Установка сканеров соответствия

Сканер Nessus

Посетите официальный сайт Nessus, чтобы загрузить Nessus v7 и установить пакет Nessus для операционной системы. Для получения плагинов, необходимо также зарегистрироваться на HomeFeed (или ProfessionalFeed). Подробный процесс установки и первичной конфигурации сканера Nessus v7 описан в официальной документации.

При использовании Nessus с модулем Net::Nessus::XMLRPC могут возникнуть проблемы. Пожалуйста, обратитесь к системе отслеживания ошибок для получения дополнительной информации.

Сканер OpenVAS

Первоначальная конфигурация

Шаг 1. Установите OpenVAS вместе с XYZ и ABC, чтобы управлять OpenVAS удаленно через командную строку **omp**.

Шаг 2. Проверьте правильность подключения AxelNAC к OpenVAS для удаленного управления. Для этого выполните следующую команду (укажите имя пользователя, который будет использоваться для связи AxelNAC с OpenVAS):

omp -u ИМЯ_ПОЛЬЗОВАТЕЛЯ -p 9390 -X "<get_version/>"

В результате выполнения этой команды должна быть получена версия OpenVAS. Если версия OpenVAS не получена, убедитесь, что:

- установлены все необходимые компоненты для управления с помощью командной строки **omp**;
- AxelNAC может взаимодействовать с OpenVAS через порт 9390.

Настройка оповещений

Шаг 1. Настройте политику оповещения в OpenVAS для информирования AxelNAC о завершении задачи. Демон **httpd.portal** отвечает за обработку обратного вызова, поэтому необходимо убедиться, что в интерфейсе управления AxelNAC в дополнительных демонах прослушивания добавлено значение **portal**.

Шаг 2. Создайте политику оповещения. Для этого зайдите в веб-интерфейс сканера OpenVAS в раздел **Configuration → Alerts** и создайте новое оповещение, заполнив следующие поля:

- **Name:** укажите имя оповещения;
- **Event:** установите значение **Task run status changed to Done**;
- **Condition:** Always;
- **Method:** HTTP Get;
- **HTTP Get URL:** укажите значение http://IP-АДРЕС_ИНТЕРФЕЙСА_УПРАВЛЕНИЯ_AxelNAC/hook/openvas?task=$n.

Поиск идентификаторов

После установления соединения между AxelNAC и OpenVAS воспользуйтесь веб-интерфейсом OpenVAS, чтобы получить следующую информацию для настройки AxelNAC Alert ID:

Шаг 1. Перейдите в раздел **Configuration → Alerts**.

Шаг 2. Кликните на оповещение, которое было настроено в предыдущей секции.

Шаг 3. Запишите идентификатор оповещения, который указан в правом верхнем углу страницы.

Идентификатор конфигурации сканирования

Шаг 1. Перейдите в раздел **Configuration → Scan Configs**.

Шаг 2. Выберите конфигурацию сканирования, которую необходимо использовать для сканирования узлов.

Шаг 3. Запишите идентификатор конфигурации, который указан в правом верхнем углу страницы.

Идентификатор формата отчета:

Шаг 1. Перейдите в раздел **Configuration → Report Formats**.

Шаг 2. Выберите формат отчета **CSV Results**.

Шаг 3. Запишите идентификатор формата отчета, который указан в правом верхнем углу страницы.

Сканер WinRS

Сканер WinRS является предустановленным в AxelNAC сканером соответствия. Данный сканер использует службу WinRM, которая является встроенным протоколом в ОС Windows и является транспортом безагентского сканера AxelNAC. Интеграция данного протокола с AxelNAC позволяет проверять соответствие клиентского устройства политикам информационной безопасности. В случаях, когда клиентское устройство не соответствует установленным политикам, оно будет изолироваться с ограничением доступа к сети для устранения несоответствий. Поэтому для использования данного механизма сканирования не требуется производить его установку и предварительную настройку на клиентском оборудовании.

Сканер Rapid7

AxelNAC поддерживает интеграцию с Rapid7 для автоматического запуска сканирования при подключении устройства к сети, а также для получения оповещений Rapid7 через syslog.

Установка Rapid7

Для того, чтобы установить сканер Rapid7, выполните следующие действия:

Шаг 1. Установите приложение InsightVM. Оно доступно по ссылке.

Шаг 2. Запустите приложение. Подробная информация доступна по ссылке.

Шаг 3. Веб-интерфейс сканера Rapid7 будет доступен по следующей ссылке: https://IP-АДРЕС_ВАШЕГО_СЕРВЕРА_Rapid7:3780.

Первоначальная конфигурация

Для интеграции AxelNAC со сканером Rapid7 необходимо создать пользователя, через которого AxelNAC будет выполнять вызовы API на Rapid7. Чтобы создать и настроить пользователя, выполните следующие действия:

Шаг 1. В веб-интерфейсе Rapid7 перейдите в раздел **Administration → Users** и нажмите **Create**.

Шаг 2. На открывшейся странице заполните поля следующим образом:

- **User name:** AxelNAC;
- **Authentication method:** InsightVM user;
- **Full name:** AxelNAC;
- **E-mail address:** укажите адрес электронной почты, на который должны приходить оповещения;
- **Password:** укажите и подтвердите пароль;
- **Account enabled:** поставьте галочку, чтобы сделать этот аккаунт активным.

Шаг 3. Перейдите во вкладку **Роли**, выберите роль **Custom** и назначьте новому пользователю как минимум следующие привилегии:

- Manage Sites;
- Manage Scan Engines;
- View Site Asset Data;
- Specify Scan Targets;
- View Group Asset Data.

Шаг 4. В разделах **Site Acess** и **Asset group access** установите галочки для параметров **Allow this user to access all sites** и **Allow this user to access all asset groups** соответственно.

ID статьи: 87
Последнее обновление: 17 июл., 2024
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Конфигурация сканеров соответствия -> Установка сканеров соответствия
https://docs.axel.pro/entry/87/