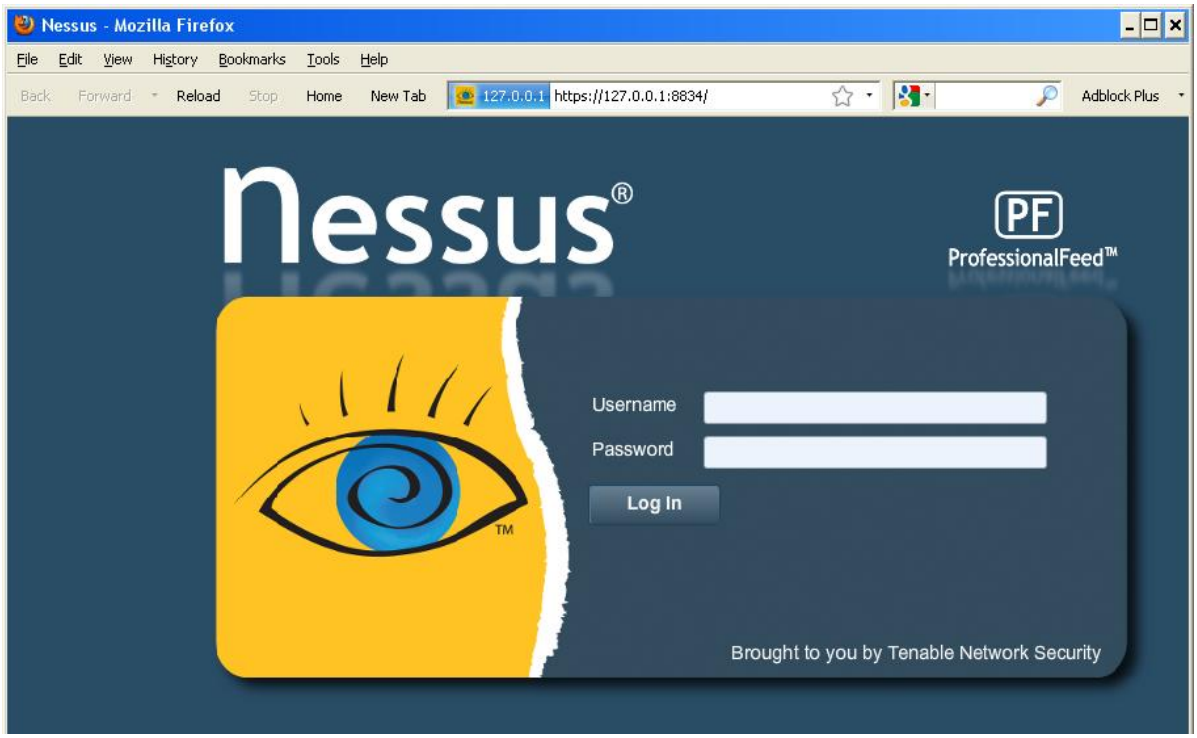
```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Если она успешно вернет информацию о пользователе nessus, то обмен ключами прошел успешно.

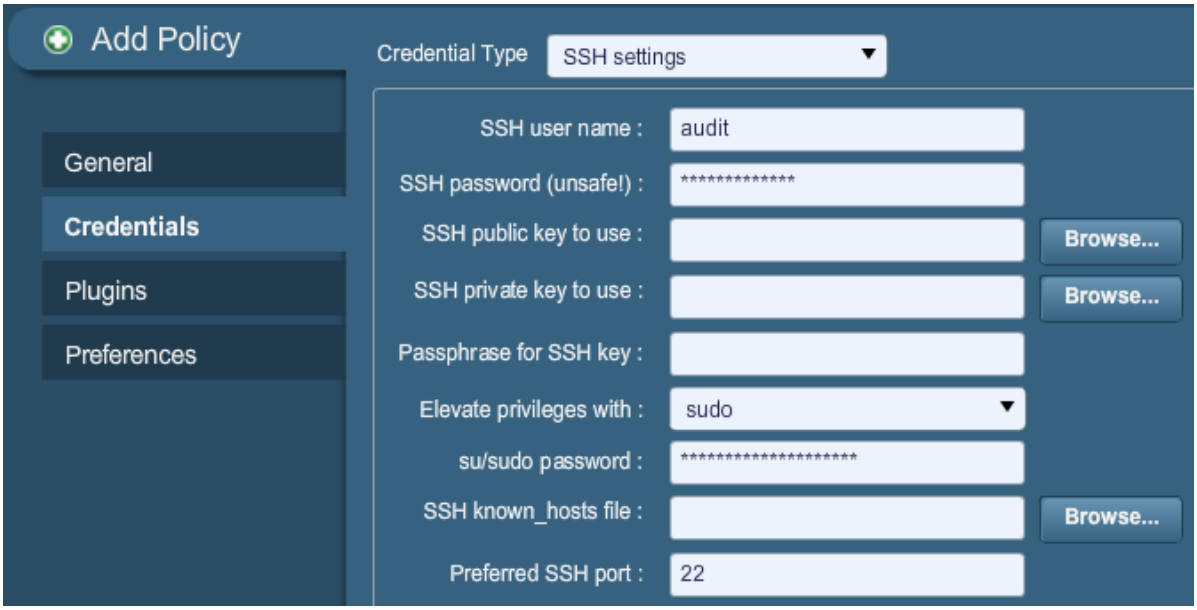
Настройка сервера Nessus для проверок SSH на базе хоста

Интерфейс пользователя Nessus

Если это еще не сделано, безопасным методом скопируйте файлы закрытого и открытого ключа в систему, которая будет использоваться для доступа к сканеру Nessus.



Откройте веб-браузер и подключитесь к интерфейсу пользователя сканера Nessus, как показано выше, а затем выберите вкладку Policies (политики). Создайте новую политику или измените существующую и перейдите на вкладку Credentials (учетные данные), расположенную слева. Выберите из раскрывающегося меню, расположенного в верхней части окна, элемент SSH settings (настройки SSH), как показано ниже:



- В поле SSH user name (имя пользователя SSH) введите имя учетной записи, предназначенной для сканера Nessus, на каждой из сканируемых систем. По умолчанию установлено значение root.
- В случае использования пароля для протокола SSH введите его в поле SSH password (пароль SSH).
- А в случае использования вместо пароля ключей SSH (рекомендуется), нажмите кнопку Select (выбрать), расположенную рядом с полем SSH public key to use (открытый ключ SSH), и укажите расположение файла открытого ключа на локальной системе.
- Для поля SSH private key to use (закрытый ключ SSH) нажмите кнопку Select (выбрать) и укажите расположение файла закрытого ключа (связанного с указанным выше открытым ключом) на локальной системе.
- В случае использования парольной фразы для ключа SSH (не обязательно) введите ее в поле Passphrase for SSH key (парольная фраза для ключа SSH).
- Пользователи сканера Nessus и консоли SecurityCenter могут дополнительно вызвать команду **su** или **sudo** с помощью настройки поля Elevate privileges with (повысить уровень привилегий с помощью) и отдельного пароля.
- Если файл SSH **known_hosts** доступен и предоставлен в рамках политики сканирования в поле SSH known_hosts file (файл SSH known_hosts), сервер Nessus будет пытаться выполнить вход только в хосты, указанные в этом файле. Это помогает гарантировать, что имя пользователя и пароль, используемые вами для аудита известных серверов SSH, не будут использованы для попытки несанкционированного входа в систему.

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 команду **su** или **sudo** с отдельным паролем для учетной записи, которой присвоены права **su** или **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:

При использовании Kerberos необходимо настроить сканер Nessus для проверки подлинности через центр KDC. Выберите элемент Kerberos configuration (настройка Kerberos) из раскрывающегося меню, как показано ниже:

Порт центра KDC по умолчанию — 88, а транспортный протокол по умолчанию — udp. Другое значение транспортного протокола — tcp. И наконец, требуется имя Kerberos Realm (сфера Kerberos) и IP-адрес центра KDC.

Учтите, что для использования этого метода проверки подлинности заранее должна быть создана среда Kerberos.

Теперь нажмите кнопку **Submit** (отправить) в нижней части окна, и настройка будет завершена. Новая политика сканирования будет добавлена в список управляемых политик сканирования.

Командная строка Nessus Unix

Поддержка сканером Nessus проверок на базе хоста доступна в версии Nessus 2.2.0 и более поздних версиях и требует поддержки SSL. Выполните команду `nessusd -d` для проверки наличия соответствующей версии и библиотек SSL следующим образом:

```
# nessusd -d
This is Nessus 4.4.1. [build M15078] for Linux 2.6.13-15-smp
compiled with gcc version 4.0.2 20050901 (prerelease) (SUSE Linux)
Current setup :
        flavor                          : suse10.0-x86
        nasl                            : 4.4.1
        libnessus                       : 4.4.1
        SSL support                     : enabled
        SSL is used for client / server communication
        Running as euid                 : 0
Magic hash: 49edd1433ffad7b87b446a4201faeedf  -
OpenSSL: OpenSSL 0.9.7g 11 Apr 2005
Include these infos in your bug reports
```

Использование файлов .nessus

Сканер Nessus может сохранять настроенные политики сканирования, целевые устройства сети и отчеты в файле **.nessus**. В приведенном выше разделе «Интерфейс пользователя Nessus» описано создание файла **.nessus**, содержащего учетные данные SSH. Инструкции по выполнению сканирования из командной строки с помощью файла **.nessus** см. в «Руководстве пользователя Nessus» по адресу:

http://www.tenable.com/products/nessus/documentation

Использование файлов .nessusrc

В случае ручного создания файлов **.nessusrc** имеется несколько параметров, которые могут быть настроены для проверки подлинности SSH. Пример незаполненного списка приведен ниже:

```
Use SSH to perform local security checks[entry]:SSH user name : =
Use SSH to perform local security checks[file]:SSH public key to use : =
Use SSH to perform local security checks[file]:SSH private key to use : =
Use SSH to perform local security checks[password]:Passphrase for SSH key
      : =
SSH settings[entry]:SSH user name : =
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : = no
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
```

В случае использования Kerberos необходимо настроить сканер Nessus для проверки подлинности через центр KDC, введя следующую информацию в файл **nessusrc** сканера:

```
Kerberos KDC port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH Only) : myrealm
```

```
Kerberos Key Distribution Center (KDC): 192.168.20.66
```

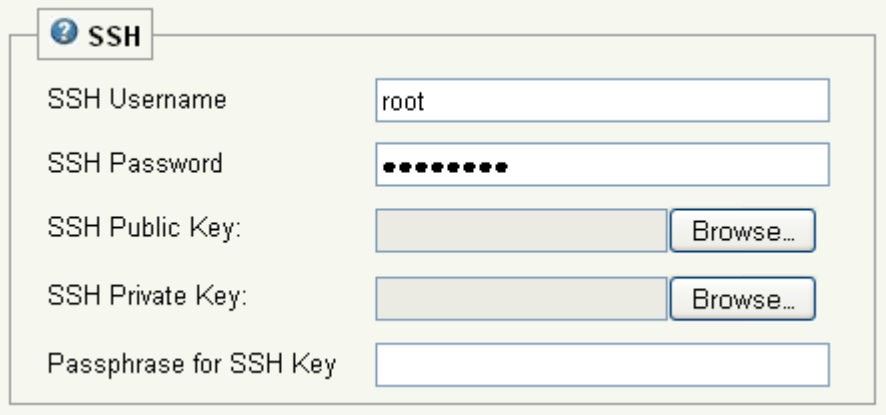
Порт центра KDC по умолчанию — 88, а транспортный протокол по умолчанию — udp. Другое значение транспортного протокола — tcp. И наконец, требуется имя Kerberos Realm (сфера Kerberos) и IP-адрес центра KDC.

Учтите, что для использования этого метода проверки подлинности предварительно должна быть создана среда Kerberos.

Использование учетных данных SSH с консолью Tenable SecurityCenter

Для использования учетных данных SSH с консолью SecurityCenter загрузите сгенерированный открытый и закрытый ключ SSH в консоль SecurityCenter. Не устанавливайте ключи непосредственно на сканеры Nessus, поскольку консоль SecurityCenter выполнит загрузку этих учетных данных на сканер Nessus при инициализации сканирования.

Ниже приведен пример части экрана Edit Scan Options (правка параметров сканирования) при изменении параметров политики. Последние три поля используются для указания учетной записи и определенного закрытого и открытого ключей SSH, которые должны использоваться при тестировании. Открытый ключ SSH необходимо поместить на каждый хост Unix, который будет тестироваться с помощью локальных проверок.



Консоль SecurityCenter поставляется с несколькими предварительно определенными политиками уязвимостей. Во всех них локальные проверки включены для каждой отдельной ОС. Однако для использования эти политики необходимо скопировать и затем добавить определенную пару открытого и закрытого ключей SSH, а также определенную учетную запись пользователя.

Пары открытого и закрытого ключей SSH управляются консолью SecurityCenter и передаются каждому управляемому сканеру Nessus.

После установки этих открытых ключей SSH на нужные хосты Unix, а закрытых ключей на консоль SecurityCenter создается отношение доверия, позволяющее

пользователю входить в каждый из хостов Unix со сканеров Nessus. В случае нарушения безопасности сканеров Nessus необходимо создать новый открытый и закрытый ключи SSH.

ПРОВЕРКИ С ИСПОЛЬЗОВАНИЕМ УЧЕТНЫХ ДАННЫХ НА ПЛАТФОРМАХ WINDOWS

Необходимые условия

Привилегии пользователя

Очень распространенной ошибкой является создание локальной учетной записи, которая не имеет достаточно прав для удаленного входа и выполнения каких-либо полезных действий. По умолчанию ОС Windows назначает новым локальным учетным записям при удаленном входе в систему права гостя (Guest). Это не позволяет успешно выполнять удаленный аудит уязвимостей. Еще одна распространенная ошибка – расширение прав доступа пользователей с гостевыми учетными записями. Это снижает уровень безопасности сервера Windows.

Настройка входа в ОС Windows для локального и удаленного аудита

В отношении учетных данных Windows наиболее важно то, что используемая для выполнения проверок учетная запись должна иметь права доступа ко всем необходимым файлам и записям реестра, а во многих случаях это означает необходимость наличия прав администратора. Если сканеру Nessus не предоставлены учетные данные учетной записи администратора, он в лучшем случае сможет выполнять проверку установки исправлений по реестру. Хотя это и допустимый метод определения установки исправлений, он несовместим с некоторыми средствами управления установкой исправлений сторонних производителей, которые могут не устанавливать ключи политик. Если сканер Nessus имеет права администратора, он проверит фактическую версию динамической библиотеки (`.dll`) на удаленном хосте, что обеспечивает значительно более точные результаты.

Настройка локальной учетной записи

Чтобы настроить учетные данные на отдельном сервере Windows, который не является частью домена, просто создайте уникальную учетную запись администратора.

Убедитесь, что созданная учетная запись не имеет настройки по умолчанию «Guest only: local users authenticate as guest» (гостевая - локальные пользователи удостоверяются как гости). Вместо этого выберите настройку «Classic: local users authenticate as themselves» (обычная - локальные пользователи удостоверяются как они сами).

Настройка учетной записи домена для локальных аудитов

Чтобы создать учетную запись домена для удаленного аудита сервера Windows на базе хоста, сервер должен иметь версию ОС Windows Vista, Windows XP Pro, Windows 2003, Windows 2008 или Windows 7 и принадлежать домену.

Чтобы настроить сервер, допускающий вход из учетной записи домена, необходимо включить модель безопасности Classic (обычная). Для этого выполните следующие действия.

1. Откройте редактор групповых политик, для чего нажмите кнопку Пуск, выберите пункт Выполнить и введите команду «gpedit.msc». Затем нажмите кнопку OK.
2. Выберите Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options (конфигурация компьютера -> конфигурация Windows -> настройки безопасности -> локальные политики -> параметры безопасности).
3. Из списка политик откройте «Network access: Sharing and security model for local accounts» (сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей).
4. В этом диалоговом окне выберите «Classic – local users authenticate as themselves» (обычная - локальные пользователи удостоверяются как они сами) и нажмите кнопку OK, чтобы сохранить настройку.

При этом локальные пользователи домена будут удостоверяться как они сами, хотя они, фактически, и не являются физически локальными на соответствующем сервере. Без этой настройки все удаленные пользователи (даже реальные пользователи домена) будут фактически удостоверяться как гости и, вероятно, не будут иметь достаточных прав для выполнения удаленного аудита.

Настройка Windows XP и 2003

При выполнении сканирования с проверкой подлинности операционных систем Windows XP или 2003 необходимо включить несколько параметров конфигурации.

1. На целевой машине должна быть включена служба WMI.
2. На целевой машине должна быть включена служба Remote Registry (удаленный реестр).
3. В конфигурации сети целевой машины должен быть включен общий доступ к файлам и принтерам.
4. Между сканером Nessus и целевой машиной должны быть открыты порты 139 и 445.
5. Должна использоваться учетная запись SMB, имеющая права локального администратора на целевой машине.

Может потребоваться изменить локальные политики безопасности Windows, или они могут заблокировать доступ либо унаследованные разрешения. Распространенная политика, влияющая на сканирование с использованием учетных данных, находится в разделе:

Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security Options -> Network access (администрирование -> локальная политика безопасности -> настройки безопасности -> локальные политики -> параметры безопасности -> сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей).

Если в этой локальной политике безопасности выбрана настройка не «Classic - local users authenticate as themselves» (обычная - локальные пользователи удостоверяются как они сами), а любая другая, сканирование на соответствие стандартам не будет успешно выполнено.

Настройка Windows 2008, Vista и 7

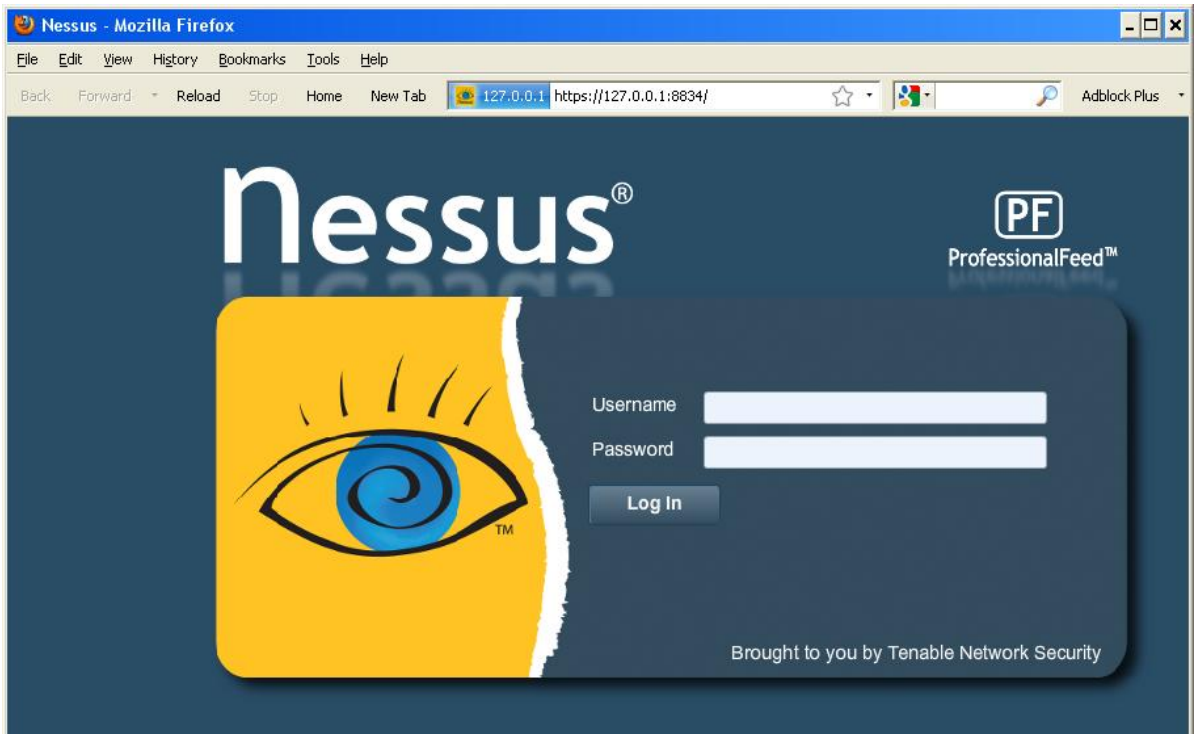
При выполнении сканирования с проверкой подлинности операционных систем Windows 2008, Vista или 7 необходимо включить несколько параметров конфигурации.

1. В разделе Windows Firewall -> Windows Firewall Settings (брандмауэр Windows -> параметры брандмауэра Windows) должен быть включен параметр File and Printer Sharing (общий доступ к файлам и принтерам).
2. С помощью средства **`gpedit.msc`** (запускается через диалоговое окно Run (выполнить...)) вызовите редактор объектов групповой политики. Перейдите к элементу Local Computer Policy -> Administrative Templates -> Network -> Network Connections - > Windows Firewall -> Standard Profile -> Windows Firewall: Allow inbound file and printer exception (политика локального компьютера -> административные шаблоны -> сеть -> сетевые соединения - > брандмауэр Windows -> стандартный профиль -> брандмауэр Windows: разрешает исключение для входящего общего доступа к файлам и принтерам) и включите его.
3. В редакторе объектов групповой политики элемент Local Computer Policy -> Administrative Templates -> Network -> Network Connections -> Prohibit use of Internet connection firewall on your DNS domain (политика локального компьютера -> административные шаблоны -> сеть -> сетевые соединения -> запрет использования брандмауэра подключения к Интернету в DNS-домене) должен иметь настройку Disabled (отключен) или Not Configured (не определен).
4. Контроль учетных записей Windows (UAC) должен быть отключен, или должен быть изменен определенный параметр реестра, чтобы разрешить аудиты Nessus. Для полного отключения контроля UAC откройте панель управления, выберите элемент User Accounts (учетные записи пользователей) и отключите контроль учетных записей пользователей. Вместо этого можно добавить новый раздел реестра LocalAccountTokenFilterPolicy и присвоить ему значение 1. Этот раздел должен быть создан в следующем месте реестра: **`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`**. Дополнительные сведения об этой настройке реестра см. в документе MSDN 766945 KB.
5. Необходимо включить службу Remote Registry (удаленный реестр). По умолчанию эта служба выключена. Ее можно включить для одноразового аудита или оставить включенной постоянно, если аудиты выполняются часто.

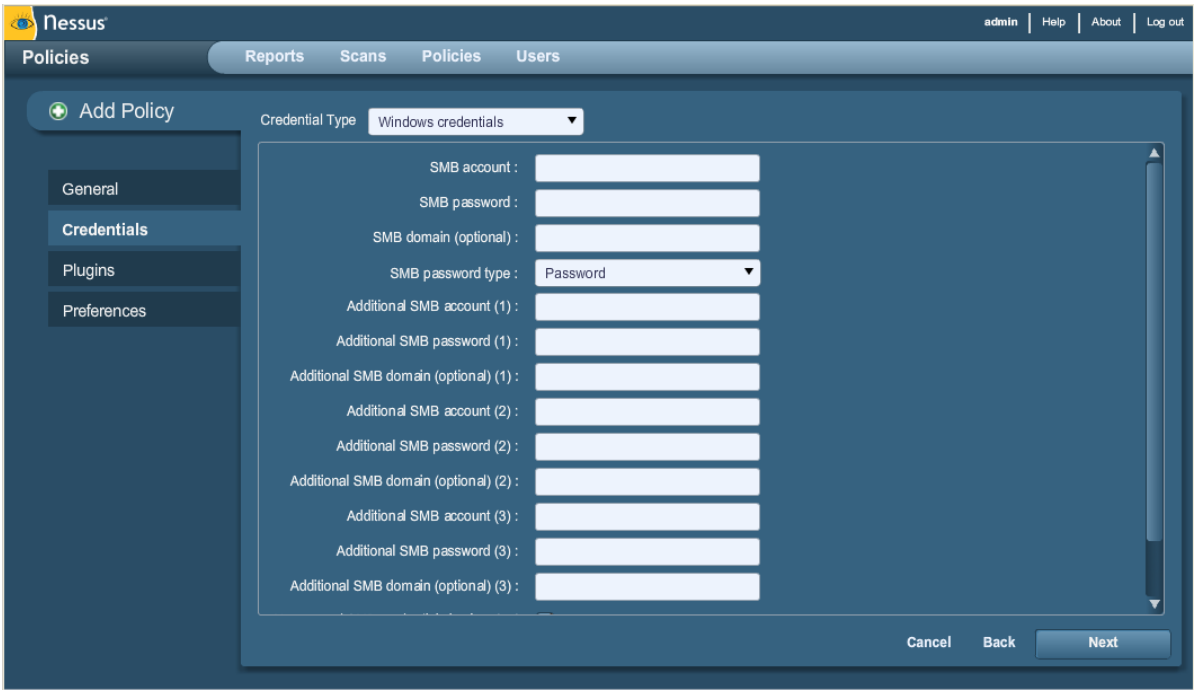
Сканер Nessus может включать и выключать службу Remote Registry (удаленный реестр). Чтобы эта функция работала, на целевой машине для службы Remote Registry (удаленный реестр) должен быть установлен параметр Manual (ручной) или Disabled (отключен).

Настройка Nessus для входа в ОС Windows

Интерфейс пользователя Nessus



Откройте веб-браузер и подключитесь к интерфейсу пользователя сканера Nessus, как показано выше, а затем выберите вкладку Policies (политики). Создайте новую политику или измените существующую и перейдите на вкладку Credentials (учетные данные), расположенную слева. Выберите из раскрывающегося меню, расположенного в верхней части окна, элемент Windows credentials (учетные данные Windows), как показано ниже:



Укажите имя учетной записи SMB, пароль и домен (не обязательно).

Теперь нажмите кнопку **Submit** (отправить) в нижней части окна, и настройка будет завершена. Новая политика сканирования будет добавлена в список управляемых политик сканирования.

Командная строка Nessus Unix

Использование файлов .nessus

Сканер Nessus может сохранять настроенные политики сканирования, целевые устройства сети и отчеты в файле **`.nessus`**. В приведенном выше разделе «Интерфейс пользователя Nessus» описано создание файла **`.nessus`**, содержащего учетные данные Windows. Инструкции по выполнению сканирования из командной строки с помощью файла **`.nessus`** см. в «Руководстве пользователя Nessus» по адресу:

http://www.tenable.com/products/nessus/documentation

Использование файлов .nessusrc

В случае создания файла **`.nessusrc`** вручную есть три записи, позволяющие настроить имя пользователя, пароль и домен (не обязательно), как показано ниже:

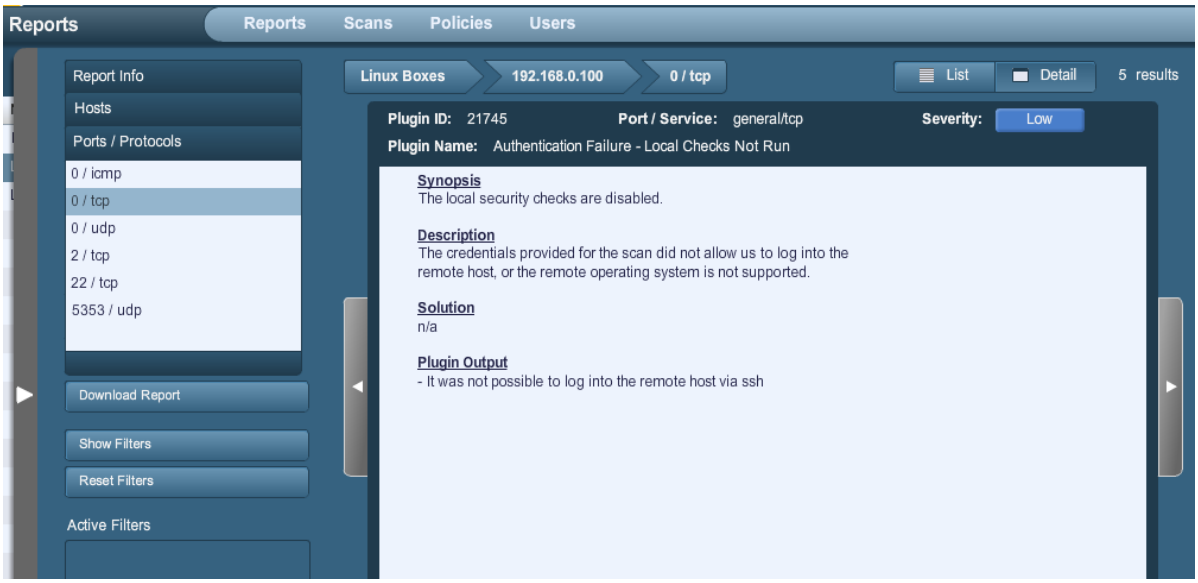
```
Login configurations[entry]:SMB account : =
Login configurations[password]:SMB password : =
Login configurations[entry]:SMB domain (optional) : =
```

ОПРЕДЕЛЕНИЕ ОШИБКИ УЧЕТНЫХ ДАННЫХ

В случае применения сканера Nessus для выполнения аудитов систем Unix или Windows с использованием учетных данных, анализ результатов для определения правильности использованных паролей и ключей SSH мог быть сложной задачей. Теперь

пользователи Nessus могут легко определять, когда их учетные данные не работают. Компания Tenable добавила подключаемый модуль Nessus №21745 в семейство подключаемых модулей Settings (настройки).

Этот подключаемый модуль определяет, если учетные данные SSH или Windows не позволили сканированию выполнить вход в удаленный хост. При успешном входе этот подключаемый модуль не выдает никаких результатов. Ниже приведен пример отчета, полученного при попытке входа сканера Nessus в удаленную машину с неверным именем пользователя или паролем:



УСТРАНЕНИЕ НЕПОЛАДОК

В. Как определить, работает ли локальное сканирование?

О. За исключением случаев, когда на сервере установлены 100 % исправлений, локальное сканирование чаще всего возвращает некоторую информацию об исправлениях. В зависимости от операционной системы сканирование также возвращает различную информацию аудитов.

Также может быть полезно временно устранить сканер Nessus и выполнить тест для проверки правильности настройки учетных записей и сетей. С помощью простой команды ОС Unix **`id`** со сканера Nessus выполните следующую команду:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
#
```

Необходимо использовать IP-адрес системы, с которой настраиваются доверительные отношения, а также соответствующую учетную запись пользователя (в данном случае пользователь nessus). В случае успешного выполнения команды вы увидите результаты команды **`id`**, как будто она была выполнена на удаленной системе.

При аудитах Unix скрипт **`ssh_get_info.nasl`** выдаст сообщение, если проверка подлинности была успешной. Если учетные данные SSH не действуют, можно повысить

настройку report_verbosity (детальность отчета) сканирования Nessus до Verbose (подробный). В этом случае будут показаны все ошибки и диагностические сообщения, полученные при выполнении данного скрипта.

В случае аудитов Windows скрипты **`smb_login.nasl`** и **`smb_registry_access.nasl`** показывают, приняты ли имя пользователя и пароль во время сканирования и удалось ли прочесть удаленный реестр. Скрипт **`smb_registry_full_access.nasl`** выдает предупреждение, только если было невозможно полностью прочесть реестр. При рассмотрении результатов проверок на базе хоста для аудитов сервера Windows можно определить, успешно ли были использованы учетные данные.

Кроме того, скрипт **`hostlevel_check_failed.nasl`** определяет, если учетные данные SSH или Windows не позволили сканированию выполнить вход в удаленный хост.

В. Как определить сбой локального сканирования?

О. В системах Windows на сервере генерируются ошибки входа. При использовании контроллера домена ошибки входа регистрируются также на нем.

В системах Unix ошибки входа регистрируются в системных журналах (например, **`/var/log/messages`**), за исключением случая использования удаленного контроллера Kerberos.

Кроме того, скрипт **`hostlevel_check_failed.nasl`** определяет, если учетные данные SSH или Windows не позволили сканированию выполнить вход в удаленный хост.

В. Какие еще могут возникнуть проблемы с проверками хоста?

О. Существует много факторов, которые могут заблокировать доступ. Ниже приведены некоторые из них, которые стоит учесть.

- Сетевые брандмауэры, фильтрующие порт 22 для SSH на ОС Unix или порт 445 на ОС Windows.
- Размещенные на хостах брандмауэры, блокирующие подключение к указанным портам.
- На системах Unix администраторы могут переводить протокол SSH на другие порты вместо порта 22.
- Некоторые системы защиты от проникновений в сеть могут мешать удаленному доступу.
- Сканируемое устройство может быть не сервером Unix или Windows, а принтером, маршрутизатором, факсом или устройством воспроизведения видео.

В. Я тестирую соединения SSH с системой Nessus из командной строки сканируемых хостов, чтобы проверить правильность подключения. При этом возникают задержки соединения, почему?

О. Наиболее вероятно, это происходит, потому что система выполняет просмотр DNS, когда DNS-сервер неправильно настроен. Если узел использует DNS, обратитесь к администратору DNS-сервера для устранения проблем конфигурации. Проблемы могут вызвать отсутствующие зоны обратного просмотра. Для проверки просмотров DNS выполните следующее:

```
# host IP_АДРЕС_СЕРВЕРА_NESSUS
```

Если установлена программа dig, можно также выполнить проверку с помощью следующей команды:

```
# dig -x IP_АДРЕС_СЕРВЕРА_NESSUS
```

Если узел не использует DNS, следующие действия помогут исключить попытки поисков DNS.

1. Внесите изменения в файл **/etc/nsswitch.conf**, чтобы в строках «hosts:» было указано «hosts: files».
   Примечание. Эта инструкция может подходить не для всех выпусков OpenSSH.

2. Добавьте IP-адрес/имя сервера, на котором установлен сервер Nessus, в файл **/etc/hosts** системы.

3. Настройте удаленный сервер OpenSSH, чтобы он **не** выполнял просмотры DNS на хосте, выполнив следующие две настройки:

   - «UseDNS no» (использование DNS - нет) в файле `sshd_config` (для выпуска 3.8), по умолчанию установлено значение «yes» (да).
   - «VerifyReverseMapping no» (проверка обратного сопоставления - нет).

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СКАНЕРА

ЗАЧЕМ НЕОБХОДИМО ОБЕСПЕЧИВАТЬ БЕЗОПАСНОСТЬ СКАНЕРА?

В случае настройки сканера Nessus для использования учетных данных для входа в сервер Unix или Windows система будет содержать учетные данные, которыми могут воспользоваться злоумышленники. Чтобы не допустить этого, необходимо не только пользоваться оптимальными методами обеспечения безопасности операционной системы, на которой установлен сканер, но и знать, как злоумышленники могут заставить сканер раскрыть информацию системы безопасности.

ЧТО ОЗНАЧАЕТ БЛОКИРОВКА СКАНЕРА?

В идеале, сканер Nessus должен управляться только с системной консоли и не принимать каких-либо сетевых подключений от каких-либо удаленных хостов. Такая система будет физически защищена, и только имеющие полномочия люди будут иметь к ней доступ. Этот сервер дополнительно можно ограничить внешним брандмауэром или коммутатором, разрешающим выполнять сканирование только определенных сетей. Не устанавливайте программное обеспечение личного брандмауэра непосредственно на систему, на которой установлен сканер Nessus. Помните, что сканер Nessus можно настроить для сканирования только определенных сетей.

Однако, такой тип сканера не настолько полезен. Рассмотрите возможность разрешения удаленного сетевого доступа к сканеру. Сканер Nessus по умолчанию поддерживает подключения HTTP к порту 8834. Системный брандмауэр можно настроить так, чтобы он принимал подключения к порту 8834 только от допустимых клиентов Nessus.

Если администрирование и управление сервером необходимо выполнять удаленно, также можно использовать защищенный удаленный доступ. На ОС Unix можно использовать протокол Secure Shell (SSH). Своевременно обновляйте демон SSH, используйте надежные пароли и/или используйте более надежные технологии проверки подлинности. На серверах Windows можно использовать удаленные службы терминалов для предоставления доступа к командам и управлению Nessus Windows через эти службы. В обоих случаях необходимо своевременно обновлять систему и не запускать ненужные сетевые службы. Рекомендации по повышению безопасности систем см. в документе Center for Internet Security (CIS) benchmarks (стандарты CIS).

Безопасная реализация аудитов Unix SSH

Никогда не используйте пароли SSH для выполнения удаленного сканирования. В случае сканирования сети злоумышленникам необходимо будет лишь запустить модифицированный демон SSH и записать используемые для входа имя пользователя и пароль. Даже в случае использования уникальной комбинации имени пользователя и пароля для каждого хоста использование статических паролей остается уязвимым.

В случае аудита одного сервера с помощью известного имени пользователя и пароля, при входе через SSH меньше шансов, что злоумышленник сможет воспользоваться этим против вас. Однако обязательно защитите конфигурацию сканирования, потому что имя пользователя и пароль хранятся в ней открытым текстом.

Безопасные аудиты Windows

Если параметр Only use NTLMv2 (использовать только NTLMv2) отключен, то существует теоретическая возможность заставить сканер Nessus выполнить попытку входа в сервер Windows с учетными данными домена через протокол NTLM версии 1. Это дает возможность осуществляющему удаленную атаку лицу возможность использовать полученный от сканера Nessus хэш-код. Этот хэш-код потенциально может быть взломан для извлечения имени пользователя или пароля. Он также может использоваться для непосредственного входа на другие серверы. Обеспечьте использование сканером Nessus протокола NTLMv2, включив настройку Only use NTLMv2 (использовать только NTLMv2) во время сканирования. Это не даст враждебному серверу Windows использовать протокол NTLM и получить хэш-код.

Протокол NTLMv2 может использовать функцию SMB Signing (подписывание SMB-пакетов). Проверьте, чтобы функция SMB Signing (подписывание SMB-пакетов) была включена на всех серверах Windows, чтобы никакой сервер, получивший хэш-код от сканера Nessus, не мог использовать его повторно. Кроме того, примените политику, требующую обязательного использования надежных паролей, которые не могут быть легко взломаны с помощью атак перебором по словарю из таких программ, как John the Ripper и L0phtCrack.

Обратите внимание, что было много разных типов атак, направленных на систему безопасности Windows, для похищения хэш-кодов с компьютеров для дальнейшего использования в атакующих серверах. "Функция SMB Signing (подписывание SMB пакетов) добавляет еще один уровень безопасности для предотвращения этих атак типа «злоумышленник посредине».

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

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

О КОМПАНИИ TENABLE NETWORK SECURITY

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

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