События безопасности, механизмы фильтрации и профилирование

В рамках данной лабораторной работы мы изучим что такое профилирование, как с помощью профилирования можно провести инвентаризацию устройств, подключенных к сети, как работает профилирование со стороны безопасности сети, какие существуют критерии профилирования и создадим собственный профиль. Мы разберем события безопасности, как работает приоритизация в них, как настраивать триггеры и действия для событий безопасности и приведем примеры эксплуатации. Также мы расскажем о работе механизмов фильтрации, объясним как обогащать сообщения **Radius-Reply** дополнительными атрибутами, и опишем процесс настройки этих механизмов. Длительность выполнения лабораторной работы — 3 часа.

Профилирование в безопасных сетях

Your browser doesn't support video.
Please download the file: video/mp4

Профилирование (профайлинг) — это процесс, с помощью которого можно определять модели конечных устройств, их производителя, ОС, и тем самым получать о них дополнительную информацию. Благодаря данным, полученным из профилирования AxelNAC может использовать их в качестве политик авторизации.

В отношении безопасности сети профилирование выполняет следующие функции:

- мониторинг конечных устройств;
- актуализация видимости BYOD-устройств;
- формирование политик сетевого доступа, на основе различных профилей устройств.

AxelNAC уже содержит созданные профили на самые часто используемые устройства. При помощи комбинаций различных критериев вы можете группировать устройства по их данным (MAC-адрес, вид устройства, DHCP-отпечаток и т.д.) и использовать эти профили в политиках аутентификации.

Иногда, при внешних атаках, устройства взлома могут мимикрировать под устройства, которые уже находятся в сети. В такой ситуации профилирование клиентских устройств позволяет настроить отдельную политику доступа, которая будет применяться к устройствам, которые внезапно поменяли свои данные.

Критерии профилирования

Для того чтобы тому или иному устройству автоматически назначался профиль, существуют различные критерии профилирования. Рассмотрим самые основные:

MAC-адрес

MAC-адрес (Media или Medium Access Control Address) — это уникальный номер, который назначает производитель каждому устройству с сетевой картой, Bluetooth- или Wi-Fi-адаптером. Он не меняется со временем и состоит из двенадцати шестнадцатеричных символов.

Первые шесть символов обозначают код производителя (MAC OUI), что позволяет определять вендора и добавлять его в профиль.

Отпечаток DHCP

Отпечаток DHCP (DHCP Fingerprinting) — это метод идентификации устройства, запрашивающего аренду IP-адреса через протокол DHCP, на основе которого может быть определен тип подключенного устройства. Идентификация осуществляется путем анализа структуры и содержимого DHCP-сообщений, поступающих от конечного устройства. При этом данный механизм не следует рассматривать как надежное средство защиты, поскольку DHCP-сообщения могут быть подделаны без нарушения процесса получения IP-адреса.

Агент пользователя

Агент пользователя (User Agent) — это программный агент, отвечающий за получение и облегчение взаимодействия конечного конечного устройства с сервером. При каждом запросе по протоколу HTTP, клиент передает свой **user-agent**, который содержит информацию о типе приложения, операционной системе, производителе устройства и т.д., которая также может быть использована для построения профиля.

Инвентаризация устройств с помощью профилирования

Использование вышеперечисленных критериев позволяет идентифицировать все устройства находящиеся в защищенной сети. При наличии достаточного количества сформированных профилей устройств, мы можем определить, какое количество АРМ, IP-телефонов, принтеров, коммутаторов и т.д. подключено к сети.

В AxelNAC в разделе **Узлы → Поиск** находится строка поиска, которая позволяет отсортировать все подключенные устройства по любому из заполненных критериев.

Создание профиля в AxelNAC

Все созданные профили устройств можно найти в разделе **Конфигурация → Соответствие → Профилирование Хранилища отпечатков → Комбинации**. При нажатии на любой из профилей вы можете его просмотреть и отредактировать. Данная страница содержит следующие поля:

- Идентификатор (данное поле нельзя изменить после создания профиля);
- Отпечаток DHCP;
- DHCP вендор;
- Отпечаток DHCPv6;
- DHCPv6 Enterprise;
- MAC-вендор (OUI);
- Агент пользователя;
- Устройство;
- Версия;
- Балл.

Поле **Балл** является оценкой безопасности профиля, и несет лишь оценочную роль. Вы можете поменять значение в предустановленных профилях на свое усмотрение.

Рассмотрим создание профиля в AxelNAC на примере подключенного устройства, которое еще не прошло процесс профилирования.

Шаг 1. Подключите новое устройство к своей сети.

Шаг 2. Перейдите в раздел **Отчеты → Хранилище отпечатков → Неизвестные отпечатки → Все** и нажмите на MAC-адрес узла. Затем нажмите **Просмотреть узел** во всплывающем окне.

Шаг 3. Перейдите на вкладку **Хранилище отпечатков** и скопируйте полученный DHCP-отпечаток.

Шаг 4. Перейдите в раздел **Конфигурация → Соответствие → Профилирование Хранилища отпечатков → Комбинации**. и нажмите **Новая комбинация**.

Шаг 5. Вставьте скопированный отпечаток DHCP в соответствующее поле и укажите название устройства. Начните печатать название устройства, чтобы найти подходящее значение. Затем нажмите **Сохранить**.

Шаг 6. Перейдите раздел **Узлы → Поиск** и вставьте в строку поиска MAC-адрес устройства, для которого вы только что создали профиль.

Шаг 7. Откройте узел и нажмите **Обновить Хранилище отпечатков**. После этого запустится процесс профилирования устройства для узла, после чего его информация обновится.

В данном примере мы настроили профилирование только по отпечатку DHCP, но настройку можно произвести по любому одному или нескольким из критериев.

Проверка работы профилирования

Если все настройки произведены верно, информация об устройстве должна обновиться на шаге 7.

События безопасности

Your browser doesn't support video.
Please download the file: video/mp4

События безопасности (Security Events) — это модуль, который позволяет реагировать на действия и состояния конечных устройств. AxelNAC позволяет реагировать на смену профиля устройства, на несоответствие политикам ИБ устройства, а также реагировать на превышение устройством порогового уровня потребляемого трафика. Функционал **событий безопасности** позволяет комбинировать уведомление администраторов ИБ и изолирование устройства, вызвавшего событие, от общей сети с последующим указанием инструкций и действий на портале администратора AxelNAC.

Настройка событий безопасности в AxelNAC

Для того чтобы настроить события безопасности, перейдите в раздел **Конфигурация → Соответствие → События в системе безопасности** и нажмите **Новое событие в системе безопасности**.

На открывшейся странице вы найдете следующие параметры:

- **Активировать событие в системе безопасности** — включение срабатывания данного события безопасности;
- **Идентификатор** — идентификатор события. Данный параметр назначается автоматически;
- **Описание** — описание события безопасности;
- **Приоритет** — приоритет события безопасности. При выявлении нескольких событий на одном конечном устройстве, будет выполняться событие с самым наименьшим значением;
    - **Игнорировать роли** — какие роли не должны быть затронуты данным событием в системе безопасности;
- **Триггеры событий** — действия или параметры, которые вызывают событие безопасности (можно выбрать одно или несколько):

    - **Параметр конечного устройства** — срабатывание произойдет, если параметр конечного устройства совпадает с указанным;
    - **Профилирование устройств** — срабатывание произойдет, если один из критериев профиля устройства совпадает с указанным;
    - **Использование данных** — срабатывание произойдет, если один из параметров использования данных совпадет с указанным;
    - **Событие** — срабатывание произойдет если случится указанное событие.

- Вводимые в поля значения чувствительны к регистру;
- В поле **MAC-вендор** необходимо указать префикс вендора (первые три октета) в формате xxaabb (например, 23ab17). Символы "-", ":" не обрабатываются;
- Поле **MAC-адрес** должно быть заполнено в формате aa:bb:cc:dd:ee:ff.

- **Действия, связанные с событием:**
    - **Снять с регистрации** — снять регистрацию с устройства;
    - **Зарегистрировать** — зарегистрировать устройство в системе. Вы можете указать целевую роль и срок предоставления доступа;
    - **Изолировать** — выдать роль изолированного устройства. Вы можете настроить страницу, которая будет отображаться на портале, кнопку, URL для переадресации, предоставление возможности хосту самостоятельно перезапустить регистрацию;
    - **Администратор электронной почты** — отправить уведомление на электронную почту администратора AxelNAC;
    - **Электронная почта владельца конечного устройства** — отправить сообщение на электронную почту устройства, вызвавшего событие (если почта указана);
    - **Адресат сообщения** — отправить сообщение на электронную почту другого пользователя. Необходимо указать адрес электронной почты;
    - **Выполнить скрипт** — выполнить скрипт в AxelNAC. Необходимо указать путь к скрипту;
    - **Закрыть еще одно событие в системе безопасности** — завершить действие другого события безопасности в системе.
- **Grace** — период "остывания" события. Событие не сработает повторно в указанный период;
- **Окно** — период, по истечении которого событие автоматически закроется;
- **Задержка на** — задержка перед срабатыванием события безопасности.

Алгоритм настройки события безопасности

Шаг 1. В окне **Новое событие безопасности** включите срабатывание и внесите описание события безопасности.

Шаг 2. Нажмите **Добавить триггер**, в колонке **Конечное устройство** выберите значение **Переключатель** и укажите IP-адрес вашего коммутатора.

Шаг 3. В колонке **Профилирование устройств** выберите значение **Отпечаток DHCP** и укажите отпечаток вашего конечного устройства.

Шаг 4. В строке **Действия, связанные с событием** активируйте флажки **Администратор электронной почты** и **Адресат сообщения** и укажите адрес электронной почты для тестирования.

Шаг 5. В строке **Grace** укажите время в 10 минут и нажмите **Создать**.

Шаг 6. Подключитесь к сети с конечного устройства, чтобы вызвать срабатывание события безопасности.

Проверка работы события безопасности

Для того, чтобы проверить срабатывание события безопасности, зайдите в электронную почту, которая указана как электронная почта администратора и в электронную почту для тестирования. Если вы получили уведомления о срабатывании события — настройка проведена верно. Повторите **шаг 6**, чтобы проверить, что событие не повторяется в течение 10 минут.

Расширенные фильтры

AxelNAC позволяет создавать расширенные правила фильтрации на основании информации RADIUS, DHCP, DNS или HTTP. Также они позволяют добавлять дополнительные данные в сообщения, которые отправляются от сервера аутентификации. В рамках этой лабораторной работы мы рассмотрим фильтрацию только по атрибутам RADIUS.

Посредством RADIUS-атрибутов производится весь обмен информацией между сервером аутентификации и RADIUS-сервером. Набор поддерживаемых RADIUS-атрибутов меняется для каждого сервера аутентификации, они также называются VSA (Vendor Specific Attribute), однако существуют и общие.

Настройка расширенных фильтров в AxelNAC

Для того чтобы создать новый фильтр, перейдите в раздел **Конфигурация → Расширенные настройки доступа → Механизмы фильтра → RADIUS Filters** и нажмите **Новый фильтр**.

На открывшейся странице вы найдете следующие параметры:

- **Имя** — отображаемое имя фильтра;
- **Описание** — отображаемое описание фильтра;
- **Активировано** — включение срабатывания данного фильтра;
- **Условие** — выбор условий для фильтрации. Вы можете указать оператор, поля RADIUS-сообщения и их значения;
- **Объединить ответ** — если активировано, указанные ответы будут объединены с исходными ответами RADIUS;
- **Ответы** — выбор типов полей и их значений для ответного сообщения;
- **Области** — область, в которую будет отправлено ответное сообщение;
- **Статус RADIUS** — статус, который будет отправлен RADIUS в ответном сообщении.

Алгоритм настройки расширенного фильтра

Шаг 1. В разделе **Конфигурация → Расширенные настройки доступа → Механизмы фильтра → RADIUS Filters** нажмите **Новый фильтр**.

Шаг 2. Заполните **Имя** и **Описание фильтра**.

Шаг 3. В строке **Условие** выберите оператор ALL (AND), нажмите на шестеренку справа от поля выбора и во всплывающем окне выберите **Добавить значение**.

Шаг 4. В колонке **Поле** выберите **radius_request.User-Name**, в качестве оператора укажите **содержит** и добавьте в значение свой домен.

Шаг 5. В строке **Ответы** нажмите **Добавить ответ**, выберите вид ответа — **Запрос**, тип — **Cisco-AVPair** и добавьте в качестве значения какой-либо ACL.

Шаг 6. Активируйте переключатель **Объединить ответ**.

Шаг 7. В строке Область выберите значение returnRadiusAccessAccept, в строке Статус RADIUS выберите RLM_MODULE_OK и нажмите **Создать**.

Проверка работы расширенного фильтра

Для проверки работы данного фильтра, переподключитесь к сети с конечного устройства и проверьте доступ к любому из адресов, которые перечислены в whitelist указанного ACL. При правильной настройке, адрес должен быть доступен.

Затем попробуйте перейти по любому из адресов, которые перечислены в blacklist указанного ACL. При правильной настройке, адрес должен быть недоступен.

Проверка результатов лабораторной работы

Для закрепления полученных знаний мы предлагаем выполнить два задания:

1. Создайте событие безопасности, которое будет ограничивать доступ в сеть с уведомлением администратора. Убедитесь, что клиентское устройство перемещено в карантинный VLAN.
2. Создайте расширенный RADIUS-фильтр, который заменит VLAN пользователю относительно коммутатора и назначит на сессию Access list, разрешающий весь трафик.

ID статьи: 9
Последнее обновление: 28 июл., 2025
Обновлено от: Егоров В.
Ревизия: 31
База знаний AxelNAC -> Обучающие материалы -> Лабораторные работы -> События безопасности, механизмы фильтрации и профилирование
https://docs.axel.pro/entry/9/