WiFi ????????

Фальшивые точки доступа

Rogue Access Point (фальшивая точка доступа) — это беспроводная точка доступа (AP), установленная и подключенная к сети без разрешения администратора и не является частью официальной инфраструктуры. Rogue AP представляют угрозу для безопасности сети, так как злоумышленник может размещать Rogue AP с целью выполнения таких атак, как перехват данных, человек посередине (man-in-the-middle), и подмену трафика. Как правило, на размещенной точке доступа устанавливается wi-fi сеть с названием (SSID), идентичным или очень похожим на имя публичной сети компании, таким образом пользователи не задумываясь могут подключаться к сети злоумышленника.

Мониторинг фальшивых точек доступа в офисном сетевом периметре может осуществляться следующими способами:

- Использование IDS/IPS — эти системы могут анализировать трафик и обнаруживать несанкционированные точки доступа.
- Проведение регулярных аудитов беспроводной сети с использованием специализированных инструментов (например, с использованием спектрального анализа).
- Мониторинг сетевого трафика.
- Мониторинг радиоэфира:
  - Спектральный анализ — использование инструментов для анализа радиочастотного спектра.
  - Использование специализированных Wi-Fi-анализаторов для сканирования беспроводного спектра.
  - Мониторинг уровней сигнала.
  - Локализация беспроводных устройств для определения физического местоположения беспроводных устройств.
  - Интеграция с системами мониторинга и управления сетью (NMS).

Существует несколько средств и методов для обнаружения фальшивых точек доступа:

1. Системы Управления Беспроводными Сетями (WLAN Management Systems, WMS)
   Позволяют мониторить и управлять беспроводными сетями: могут автоматически сканировать беспроводное пространство для обнаружения новых точек доступа и анализа их характеристик. Эти системы также могут предоставлять средства для удаления или блокирования фальшивых точек доступа.
2. Беспроводные системы предотвращения вторжений (Wireless Intrusion Prevention Systems, WIPS)
   Могут использовать различные методы обнаружения, такие как сбор статистики с беспроводных клиентов, анализ аномалий, и сканирование беспроводного

пространства для обнаружения новых точек доступа. Некоторые WIPS также предоставляют средства для блокирования или предотвращения деятельности фальшивых точек доступа.
3. Анализаторы спектра
   Могут обнаруживать беспроводные сигналы в диапазоне, включая те, которые исходят от Rogue AP.
4. Мониторинг системных логов и событий
   Может выявить аномальную активность, такую как появление новых точек доступа, которые либо не входят в списки разрешенных, либо в целом не встречались ранее. Это требует внимательного мониторинга логов и реагирования на события, связанные с беспроводными сетями, техническим средством реализации такого мониторинга может являться SIEM система.
5. Пассивное Сканирование
   Можно "прослушивать" беспроводные каналы, записывая информацию о видимых устройствах, тем самым можно иметь возможность обнаруживать новые подключенные точки доступа.
6. Активное сканирование
   На точки доступа отправляются запросы и анализируются ответы с целью выявления фальшивых точек доступа.

Атака Evil Twin

Evil Twin — это атака на беспроводные сети, при которой злоумышленник создает поддельную точку доступа (AP), которая имитирует легитимную точку доступа. Злоумышленник заставляет пользователей подключаться к своей поддельной точке доступа, вместо легитимной, с целью перехвата данных или проведения других атак.

Основные этапы:

- Обнаружение сетей
  Злоумышленник сканирует беспроводные сети в поисках доступных точек доступа и их параметров (SSID, канал, MAC-адрес и др.).
- Создание поддельной точки доступа
  Злоумышленник создает точку доступа с тем же SSID, что и легитимная сеть, чтобы привлечь внимание пользователей.
- Имитация легитимной сети
  Поддельная точка доступа имитирует характеристики легитимной сети, такие как SSID, BSSID (MAC-адрес точки доступа), и другие параметры.
- Привлечение пользователей
  Злоумышленник может использовать различные методы для привлечения пользователей к своей поддельной сети. Это может включать в себя отправку пакетов деаутентификации, отправку фишинговых уведомлений о необходимости обновления пароля или обновления программного обеспечения.
- Перехват данных
  Когда пользователи подключаются к фальшивой точке доступа, злоумышленник может перехватывать и анализировать их сетевой трафик. Это может включать в

себя анализ посещенных веб-сайтов, перехват данных для входа в системы и т.д.
- Внедрение вредоносного контента
  Злоумышленник может также использовать поддельную сеть для внедрения вредоносных скриптов или фишинговых страниц
- Выполнение других атак
  В зависимости от целей злоумышленника, атака Evil Twin может использоваться для различных целей, включая внедрение вредоносного программного обеспечения, уклонение от обнаружения и аутентификации, атак на данные и другие.

Защита от Evil Twin:

- Использовать шифрование (WPA2 или WPA3) для защиты беспроводных сетей.
- Обеспечить обнаружение фальшивых точек доступа.
- Обучать пользователей определять нелегитимные сети и избегать подключения к незащищенным сетям.

Атака Deauth

Атака deauthentication (или deauth) — это вид атаки, при которой отправляются пакеты деаутентификации клиентским устройствам или точке доступа (AP), с целью принудительного отключения устройства от Wi-Fi сети. Эта атака может быть использована с различными целями, включая отслеживание устройств, сбор информации о сети или даже проведение других атак, таких как атаки на перехват трафика.

Цели:

- Отключение пользователей. Основная цель атаки Deauth - принудительное отключение пользователей от беспроводной сети.
- Установка MITM-атак. Атака Deauth может использоваться в сочетании с атакой Man-in-the-Middle (MITM). После отключения клиента, злоумышленник может пытаться предоставить фальшивую точку доступа с тем же именем сети (Evil Twin) и перехватывать трафик между клиентом и настоящей точкой доступа
- Идентификация уязвимостей. Атака Deauth может использоваться для идентификации уязвимостей в протоколах аутентификации и управления доступом Wi-Fi.

Принцип работы

- Имитация точки доступа. В некоторых случаях, злоумышленник может создавать свою собственную фальшивую точку доступа с тем же идентификатором сети (SSID) как реальная сеть, чтобы устройства автоматически подключались к ней.
- Отправка пакетов деаутентификации (Deauth Frames). злоумышленник посылает пакеты деаутентификации клиентским устройствам, представляясь точкой доступа.
- Принудительное отключение устройств. Когда устройство получает фрейм деаутентификации, оно теряет связь с точкой доступа и вынуждено повторно аутентифицироваться и подключаться к сети, и в случае использования имитированной фальшивой точки доступа, пользователь может подключиться к

сети злоумышленника.

Защита от атаки deauth

- Использование защиты от деаутентификации (Deauthentication Protection). Некоторые точки доступа поддерживают функционал защиты от деаутентификации.
- Мониторинг сетевого трафика может помочь выявить аномалии, связанные с атакой deauth.
- Использование сетей WPA3. Использование последних стандартов безопасности, таких как WPA3, может уменьшить уязвимость к атакам deauth.

Одним из инструментов обнаружения атаки deauth является Deauthentication Detector. Deauthentication Detector использует python-библиотеку Scapy, которая содержит функционал для анализа сетевого трафика. Скрипт анализирует захваченный трафик и выявляет атаку по наличию deauth-пакета в трафике, в wireshark этот пакет будет выглядеть так:

Revision #1
Created 25 October 2025 12:55:48 by Admin
Updated 25 October 2025 13:06:49 by Admin