Страница «Профилирование/хранилище отпечатков»

В данном разделе осуществляется настройка параметров профилирования, а также просмотр записей, содержащихся в хранилище отпечатков. Хранилище отпечатков используется для точной идентификации конечных устройств в сети.

Профилирование (профайлинг) — это процесс, с помощью которого можно определять модели оконечных 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 оконечных 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.

ID статьи: 461
Последнее обновление: 23 мая, 2025
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Соответствие» -> Страница «Профилирование/хранилище отпечатков» -> Страница «Профилирование/хранилище отпечатков»
https://docs.axel.pro/entry/461/