УДК 004.056.53

Паршинцева А.Г.

студент

РГУ нефти и газа (НИУ) им. И.М.Губкина

ARP CACHE POISONING. МЕТОДЫ ЗАЩИТЫ.

Аннотация. В рамках данной статьи рассматривается качественный подход к изучению существующих методов защиты от APR Cache Poisoning на основе проведённого моделирования. Работа была выполнена на ОС ALT Linux. В результатах исследования можно увидеть комплексную реализацию рассматриваемых методов защиты. Работа подчёркивает важность создания и повышения эффективности защитных механизмов в сфере информационной безопасности. Статья будет интересна специалистам в области информационной безопасности, а также начинающим специалистам в сфере IT, которые хотят познакомиться с работой базового протокола обмена данными.

Ключевые слова: безопасность сетей, ARP, ARP Cache Poisoning, DAI.

Parshintseva A.G.

student

Gubkin Russian State University of Oil and Gas

ARP CACHE POISONING. METHODS OF PROTECTION.

Abstract. Within the framework of this article, a qualitative approach to the study of existing methods of protection against APR Cache Poisoning based on the conducted modeling is considered. The work was done on ALT Linux OS. In the research results, you can see the comprehensive implementation of the protection methods under consideration. The work highlights the importance of creating and improving the effectiveness of protective mechanisms in the field of information security. The article will be of interest to specialists in the field of information security, as well as novice IT industry specialists who want to get acquainted with the work of the basic data exchange protocol.

Keyword: network security, ARP, ARP Cache Poisoning, DAI.

Введение. В современном мире компьютерная сеть стала неотъемлемой частью нашей повседневной жизни, а именно привычным средством коммуникации. Однако с развитием технологий и увеличением числа пользователей, чьи намерения могут быть отнюдь не добросовестными, возникают новые вызовы и проблемы, связанные с информационной безопасностью. В связи с этим появилась и продолжает существовать необходимость в создании дополнительных аппаратных и программных средств защиты сетевых ресурсов [3].

Address Resolution Protocol (ARP) атаки — это атаки второго уровня модели OSI, которые используют уязвимость данного протокола, а именно отсутствия реализации мер безопасности по отношению нарушений назначений MAC-IP для устройств. Последствия подобных атак зависят от их возникших разновидностей и целей, которые преследуют злоумышленники – так или иначе основной является перехват трафика, предназначенный для конкретного хоста и создающий помехи нормальной коммуникации в сети. Так называемое «отравление APR», представленное на Рисунке 1, происходит по следующему сценарию: чтобы плавно выполнять сопоставление MAC- и IP-адресов, каждый хост в локальной сети поддерживает локальную таблицу, называемую ARP Cache. Из-за «безотказности» протокола злоумышленник, находящийся за устройством ALT1, способен фальсифицировать пакеты, так как каждое устройство в сети может отвечать на запрос ARP независимо от того, адресован ли он ему, а жертва атаки примет его ответ как легитимный [5, С.49-50]. Прежде чем произойдет эта инкапсуляция, хосту-отправителю требуется MAC адрес хоста-получателя: учитывая IP-адрес, ARP может динамически определять MAC-адрес соответствующего хоста, а ALT1 вынуждать хост Router «подменить» истинный MAC-адрес на свой, ломающее логику сопоставления адресов и ARP-таблиц в сети. После проникновения злоумышленнику доступны всевозможные операции с трафиком – хакер

может просматривать и изменять пакеты данных, прежде чем отправить его в истинный пункт назначения, или вовсе перекрыть пути коммуникации.

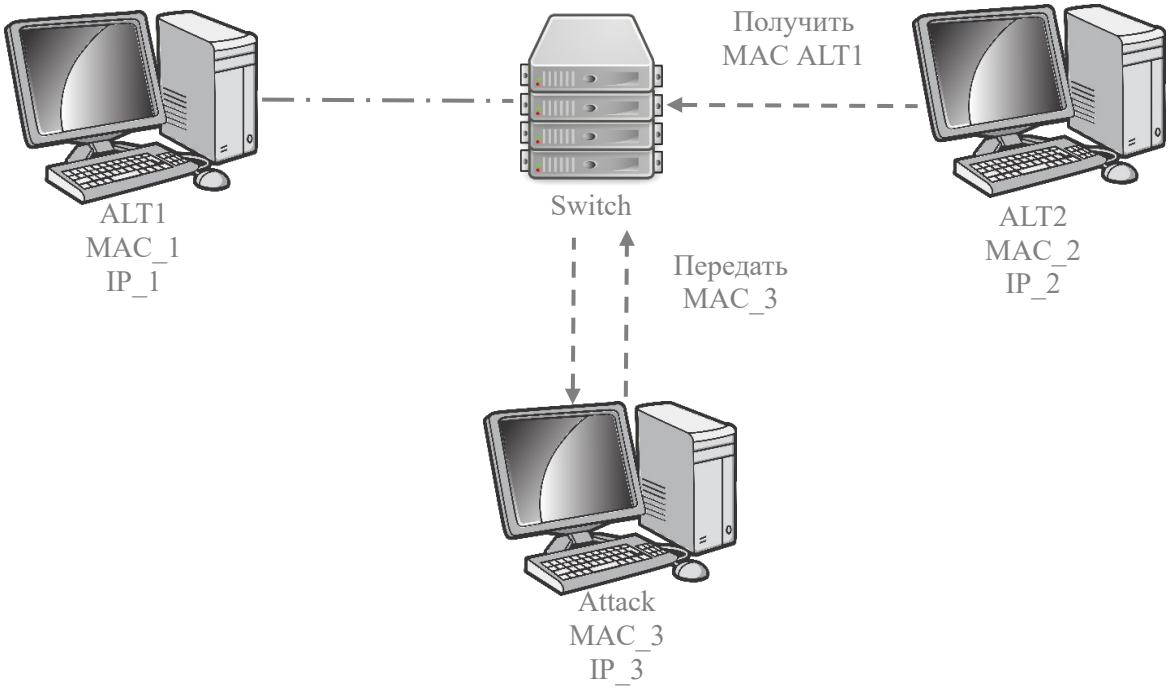

Рисунок 1 – Простейшая топология сети и результат проведения ARP Cache Poisoning Attack

Производители сетевого оборудования и программного обеспечения такие, как Cisco, Eltex, Fortinet и другие, разрабатывают решения для защиты от ARP-атак, предлагая встроенные средства безопасности в свои устройства и системы. Также некоторые организации, как OWASP (Open Web Application Security Project), включают ARP-атаки в свои методики тестирования на проникновение и оценки уязвимостей.

Современные системы также включают методы мониторинга сетевого трафика для обнаружения аномалий, связанных с подделкой ARP,

и созданные методы аутентификации ARP, а также иные решения на уровне сети.

Однако существующие методы защиты имеют ряд ограничений, и именно их грамотное комбинирование и развитие будут способствовать ресурсной и интуитивной доступности в выявлении уязвимостей и предотвращению атак на сети.

В рамках данной работы проведён анализ существующих решений по методам защиты от ARP Cache Poisoning, выявлены их сильные и слабые стороны, а также предложены комбинированные подходы и технологии для повышения уровня безопасности в сетях.

Основная цель – выявить практические решения, которые можно интегрировать в существующие инфраструктуры, а также оценке их эффективности, доступности и простоты применения, а также специфических условий пользования. Результаты исследования могут помочь в повышении уровня кибербезопасности и снижения рисков, связанных с атаками на локальные сети.

Исторический обзор. В истории разработки протоколов TCP/IP можно выделить несколько этапов, каждый из которых имел свои особенности и приоритеты. Во времена разработки первых из них аспекты безопасности были не самыми приоритетными и определяющими [2, С.172]. В связи с этим в 1982 г., когда впервые появился протокол ARP, разработчики не предусмотрели аутентификационные механизмы для проверки сообщений [4, С.49], поэтому это привело к острой постановке вопроса о защите от возникших способов атак на сети практически сразу после появления.

Одними из первых способов защиты от ARP Cache Poisoning Attack стали инспекция ARP и статические ARP-записи. Однако, с течением времени и увеличением сложности атак, эти методы оказались

недостаточными с позиции своего прямого назначения, помимо всех возможных наложенных ограничений при создании:

1. *Ограничение масштабируемости сети:* использование этих методов исключала возможность быстрого изменения в топологии сети или добавлению новых устройств;
2. *Ограничение функциональности сети:* для эффективной защиты от атак необходимо было проводить постоянную инспекцию, приводящую к дополнительным затратам времени и ресурсов на администрирование;
3. *Ограничение в автоматическом реагировании на атаки* заключалось в отсутствии управления «линиями защиты», а именно к задержкам в обнаружении и реагировании на атаки;
4. *Ограничение анализа трафика:* аналогично *пункту 3* описанные методы могут ограничивать анализ трафика, что затрудняет выявление подозрительной активности и своевременное реагирование на атаку.

На данный момент существуют несколько базовых методов по обеспечению предотвращения ARP атак: статический (сохранился из ранних), динамический и специальные средства мониторинга на примере ARPwatch.

Статические ARP-таблицы. Один из самых простых и эффективных методов защиты от ARP атак, существующих в современных реалиях. Суть заключается в назначении фиксированных пар MAC-IP адресов; доступна совместная работа с инструментами для автоматического сканирования сети и сбора информации.

Ограничением метода является эффективность исключительно в небольших сетях, где количество возможных ARP-запросов ограничено из-за увеличения числа возможных комбинаций MAC-IP адресов.

Статические ARP-таблицы требуют регулярного управления и обслуживания для обновления пар MAC-IP адресов при добавлении или удалении устройств. Регулярное создание резервных копий ARP-таблиц обеспечит возможность восстановления в случае сбоя или атаки. В случае обнаружения подозрительной активности или несоответствий в ARP-таблицах необходимо уведомить администратора сети для принятия соответствующих мер.

Dynamic ARP Inspection (DAI). Способ также активно используется для предотвращения ARP Cache Poisoning атак путём настройки функции безопасности DHCP Snooping или DAI на коммутаторе. В данной процедуре не мало важную роль играет архитектура охраняемой сети, а именно разделение на сегменты (в примере VLAN): когда устройство VLAN с поддержкой DAI получает пакет ARP, оно сопоставляет IP-адрес источника, MAC-адрес источника, идентификатор VLAN и номер интерфейса пакета ARP с записями привязки в таблице DAI, содержащая MAC-адрес источника, VLAN и номер интерфейса – они создаются динамически с помощью отслеживания DHCP. На основе результатов сопоставления принимается решение о том, является ли пакет действительным (пропустить) или подозрительным (отбросить): запись о подозрительных пакетах может быть занесена в журнал событий для последующего анализа или генерации оповещений для администраторов.

Стоит отметить, что только устройства, поддерживающие DAI, могут участвовать в данном процессе, например *MES1428 Eltex* [1], используемый для проведения моделирования.

Специальные средства мониторинга (Arpwatch). Данного типа программы предназначены для отслеживания активности трафика в сети, а именно изменения пар MAC-IP адресов – эти данные могут быть получены

из различных источников, включая маршрутизаторы, коммутаторы и конечные устройства.

Методы сбора данных включает в себя активный и пассивный способ: первый отправляет ARP-запросы на устройства в сети, чтобы получить их MAC-адреса и соответствующие IP-адреса для формирования указанной базы данных текущих пар MAC-IP, которая может быть локальной или централизованной; второй использует журналы событий маршрутизаторов и коммутаторов.

Суть работы последнего заключается в регистрации изменений в формате сообщения или отчёта по электронной почте администратору при добавлении или изменении пары в режиме реального времени.

Arpwatch хорошо себя показывает в интеграции с другими сетевыми инструментами и методами защиты: программа предлагает гибкие настройки, обеспечивающие полный контроль и управление сетевой инфраструктурой любой сложности.

Согласно заданной топологии и описанным характеристикам, было проведено комплексное оснащение сети: на ALT1, описанном как пункт назначения, настраиваем статическую таблицу, сопоставляя MAC-IP ALT2 –

назначение «доверенного порта» на коммутаторе Switch невозможно в рамках данной топологии, так как все порты, подключенные к конечному пользователю, не являются доверенными [4]. Настройка произведена с помощью команды *arp -s **IP_2 MAC_2.***

На самом ALT2 будет применён динамический метод защиты включением функции DAI – для этого предварительно проведена настройка DHCP Spoofing. Основными этапами настройки являются [4]:

1. Добавление ALT2 в access-list командой

*permit ip host **IP_2** mac host **MAC_2***

или

*arp access-list **ALT2**;*

2. Ожидаем заполнение ARP-таблицы;
3. Включаем ARP Inspection в режиме глобальной конфигурации командой, где *vlan **<id>*** обеспечивает дополнительную защиту сети за счёт её сегментированности:

   *ip arp inspection vlan **<id>** ;*

4. *Опционально можно добавить дополнительные проверки на соответствие MAC адресов в заголовках ARP и Ethernet:

   *ip arp inspection validate **<option>.***

Анализ трафика с помощью APRwatch проходит на ALT1: согласно алгоритму работы, ложная тревога не будет генерироваться, так как программа полагается только на ARP-трафик путем локальной проверки на соответствующем хосте.

При проведении атаки подозрительная активность была зафиксирована. Результаты исследования и эффективности рассматриваемых методов расположены в Таблице 1 и включают себя как оценку по общепринятым критериям внедрения методов защиты информации (п.1-3), так и анализ с позиции определенных ранее ограничений.

Таблица 1 – Результаты исследования

Критерии	Статический метод	Динамический метод	ARPwatch
	1	**2**	**3**
1. Защищённость[1]	**1**	**2**	-
2. Простота реализации	**1**	**3**	**2**
3. Минимальные затраты на реализацию	**1**	**3**	**2**
4. Решение ограничения функциональности сети:	✕	✓	✓

[1] Ключевой критерий в данной выбоке – доказательство действия данного метода защиты.

4.1. Рекомендуемый размер сети	Маленький	Любой	Любой
5. Решение ограничения масштабируемости сети	✕	✓	✓
6. Решение ограничения в автоматическом реагировании на атаки:	✕	✓	✓
6.1. Исключение возможности ложных срабатываний	-	✕	✕
7. Решение ограничения анализа трафика	✕	✕	✓
8. Совместимость с другими средствами защиты	✓	✓	✓

Эксперимент показал, что существующие методы не являются универсальными в решении вопроса безопасности сетей.

Статический метод является самым простым и эффективным в данной выборке, не требует никаких ресурсов, однако доказывает свою несостоятельность в самостоятельном решении вопроса безопасности в быстро растущей и развивающейся отрасли – его рекомендуется использовать на отдельных машинах и сегментах сети, на которых не планируются изменения.

Динамический метод является одним из самых распространённых в данной выборке, ключевым решением в настоящий момент, однако также имеет ряд недостатков: метод требует ряд дополнительных настроек и накладывает ряд новых ограничений на сеть, например ограничения скорости передачи.

ARPwatch, который имеет наибольшее количество преимуществ по выделенныи критериям, представляет из себя лишь вспомогательный элемент для реальных сетей и требует обязательной организационной работы с персоналом по обучению работе с программой.

Заключение. В рамках проведенного исследования была доказана важность разностороннего подхода в обеспечении безопасности от вида атаки ARP Cache Poisoning – ни один из рассматриваемых методов не является универсальным в решении вопросов безопасности; в комплексе

же они способны действовать с позиции как активной защиты сети, так и мониторинга сетевой активности с реализацией организационных мер и общих мер обеспечения сетевой безопасности.

Результаты подчеркивают необходимость постоянного совершенствования методов защиты и адаптации к новым угрозам, чтобы оставаться на шаг впереди киберпреступников. В будущих исследованиях может быть развёрнуто тестирование новых технологий обнаружения и предотвращения ARP Cache Poisoning на базе машинного обучения и искусственного интеллекта для повышения точности и скорости реагирования на угрозы.

СПИСОК ИСТОЧНИКОВ

1. MES1428 Eltex | Коммутатор 24 порта 100M / [Электронный ресурс] // Eltex Коммуникации | Официальный дилер Eltex : [сайт]. — URL: https://eltexcm.ru/catalog/ethernet-kommutatory/kommutatory-dostupa-100m/mes1428.html?utm_medium=cpc&utm_source=yandex&utm_campaign=78721658&utm_content=cid%7C78721658%7Cgid%7C5038644987%7Caid%7C12814399673%7Cadp%7Cno%7Cdvc%7Cdesktop%7Cpid%7C41265959818%7Crid%7C41265959818%7Cdid%7C41265959818%7Cpos%7Cpremium1%7Cadn%7Csearch%7Ccrid%7C0%7C&utm_term=mes1428&roistat_referrer=none&roistat_pos=premium_1&roistat=direct6_search_12814399673_mes1428&yclid=2558028141143261183 (дата обращения: 28.10.2024).

2. Дубров, С. В. ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ (курс лекций) [Текст] / С. В. Дубров — Новосибирск: Новосибирский государственный университет, 2012 — 259 с.

3. Палмер Майкл, Синклер Роберт Брюс. Проектирование и внедрение компьютерных сетей. Учебное пособие 2-издание. СПб.: BHV, 2004. — 752с.
4. Технологии безопасности сети на 2-ом уровне OSI. Часть 1 / [Электронный ресурс] // Хабр : [сайт]. — URL: https://habr.com/ru/articles/313782/#Dynamic%20ARP%20inspection (дата обращения: 27.11.2024).
5. Уймин, А. Г. Компьютерные сети. L2-технологии: практикум [Текст] / А. Г. Уймин — Москва: Ай Пи Ар Медиа, 2024.