Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)

ОТЧЁТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Тип практики: производственная

Название предприятия: АО «НПО «Эшелон»

Студент:
Булатов Марк Станиславович,
группа ИУ8-62 (3 курс)

(подпись, дата)

Руководитель от предприятия:
ведущий разработчик, Борзых Сергей Сергеевич

(подпись, дата)

Руководитель от кафедры:
доцент кафедры ИУ8, Зайцева Анастасия Владленовна _____

(подпись, дата)

Оценка: отлично

Москва, 2021

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Тип практики: производственная

Название предприятия: АО «НПО «Эшелон»

Сроки практики: с 7 июля 2021 г. по 20 июля 2021 г.

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

За время прохождения практики студенту надлежит согласно программе практики:

- **Изучить** причины отправления ARP, предотвращение ARP-спуфинга.

Студент:
Булатов Марк Станиславович,
группа ИУ8-62 (3 курс)

(подпись, дата)

Руководитель от предприятия:
ведущий разработчик, Борзых Сергей Сергеевич

(подпись, дата)

Руководитель от кафедры:
доцент кафедры ИУ8, Зайцева Анастасия Владленовна _____

(подпись, дата)

Является обязательным листом отчёта по практике. Лист 2
Документ не должен содержать информацию, отнесённую в установленном порядке к государственной тайне РФ.

Оглавление

Введение 4

Основная часть 5

1. Характеристика предприятия 5
2. Практическая часть 7

Заключение 17

Список использованных источников 18

Введение

Время прохождения практики

- Срок прохождения практики – с 7 июля 2021 г. по 20 июля 2021 г.

Цели и задачи практики

- Изучение причин отправления ARP.
- Изучение предотвращения ARP-спуфинга.

Поставленные цели и задачи позволяют тщательно разобраться в том, что представляет собой ARP и как злоумышленник может воздействовать на ARP в своих интересах. Также полученные знания помогут понять, что такое ARP-спуфинг, чем он отличается от отправления ARP и как можно защититься от них обоих.

Основная часть

1. Характеристика предприятия

АО «НПО «Эшелон» - один из лидеров российского рынка информационной безопасности. Наша команда объединяет профессионалов, имеющих различные звания и статусы, среди которых: кандидаты наук, CISSP, CISA, SBCI и сертифицированные специалисты Cisco, IBM, Microsoft и др. Компания «Эшелон» аккредитована в качестве испытательной лаборатории Минобороны России, ФСТЭК России, ФСБ России. АО «НПО «Эшелон» является органом по сертификации ФСТЭК России, органом по аттестации ФСТЭК России и аттестационным центром Минобороны России. Компания предоставляет услуги по проведению сертификационных испытаний средств защиты информации, защите персональных данных, аудиту информационной безопасности, тестированию на проникновение, аттестации объектов информатизации и др. Так же на базе объединения ведутся разработки собственных программных решений информационной безопасности. Компанией учрежден учебный центр «Эшелон», в котором проводится переподготовка специалистов по программам информационной безопасности, согласованным с ФСТЭК России, Минобороны России, СДС «Военный Регистр». [1]

АО «НПО «Эшелон» специализируется на комплексном обеспечении информационной безопасности.

Основными направлениями деятельности являются:

- проектирование, внедрение и сопровождение комплексных систем обеспечения информационной безопасности;
- сертификация программных и программно-аппаратных средств;
- аттестация объектов информатизации, в том числе защищенных помещений, автоматизированных рабочих мест, локальных вычислительных сетей;

- лицензирование деятельности в области создания средств защиты информации;
- проведение анализа защищенности компьютерных систем;
- аудит информационной безопасности организаций;
- проектирование и аудит систем управления (менеджмента) информационной безопасностью;
- разработка стратегий, политик, стандартов и процедур по обеспечению информационной безопасности, профилей защиты, заданий по безопасности;
- обучение сотрудников компаний по вопросам обеспечения информационной безопасности;
- поставка оборудования и средств защиты информации;
- разработка средств защиты информации, средств анализа эффективности защиты информации и устройств (схемотехнических решений) в защищенном исполнении;
- обеспечение технической поддержки и сопровождение поставляемых решений, систем и продуктов;
- испытания, экспертизы, исследования в области безопасности информации;
- оценка применяемых процедур безопасной разработки программного обеспечения;
- выстраивание процессов безопасной разработки;
- внедрение ГОСТ 56939-2016;
- аудит информационной безопасности программного обеспечения, а также банковских приложений;
- проведение анализа уязвимостей в соответствии с требованиями 382-П, 683-П, 684-П ЦБ РФ, а также оценки соответствия требованиям профилей защиты ЦБ РФ. [2]

2. Практическая часть

Что такое ARP?

ARP (англ. Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера.[3] ARP позволяет подключенным к сети устройствам запрашивать, какому устройству в настоящее время назначен конкретный IP-адрес (рис.1). Устройства также могут сообщать об этом назначении остальной части сети без запроса. В целях эффективности устройства обычно кэшируют эти ответы и создают список текущих назначений MAC-IP.

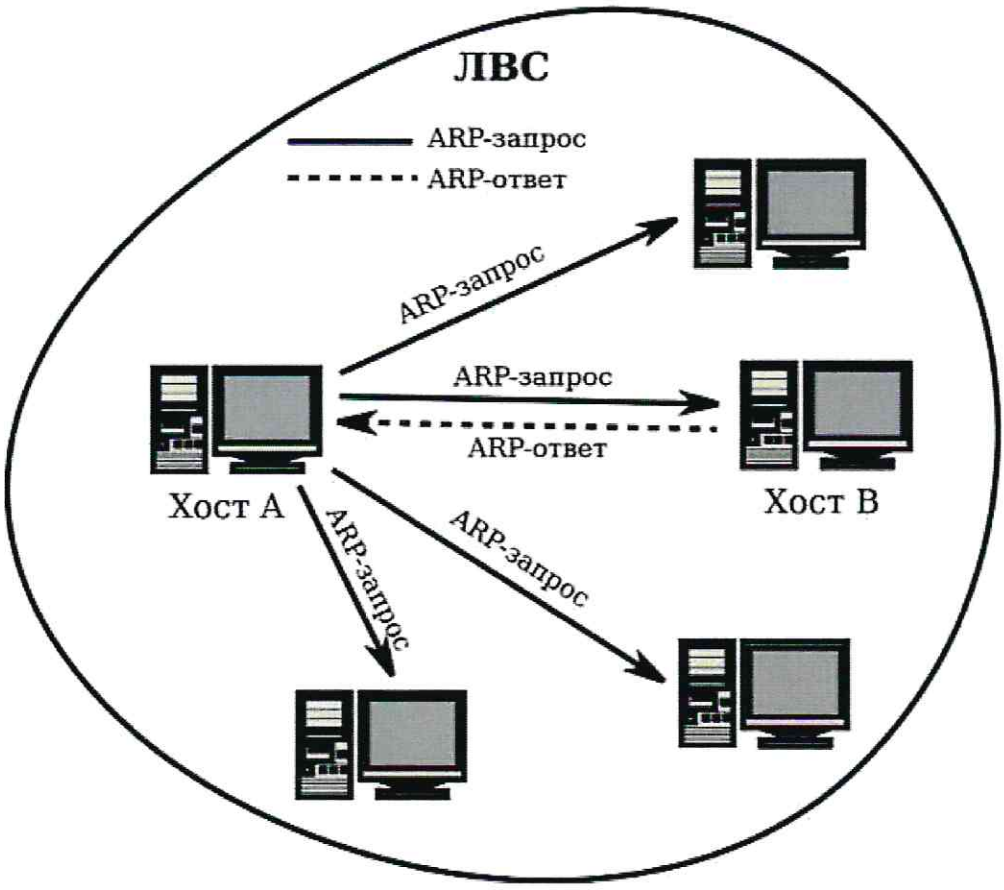

Рис.1. Пример работы ARP.

Что такое отравление ARP?

«Отравление» ARP (ARP Poisoning) — это тип кибератаки, которая использует слабые места широко распространенного протокола разрешения адресов (Address Resolution Protocol, ARP) для нарушения или перенаправления

сетевого трафика или слежения за ним. В 1982 году, когда был представлен протокол ARP, обеспечение безопасности не было первостепенной задачей, поэтому разработчики протокола никогда не использовали механизмы аутентификации для проверки сообщений ARP. Любое устройство в сети может ответить на запрос ARP, независимо от того, является ли оно адресатом данного запроса. Например, если компьютер А запрашивает MAC-адрес компьютера В, ответить может злоумышленник на компьютере С, и компьютер А примет этот ответ как достоверный. За счет этой уязвимости было проведено огромное количество атак. Используя легкодоступные инструменты, злоумышленник может «отравить» кэш ARP других хостов в локальной сети, заполнив его неверными данными (рис.2).

Рис.2. Отравление ARP.

Какова цель отравления ARP?

У хакеров всегда самые разные мотивы, в том числе при осуществлении отравления ARP, начиная от шпионажа высокого уровня и заканчивая азартом создания хаоса в сети. В одном из возможных сценариев злоумышленник может использовать ложные сообщения ARP, чтобы взять на себя роль шлюза

по умолчанию для данной подсети, эффективно направляя весь трафик на свое устройство вместо локального маршрутизатора. Затем он может следить за трафиком, изменять или сбрасывать его. Такие атаки являются «громкими», поскольку оставляют за собой улики, но при этом не обязательно влияют на работу сети. Если целью атаки является шпионаж, машина злоумышленника просто перенаправляет трафик изначальному адресату, не давая ему оснований подозревать, что что-то изменилось. Другой целью может быть значительное нарушение работы сети. Например, довольно часто DoS-атаки выполняются не очень опытными хакерами просто для получения удовольствия от созданных проблем.

Опасным типом отравления ARP являются инсайдерские атаки. Поддельные сообщения ARP не выходят за пределы локальной сети, поэтому атака должна исходить от локального устройства. Внешнее устройство также потенциально может инициировать ARP-атаку, но сначала ему нужно удаленно скомпрометировать локальную систему другими способами, в то время как инсайдеру требуется только подключение к сети и некоторые легкодоступные инструменты.

Типы атак ARP Poisoning.

Имеется два основных способа отравления ARP: злоумышленник может либо дождаться запроса ARP в отношении конкретной цели и дать на него ответ, либо использовать самообращённые запросы (gratuitous ARP). Первый вариант ответа будет менее заметен в сети, но его потенциальное влияние также будет меньшим. Самообращенные запросы ARP могут быть более эффективными и затронуть большее количество жертв, но они имеют обратную сторону — генерирование большого объема сетевого трафика. При любом подходе поврежденный кэш ARP на устройствах-жертвах может быть использован для дальнейших целей:

- **Атаки Man-in-the-Middle.** Атаки MiTM, вероятно, являются наиболее распространенной и потенциально наиболее опасной целью отравления

ARP. Злоумышленник отправляет ложные ответы ARP по заданному IP-адресу (рис.3). Это заставляет устройства-жертвы заполнять свой кэш ARP MAC-адресом машины злоумышленника вместо MAC-адреса локального маршрутизатора. Затем устройства-жертвы некорректно пересылают сетевой трафик злоумышленнику. Такие инструменты, как Ettercap, позволяют злоумышленнику выступать в роли прокси-сервера, просматривая или изменяя информацию перед отправкой трафика по назначению. Жертва при этом может не заметить каких-либо изменений в работе. Одновременное отравление ARP и отравление DNSможет значительно повысить эффективность атаки MiTM. В этом сценарии пользователь-жертва может ввести адрес легитимного сайта (например, google.com) и получить IP-адрес машины злоумышленника вместо корректного адреса.

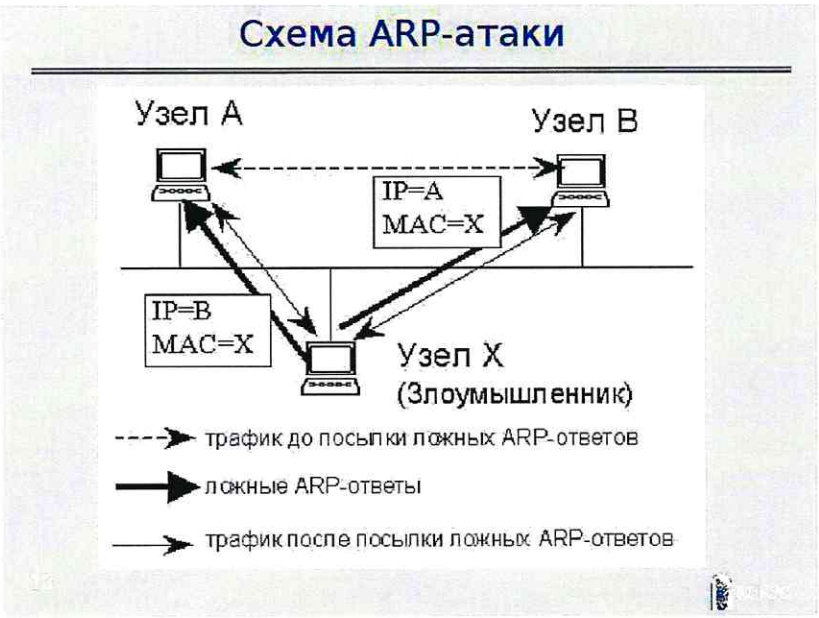

Рис.3. Атаки Man-in-the-Middle.

- **Отказ в обслуживании (Denial of Service, DoS).** DoS-атака заключается в том, что одной или нескольким жертвам отказывается в доступе к сетевым ресурсам (рис.4). В случае ARP, злоумышленник может отправить ответ ARP, который ложно назначает сотни или даже тысячи

IP-адресов одному MAC-адресу, что потенциально может привести к перегрузке целевого устройства. Атака этого типа, иногда называемая «лавинной рассылкой ARP» (ARP-флудингом), также может быть нацелена на коммутаторы, что потенциально может повлиять на производительность всей сети.

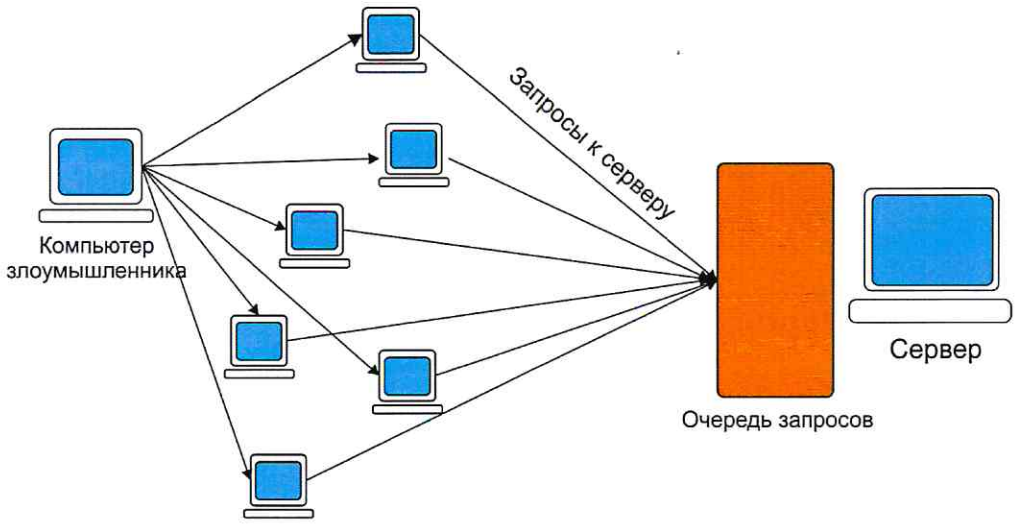

Рис.4. Отказ в обслуживании.

- **Перехват сеанса.** Перехват сеанса по своей природе похож на MiTM за исключением того, что злоумышленник не будет напрямую перенаправлять трафик с машины жертвы на целевое устройство. Вместо этого он захватывает подлинный порядковый номер TCP или файл cookie жертвы и использует его, чтобы выдавать себя за жертву. Так он может, к примеру, получить доступ к учетной записи данного пользователя в социальные сети, если тот в нее вошел.

Этапы отравления ARP.

Этапы отравления ARP могут различаться, но обычно их минимальный перечень таков:

1) Злоумышленник выбирает машину или машины жертвы. Первым шагом в планировании и реализации атаки ARP Poisoning является выбор цели.

Это может быть конкретная конечная точка в сети, группа конечных точек или сетевое устройство, такое как маршрутизатор. Маршрутизаторы являются привлекательными целями, поскольку успешное отравление ARP маршрутизатора может нарушить трафик для всей подсети.

2) Злоумышленник запускает инструменты и начинает атаку. Всем злоумышленникам, желающим выполнить отравление ARP, легко оступен широкий спектр инструментов. После запуска выбранного инструмента и настройки соответствующих параметров злоумышленник начинает атаку. Он может незамедлительно начать рассылку сообщений ARP или дождаться получения запроса.
3) Злоумышленник выполняет определенные действия с некорректно направленным трафиком. После повреждения кэша ARP на устройстве (устройствах) жертвы злоумышленник обычно выполняет какие-то действия с некорректно направленным трафиком. Он может просматривать или изменять его, либо создать «черную дыру», чтобы данные никогда не доходили до адресата. Выбор действий зависит от мотивов злоумышленника.

Отличия ARP-спуфинг от отравления ARP.

Термины «ARP-спуфинг» и «отравление ARP» обычно используются как синонимы. Под спуфингом (рис.5) понимается выдача злоумышленником своего адреса за MAC-адрес другого компьютера, в то время как отравлением называют повреждение ARP-таблиц на одной или нескольких машинах-жертвах. Однако на практике это элементы одной и той же атаки. [4] Эту атаку иногда называют «отравлением кэша ARP» или «повреждением ARP-таблицы».

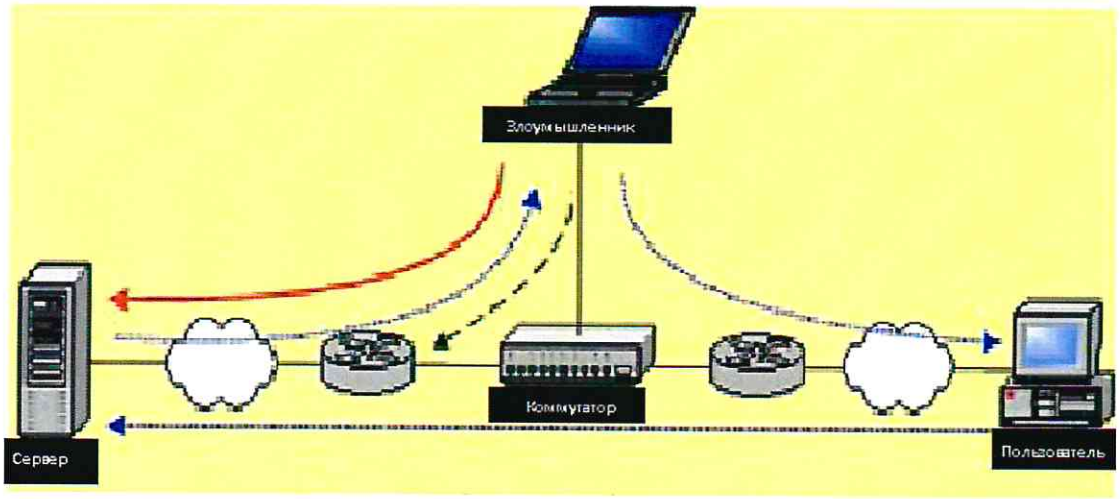

Рис.5. ARP-спуфинг.

Как обнаружить отравление кэша ARP.

Существует множество платных программ и программ с открытым исходным кодом для обнаружения отравления кэша ARP, однако проверить ARP-таблицы на своем компьютере можно даже без установки специального ПО. В большинстве систем Windows, Mac и Linux ввод команды arp -a в терминале или командной строке отобразит текущие назначения IP-адресов и MAC-адресов машины (рис.6). Если таблица содержит два разных IP-адреса, которые имеют один и тот же MAC-адрес, то вы, вероятно, подвергаетесь атаке отравления ARP.

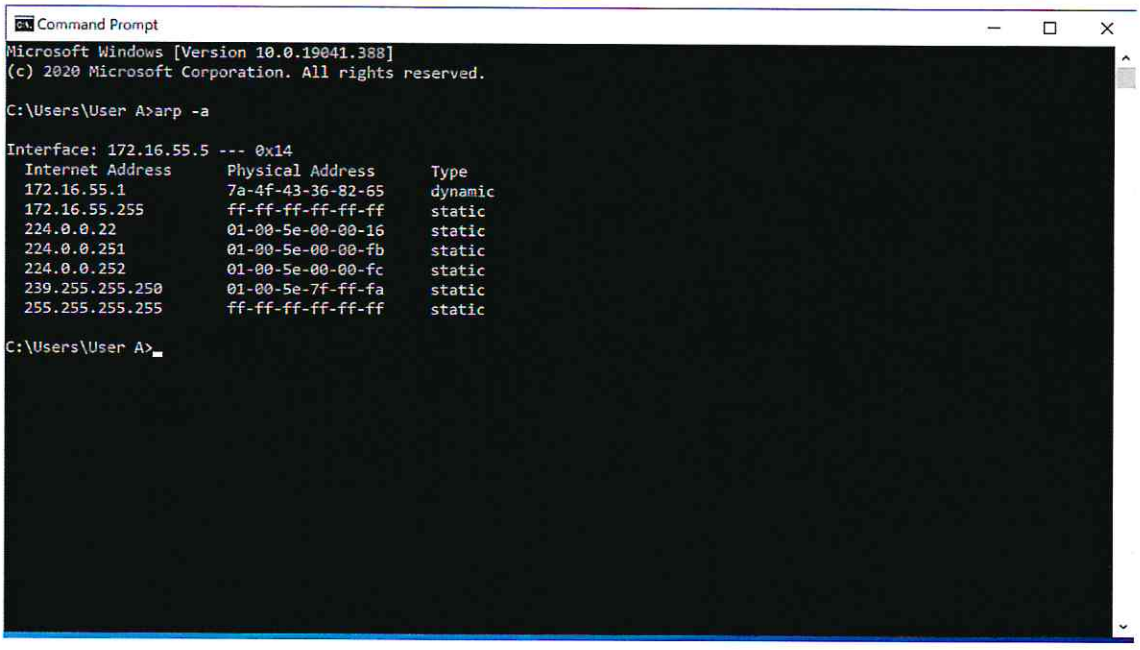

Рис.6. Ввод команды arp -a в командной строке.

Пример отравления ARP представлен в таблице 1. На ней можно увидеть, что физические адреса первого и третьего интернет-адреса совпадают. Вероятнее всего под третьим интернет-адресом и кроется злоумышленник.

Таблица 1. Пример отравления ARP.

Интернет-адрес	Физический адрес
192.168.0.1	00-17-31-dc-39-ab
192.168.0.105	40-d4-48-cr-29-b2
192.168.0.106	00-17-31-dc-39-ab

Такие инструменты, как arpwatch и X-ARP, позволяют осуществлять непрерывный мониторинг сети и могут предупредить администратора о выявлении признаков отравления кэша ARP. Однако достаточно высока вероятность ложных срабатываний.

Как предотвратить отравление ARP.

Существует несколько методов предотвращения отравления ARP:

- **Статические ARP-таблицы.** Можно статически назначить все MAC-адреса в сети соответствующим IP-адресам. Это очень эффективно для предотвращения отравления ARP, но требует огромных трудозатрат. Любое изменение в сети потребует ручного обновления ARP-таблиц на всех хостах, в связи с чем для большинства крупных организаций использование статических ARP-таблиц является нецелесообразным. Но в ситуациях, когда безопасность имеет первостепенное значение, выделение отдельного сегмента сети для статических ARP-таблиц может помочь защитить критически важную информацию. [5]
- **Защита коммутатора.** Большинство управляемых коммутаторов Ethernet оснащены функциями предотвращения атак ARP Poisoning. Эти функции, известные как динамическая проверка ARP (Dynamic ARP Inspection, DAI), оценивают достоверность каждого сообщения ARP и отбрасывают пакеты, которые выглядят подозрительными или вредоносными. С

помощью DAI также можно ограничить скорость прохождения сообщений ARP через коммутатор, эффективно предотвращая DoS-атаки. DAI и аналогичные функции когда-то были доступны исключительно для высокопроизводительного сетевого оборудования, но теперь они представлены практически на всех коммутаторах бизнес-класса, в том числе используемых в небольших компаниях. Обычно рекомендуется включать DAI на всех портах, кроме подключенных к другим коммутаторам. Эта функция не оказывает значительного влияния на производительность; при этом, вместе с ней может понадобиться включение других функций, например DHCP Snooping. Включение защиты порта на коммутаторе также может помочь минимизировать последствия отравления кэша ARP. Защиту порта можно настроить таким образом, чтобы разрешить использование только одного MAC-адреса на порте коммутатора, что лишает злоумышленника возможности применять несколько сетевых идентификаторов.

- **Физическая защита.** Предотвратить атаки ARP Poisoning также поможет надлежащий контроль физического доступа к рабочему месту пользователей. Сообщения ARP не выходят за пределы локальной сети, поэтому потенциальные злоумышленники должны находиться в физической близости к сети жертвы или уже иметь контроль над машиной в сети. Обратите внимание, что в случае беспроводной сети территориальная близость не обязательно означает прямой физический доступ: может быть достаточно сигнала, который достигает двора или парковки. Независимо от типа соединения (проводное или беспроводное), использование технологии наподобие 802.1x может гарантировать подключение к сети только доверенных и/или управляемых устройств.

- **Сетевая изоляция.** Хорошо сегментированная сеть может быть менее

восприимчива к отравлению кэша ARP в целом, поскольку атака в одной подсети не влияет на устройства в другой. Концентрация важных ресурсов в выделенном сегменте сети с более строгими мерами безопасности может значительно снизить потенциальное влияние атаки ARP Poisoning.

- **Шифрование.** Хотя шифрование не предотвращает ARP-атаку, оно может снизить потенциальный ущерб. Раньше популярной целью атак MiTM было получение учетных данных для входа в систему, которые когда-то передавались в виде обычного текста. Благодаря распространению шифрования SSL/TLS совершать такие атаки стало сложнее.

Заключение

В ходе прохождения практики были получены и закреплены знания по поставленным целям и задачам, а именно:

- Что такое ARP
- Что такое отравление ARP и этапы отравления, а также его разновидности отравления
- Что такое ARP-спуфинг и чем он отличается от отравления ARP
- Методы обнаружения воздействия злоумышленника на ARP
- Способы защиты от ARP-спуфинга или отравления ARP

Список использованных источников

1. Руководство по АО «НПО «Эшелон». – Режим доступа: https://npo-echelon.ru/ (дата обращения: 15.07.2021)
2. Руководство по основным направлениям деятельности АО «НПО «Эшелон». – Режим доступа: https://npo-echelon.ru/about/(дата обращения: 15.07.2021)
3. Руководство по протоколу ARP. – Режим доступа: https://ru.wikipedia.org/wiki/ARP (дата обращения: 15.07.2021)
4. Руководство по ARP-спуфингу. – Режим доступа: https://heritage-offshore.com/vpn-i-konfidencialnost/arp-otravlenie-poddelka-kak-obnaruzhit-i/ (дата обращения: 15.07.2021)
5. Руководство по предотвращению отравления ARP. – Режим доступа: https://codeby.net/threads/arp-zarazhenie-i-spufing-obnaruzhenija-i-predotvraschenija.66772/ (дата обращения: 15.07.2021)