Атаки человека посередине (MITM)

Методы MITM, обнаружение и рекомендации по предотвращению

Что такое атака «человек посередине» (MiTM)?

Атаки «человек посередине» (MITM) — это распространенный тип кибератак (/fundamentals/types-of-attacks/), который позволяет злоумышленникам подслушивать обмен данными между двумя целями. Атака происходит между двумя законно общающимися хостами, что позволяет злоумышленнику «прослушать» разговор, который он обычно не может слушать, отсюда и название «человек посередине».

Вот аналогия: Алиса и Боб разговаривают; Ева хочет подслушать разговор, но при этом оставаться открытой. Ева могла сказать Алисе, что она Боб, а Бобу, что она Алиса. Это заставит Алису поверить, что она разговаривает с Бобом, в то время как на самом деле она раскрывает свою часть разговора Еве. Затем Ева может собрать из этого информацию, изменить ответ и передать сообщение Бобу (который думает, что разговаривает с Алисой). В результате Ева может незаметно перехватить их разговор.

Типы атак «человек посередине»

Мошенническая точка доступа

Устройства, оснащенные беспроводными картами, часто пытаются автоматически подключиться к точке доступа, излучающей самый сильный сигнал. Злоумышленники могут настроить свою собственную беспроводную точку доступа и обманным путем заставить близлежащие устройства присоединиться к ее домену. Злоумышленник теперь может управлять всем сетевым трафиком жертвы. Это опасно, потому что для этого злоумышленнику даже не обязательно находиться в доверенной сети — злоумышленнику просто нужно достаточно близкое физическое соседство.

Man in the Middle (MITM) Attacks

ARP-спуфинг

ARP — это протокол разрешения адресов. Он используется для преобразования IP-адресов в физические MAC-адреса (управление доступом к среде) в локальной сети. Когда хосту необходимо связаться с хостом с заданным IP-адресом, он обращается к кэшу ARP для преобразования IP-адреса в MAC-адрес. Если адрес неизвестен, выполняется запрос MAC-адреса устройства с IP-адресом.

Злоумышленник, желающий выдать себя за другой хост, может отвечать на запросы, на которые он не должен отвечать, используя свой собственный MAC-адрес. С помощью некоторых точно размещенных пакетов злоумышленник может прослушивать частный трафик между двумя хостами. Из трафика можно извлечь ценную информацию, такую как обмен маркерами сеанса, что дает полный доступ к учетным записям приложений, к которым злоумышленник не должен иметь доступа.

mDNS-спуфинг

Многоадресная рассылка DNS похожа на DNS, но выполняется в локальной сети (LAN) с использованием широковещательной передачи, такой как ARP. Это делает его идеальной мишенью для спуфинговых атак. Предполагается, что локальная система разрешения имен максимально упростит настройку сетевых устройств. Пользователям не нужно точно знать, с какими адресами должны

связываться их устройства; они позволяют системе решать это за них. Такие устройства, как телевизоры, принтеры и развлекательные системы, используют этот протокол, поскольку они обычно находятся в доверенных сетях. Когда приложению необходимо узнать адрес определенного устройства, например tv.local, злоумышленник может легко ответить на этот запрос поддельными данными, поручив ему разрешить адрес, который он контролирует. Поскольку устройства хранят локальный кеш адресов, жертва теперь какое-то время будет считать устройство злоумышленника доверенным.

DNS-спуфинг

Подобно тому, как ARP преобразует IP-адреса в MAC-адреса в локальной сети, DNS разрешает доменные имена в IP-адреса. При использовании атаки с подменой DNS злоумышленник пытается ввести поврежденную информацию кэша DNS на хост, пытаясь получить доступ к другому хосту, используя свое доменное имя, например www.onlinebanking.com. Это приводит к тому, что жертва отправляет конфиденциальную информацию на вредоносный хост, полагая, что она отправляет информацию в надежный источник. Злоумышленнику, который уже подделал IP-адрес, может быть гораздо проще подделать DNS, просто преобразовав адрес DNS-сервера в адрес злоумышленника.

Методы атаки

«Человек посередине»

нюхает

Злоумышленники используют инструменты захвата пакетов для проверки пакетов на низком уровне. Использование определенных беспроводных устройств, которые разрешено переводить в режим наблюдения или неразборчивый режим, может позволить злоумышленнику увидеть пакеты, которые ему не предназначены, например, пакеты, адресованные другим хостам.

Пакетная инъекция

Злоумышленник также может использовать режим мониторинга своего устройства для внедрения вредоносных пакетов в потоки передачи данных. Пакеты могут сливаться с действительными потоками передачи данных, выглядя как часть связи, но злонамеренные по своей природе. Внедрение пакетов обычно включает в себя сначала прослушивание, чтобы определить, как и когда создавать и отправлять пакеты.

Перехват сеанса

Большинство веб-приложений используют механизм входа в систему, который генерирует временный токен сеанса для использования в будущих запросах, чтобы не требовать от

пользователя ввода пароля на каждой странице. Злоумышленник может прослушивать конфиденциальный трафик, чтобы идентифицировать маркер сеанса для пользователя и использовать его для отправки запросов от имени пользователя. Злоумышленнику не нужно подделывать, если у него есть токен сеанса.

Удаление SSL

Поскольку использование HTTPS является распространенной защитой от спуфинга ARP или DNS, злоумышленники используют разделение SSL для перехвата пакетов и изменения своих адресных запросов на основе HTTPS для перехода к эквивалентной конечной точке HTTP, вынуждая хост отправлять запросы к серверу в незашифрованном виде. Конфиденциальная информация может быть передана в виде простого текста.

Как обнаружить атаку «человек посередине»

Обнаружение атаки «человек посередине» может быть затруднено без принятия надлежащих мер. Если вы не пытаетесь определить, были ли перехвачены ваши сообщения, атака «человек посередине» потенциально может остаться незамеченной, пока не станет слишком поздно. Проверка надлежащей аутентификации страницы и реализация некоторого обнаружения

несанкционированного доступа обычно являются ключевыми методами обнаружения возможной атаки, но эти процедуры могут потребовать дополнительного судебного анализа постфактум.

Важно принять меры предосторожности, чтобы предотвратить атаки MITM до того, как они произойдут, а не пытаться обнаружить их, пока они активно происходят. Осведомленность о ваших методах просмотра и распознавание потенциально опасных областей может иметь важное значение для поддержания безопасной сети. Ниже мы включили пять лучших практик для предотвращения атак MITM, которые могут поставить под угрозу ваши коммуникации.

Рекомендации по предотвращению атак типа «злоумышленник посередине»

Надежное шифрование WEP/WAP на точках доступа

Наличие надежного механизма шифрования в точках беспроводного доступа предотвращает подключение нежелательных пользователей к вашей сети, просто находясь поблизости. Слабый механизм шифрования может позволить злоумышленнику взломать (/resources/testing-user-credentials-in-metasploit/)пробраться в сеть и

начать атаку «человек посередине». Чем надежнее реализация шифрования, тем безопаснее.

Надежные учетные данные для входа в маршрутизатор

Важно убедиться, что ваш логин маршрутизатора по умолчанию изменен. Не только ваш пароль Wi-Fi, но и учетные данные для входа в маршрутизатор. Если злоумышленник найдет учетные данные для входа в ваш маршрутизатор, он может изменить ваши DNS-серверы на свои вредоносные серверы. Или, что еще хуже, заразите свой роутер вредоносным ПО.

Виртуальная частная сеть

VPN можно использовать для создания безопасной среды для конфиденциальной информации в локальной сети. Они используют шифрование на основе ключей для создания подсети для безопасного обмена данными. Таким образом, даже если злоумышленник попадет в общую сеть, он не сможет расшифровать трафик в VPN.

Принудительно HTTPS

HTTPS можно использовать для безопасного обмена данными по протоколу HTTP с использованием обмена открытым и закрытым ключами. Это не позволяет злоумышленнику использовать данные, которые он может

прослушивать. Веб-сайты должны использовать только HTTPS и не предоставлять альтернативы HTTP. Пользователи могут установить плагины для браузера, чтобы всегда использовать HTTPS в запросах.

Аутентификация на основе пары открытых ключей

Атаки типа «человек посередине» обычно включают подделку того или иного объекта. Аутентификация на основе пары открытых ключей, такая как RSA, может использоваться на различных уровнях стека, чтобы убедиться, что вещи, с которыми вы общаетесь, действительно являются теми вещами, с которыми вы хотите общаться.

Объяснение и предотвращение межсайтового скриптинга (XSS) (/fundamentals/cross-site-scripting/)

Атаки вредоносных программ: анализ и передовой (/fundamentals/malware-attacks/)

Искать все вещи

ВЕРНУТЬСЯ НА ВЕРХ

РЕШЕНИЯ

Все решения (https://www.rapid7.com/solutions)

Отраслевые решения по обеспечению (https://www.rapid7.com/solutions/industry)

соответствия нормативным требованиям (https://www.rapid7.com/solutions/compliance/)

ПОДДЕРЖКА И РЕСУРСЫ

Поддержка продуктов (https://www.rapid7.com/for-customers)

Библиотека ресурсов (https://www.rapid7.com/resources)

Истории клиентов (https://www.rapid7.com/about/customers)

События и веб-трансляции (https://www.rapid7.com/about/events-webcasts)

Обучение и сертификация (https://www.rapid7.com/services/training-certification)

Основы ИТ и безопасности (https://www.rapid7.com/fundamentals)

База данных уязвимостей и эксплойтов (https://www.rapid7.com/db)

О НАС

компании (https://www.rapid7.com/about/company)

, акционерный капитал и инклюзивность (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Лидерство (https://www.rapid7.com/about/leadership)

Новости и пресс-релизы (https://www.rapid7.com/about/news)

Государственная политика (https://www.rapid7.com/about/public-policy)

открытым исходным кодом (https://www.rapid7.com/open-source/)

Инвесторы (https://investors.rapid7.com/)

СВЯЗАТЬСЯ С НАМИ

Контакты (https://www.rapid7.com/contact)

Блог (https://blog.rapid7.com/)

Служба поддержки Войти (https://support.rapid7.com/)

Карьера (https://www.rapid7.com/careers)

Свяжитесь С Нами

Man in the Middle (MITM) Attacks