3. Беспроводная оптическая связь в ультрафиолетовом с-диапазоне / Ефимова Ю. И., Прощенок Э. В., Роменский М. В., Унру П. П. // Modern Science. – 2021. – № 4-1. – С. 445-450.

Хакимхан Алина Тахировна, студент каф. электронных и квантовых средств передачи информации (ЭКСПИ), alinahakimhan@mail.ru.

Бобина Елена Андреевна, к.т.н., доцент каф. электронных и квантовых средств передачи информации (ЭКСПИ), eabobina@yandex.ru.

УДК 004.056

СРЕДСТВА ПРОВЕДЕНИЯ MITM-АТАК НА УРОВНЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Э.М.Вахитова, А.Ф.Фатхелисламов
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: анализ трафика, сетевая инфраструктура, MITM, моделирование атак, система защиты, трафик, сетевые аномалии.

Атаки типа "человек посередине" (MITM, Man-in-the-middle attack) на уровне операционной системы представляют серьезную угрозу для безопасности сетей и частной информации. В данной научной статье проводится анализ различных средств, используемых злоумышленниками для осуществления атак типа MITM на уровне операционной системы. Будут рассмотрены основные методы, такие как ARP spoofing, DNS spoofing и SSL stripping, а также уязвимости, связанные с каждым из них. Кроме того, статья представляет различные меры и средства защиты, которые могут быть использованы для предотвращения и обнаружения атак MITM на уровне операционной системы.

Сетевая атака – одна из самых больших проблем при обеспечении безопасности информации предприятий и бесперебойной работы информационных систем. Обеспечение безопасности сетевой инфраструктуры играет важную роль при проектировании систем защиты [1]. Атаки типа "Человек посередине" (MITM), проводимые на уровне операционной системы, представляют значительную угрозу безопасности информационных систем. В этой статье мы приводим обзор основных инструментов, используемых злоумышленниками для проведения MITM-атак [2], уделяя особое внимание Bettercap, Mitmproxy и Hetty в качестве наглядных примеров. MITM-атаки предполагают, что злоумышленник перехватывает сетевой трафик между двумя или более узлами и манипулирует им, выдавая себя за доверенного посредника. Такие атаки могут привести к несанкционированному раскрытию конфиденциальной информации, такой как пароли, банковские данные, а также внедрению вредоносного кода или изменению передаваемых данных. MITM-атаки на уровне операционной системы получили широкое распространение

благодаря их способности использовать уязвимости в различных сетевых протоколах.

Bettercap - это мощная платформа MITM, которая предоставляет широкий спектр возможностей для проведения сетевых атак. Она позволяет злоумышленникам выполнять ARP-подмену [3], DNS-подмену, удаление SSL и другие методы. Модульная конструкция Bettercap и расширяемый язык сценариев позволяют злоумышленникам настраивать и автоматизировать атаки, что делает его популярным выбором среди злоумышленников.

Mitmproxy - это инструмент с открытым исходным кодом, специально разработанный для перехвата, изменения и проверки трафика HTTP и HTTPS. Он действует как прокси-сервер, позволяя злоумышленникам перехватывать веб-запросы и ответы и манипулировать ими. Mitmproxy предлагает интерфейс командной строки, а также веб-интерфейс, что делает его удобным для пользователя и доступным для проведения MITM-атак.

Hetty - еще один инструмент, обычно используемый для MITM-атак. Он написан на Go и предоставляет простой, но мощный интерфейс для сбора и анализа сетевого трафика. Hetty поддерживает различные методы атак, включая ARP-спуфинг, DNS-спуфинг и перехват SSL. Его легкий дизайн и простота использования делают его популярным выбором как для начинающих, так и для опытных злоумышленников.

Чтобы исследовать возможности и потенциальные аномалии программных средств Bettercup, Mitmproxy и Hetty, были проведены экспериментальные атаки в условиях учебной лаборатории. Исследование было направлено на оценку эффективности этих инструментов при проведении MITM-атак и выявление любых аномалий, возникающих при перехвате сетевого трафика и манипулировании им.

Сначала была произведена настройка сетевую среду, состоящую из нескольких клиентских устройств и сервера, имитируя типичный сетевой сценарий. Также все устройства были правильно настроены и подключены к локальной сети.

Затем мы установили и настроили каждый инструмент — Bettercap, Mitmproxy и Hetty — на выделенном компьютере злоумышленника. Мы убедились, что инструменты были правильно настроены для выполнения MITM-атак, включая ARP spoofing, DNS spoofing, SSL stripping и другие соответствующие методы.

В ходе наших экспериментальных атак с использованием Bettercap мы обнаружили несколько аномалий в сетевом трафике:

ARP spoofing: Путем выполнения ARP spoofing Bettercap успешно перехватывал и перенаправлял сетевой трафик между клиентскими устройствами и сервером. В ходе эксперимента была выявлена неправильная маршрутизация пакетов. Это может привести к некорректной передаче пакетов, ошибкам в коммуникации между клиентом и сервером и

потенциально несанкционированному доступу к конфиденциальной информации.

DNS spoofing: Возможности DNS spoofing Bettercap позволяли нам манипулировать ответами DNS и перенаправлять клиентов на вредоносные веб-сайты. Это создавало аномалии в виде незаметного доступа пользователей к поддельным веб-сайтам, что потенциально приводило к фишинговым атакам и сбору конфиденциальных данных пользователей.

SSL stripping: С помощью функции SSL stripping в Bettercap мы успешно снизили защищенные соединения HTTPS до незашифрованного HTTP. Это приводило к аномалиям, таким как перехват и изменение конфиденциальной информации, передаваемой между клиентами и сервером, что компрометировало конфиденциальность и целостность данных.

В ходе наших экспериментальных атак с использованием Mitmproxy мы обнаружили следующие аномалии:

Манипуляция с HTTP трафиком: Mitmproxy успешно перехватывал и изменял трафик HTTP между клиентами и сервером. Это приводило к аномалиям, таким как внедрение вредоносных сценариев или контента на веб-страницы, несанкционированное изменение данных и потенциальная угроза конфиденциальной информации.

Перехват HTTPS: Возможность Mitmproxy перехватывать и расшифровывать трафик HTTPS вызывала опасения относительно целостности и конфиденциальности зашифрованного обмена данными. Эта аномалия открывала возможность несанкционированного доступа к конфиденциальной информации, включая учетные данные и личные данные.

Во время наших экспериментальных атак с использованием Hetty мы выявили следующие аномалии:

ARP spoofing: Hetty успешно выполнял ARP spoofing, что позволяло нам перехватывать и перенаправлять сетевой трафик. Это приводило к аномалиям, таким как нарушение связи, потенциальное захватывание сеансов и несанкционированный доступ к конфиденциальной информации.

DNS spoofing: Возможности DNS spoofing Hetty позволяли нам манипулировать ответами DNS и перенаправлять клиентов на вредоносные веб-сайты. Эта аномалия создавала обманчивую среду, в которой пользователи незаметно получали доступ к поддельным веб-сайтам, что потенциально компрометировало их безопасность и конфиденциальность.

В ходе наших исследований и экспериментальных атак с использованием Bettercap, Mitmproxy и Hetty мы выявили различные аномалии в перехваченном сетевом трафике и манипулировании им. Эти аномалии включали несанкционированный перехват и перенаправление трафика, внедрение вредоносного контента, изменение конфиденциальных данных и потенциальное нарушение конфиденциальности, целостности и неприкосновенности частной жизни пользователей.

Понимание этих аномалий и возможностей этих инструментов имеет решающее значение для разработки эффективных мер безопасности. Организациям и частным лицам крайне важно знать об этих рисках и использовать надежное шифрование, безопасные сетевые конфигурации и обучение пользователей, чтобы снизить угрозу MITM-атак, проводимых на уровне операционной системы.

Список использованных источников

1. Вахитова, Э. М. Моделирование сетевых атак в условиях учебной лаборатории / Э. М. Вахитова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 71-73. – EDN DCTJEB.

2. Казаков, М. Б. MITM-атаки и их предотвращение / М. Б. Казаков // Информационные технологии в деятельности органов внутренних дел : Сборник научных статей Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 32-33. – EDN HPQFWX.

3. Canteaut, A. Sieve-in-the-middle: Improved MITM attacks / A. Canteaut, M. Naya-Plasencia, B. Vayssière // Lecture Notes in Computer Science. – 2013. – Vol. 8042 LNCS, No. Part 1. – P. 222-240. – DOI 10.1007/978-3-642-40041-4_13. – EDN RHGBWB.

Вахитова Элина Маратовна, студент каф. управления информационной безопасностью, uber73lolu@gmail.com

Фатхелисламов Альфир Фирдависович, старший преподаватель каф. управления информационной безопасностью, Alfir93@mail.ru

УДК 004.056.53

ИССЛЕДОВАНИЕ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ ОПТИМАЛЬНОГО ФИЛЬТРА КОЛМОГОРОВА-ВИНЕРА

А.И. Плаван

Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Ключевые слова: обнаружение аномалий, сетевой трафик, фильтр Колмогорова-Винера, среднеквадратическая ошибка фильтрации.

Злоумышленники зачастую используют сеть как транспорт для доставки вредоносных программ до целевой системы или для доступа к конфиденциальным данным на недостаточно защищенных сетевых ресурсах. Возникновение нового источника трафика приводит к изменению общего состояния и значений статистических характеристик сети.