МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Забайкальский государственный университет»

(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет

Кафедра информатики, вычислительной техники и прикладной математики

КУРСОВОЙ ПРОЕКТ

по дисциплине: Протоколы вычислительных систем

на тему «Реализация атаки ARP spoofing»

Выполнил ст. гр. ИВТ-20,

Борисова Е.О.

Проверил доцент кафедры ИВТ и ПИ

Машкин В.А.

Чита

2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Забайкальский государственный университет»

(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет

Кафедра информатики, вычислительной техники и прикладной математики

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

по 09.03.01 Информатика и вычислительная техника

на тему «Реализация атаки ARP spoofing»

Выполнил студент группы ИВТ-20 Борисова Екатерина Олеговна

Руководитель работы: доцент Машкин Владимир Анатольевич.

Чита

2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Забайкальский государственный университет»

(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет

Кафедра информатики, вычислительной техники и прикладной математики

ЗАДАНИЕ

на курсовой проект

по дисциплине: Протоколы вычислительных систем

Студенту Борисовой Екатерине Олеговне

направления подготовки 09.03.01 Информатика и вычислительная техника

1. Тема курсового проекта: Реализация атаки ARP spoofing
2. Срок подачи студентом законченной работы: 26.05.2023 г.
3. Исходные данные к проекту: знания о протоколе ARP подробное описание атаки, инструменты для реализации атак.
4. Перечень подлежащих разработке в курсовом проекте вопросов:
5. Исследование существующих атак на протокол ARP;
6. Анализ данных;
7. Реализация атаки на протокол ARP.

Дата выдачи задания 06.02.2023 г.

Руководитель курсового проекта \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/В.А. Машкин/

Задание принял к исполнению 06.02.2023 г.

Подпись студента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Е.О. Борисова/

РЕФЕРАТ

Пояснительная записка – 20 с, 10 рис., 3 источников

ARP, ARP-Spoofing, локальная сеть, кража данных.

Цель работы состоит в том, чтобы изучить атаку ARP Spoofing.

**Календарный график**

Утверждаю

Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_

«\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

выполнения курсовой работы

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Наименование раздела курсовой работы | Февраль | | Март | | | | Апрель | | | | Май | | | |
| 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Выдача задания |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Поиск источников информации |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Теоретическая часть |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Реализация и настройка приложения |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Программная реализация |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Тестирование |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Оформление пояснительной записки |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | Защита работы |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

План выполнен: руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, расшифровка подписи)

«\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 7](#_Toc165071100)

[1 Анализ задачи 8](#_Toc165071101)

[1.1 Описание предметной области 8](#_Toc165071102)

[1.2 Постановка задачи 8](#_Toc165071103)

[2 Анализ данных 9](#_Toc165071104)

[3 Программная реализация 10](#_Toc165071105)

[4 Руководство пользователя 11](#_Toc165071106)

[5 Анализ полученных результатов 12](#_Toc165071107)

[ЗАКЛЮЧЕНИЕ 13](#_Toc165071108)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 14](#_Toc165071109)

ВВЕДЕНИЕ

Протокол ARP играет ключевую роль в переводе IP-адресов в физические MAC-адреса в локальных сетях. Он позволяет сетевым устройствам идентифицировать друг друга на уровне канала данных, что обеспечивает правильную доставку пакетов данных в Ethernet-сетях. Без ARP коммуникация между устройствами в сети была бы невозможна, так как устройства не знали бы физические адреса друг друга.

ARP уязвим по ряду причин, главным образом из-за отсутствия механизма аутентификации или проверки подлинности запросов и ответов ARP. Вот несколько причин, почему ARP может быть уязвим:

1. ARP-Spoofing (ARP-подмена): поскольку ARP не проверяет подлинность источника, злоумышленники могут отправлять поддельные ARP-ответы, чтобы перенаправить сетевой трафик к себе или к другим нежелательным местам. Это позволяет злоумышленникам перехватывать трафик, осуществлять атаки "человек-посередине" или вызывать перебои в работе сети;
2. отсутствие шифрования: ARP-сообщения передаются в открытом виде, что позволяет злоумышленникам легко перехватывать и изменять их в процессе передачи;
3. уязвимость к атакам "Denial of Service" (DoS): Отправка большого количества поддельных ARP-ответов или запросов может вызвать перегрузку сети или повлиять на нормальное функционирование устройств в сети;
4. отсутствие механизма мониторинга: Большинство сетевых устройств не имеют встроенных механизмов мониторинга или журналирования для отслеживания подозрительной активности ARP, что делает обнаружение атак затруднительным.

В данной работе рассматривается ARP-Spoofing.

**1** **Анализ задачи**

**1.1 Описание предметной области**

ARP (Address Resolution Protocol, RFC 826) — протокол для определения соответствия между логическим адресом сетевого уровня (IP) и физическим адресом устройства (MAC). Сама связь между двумя устройствами в сети проходит именно на канальном уровне [1]

ARP spoofing (ARP-подмена) – это атака, при которой злоумышленник вводит в сеть поддельные ARP-сообщения, чтобы перехватить или изменить сетевой трафик [2].

ARP spoofing представляет значительную угрозу безопасности, поскольку злоумышленник может:

* перехватывать данные: изменяя таблицу ARP, злоумышленник может заставить трафик от одного устройства идти через его компьютер, позволяя ему отслеживать или изменять пакеты данных;
* выполнить атаку "человек посередине" (MitM): это позволяет злоумышленнику изменить данные в реальном времени или перенаправить трафик к другим целям;
* создать сети-дубли: подмена ARP также может вызвать появление множества устройств с одним и тем же IP-адресом, что приводит к отказу в обслуживании (DoS).

В нормальных условиях устройство посылает ARP-запрос в сеть, чтобы узнать MAC-адрес, связанный с конкретным IP-адресом. Сеть отвечает соответствующим ARP-ответом, который записывается в ARP-таблицу устройства для дальнейшего использования. Однако в случае ARP spoofing злоумышленник, пользуясь тем, что ARP-ответы не проверяются и автоматически записываются в таблицу, отправляет поддельные ARP-ответы, привязывая свой MAC-адрес к IP-адресам других устройств. Это приводит к неверной маршрутизации трафика.

ARP spoofing может быть частью более крупных атак, включая кражу данных, распространение вредоносного ПО или взлом инфраструктуры. Однако важно отметить, что использование данных техник без разрешения является незаконным, и предназначены они исключительно для тестирования безопасности и исследований.

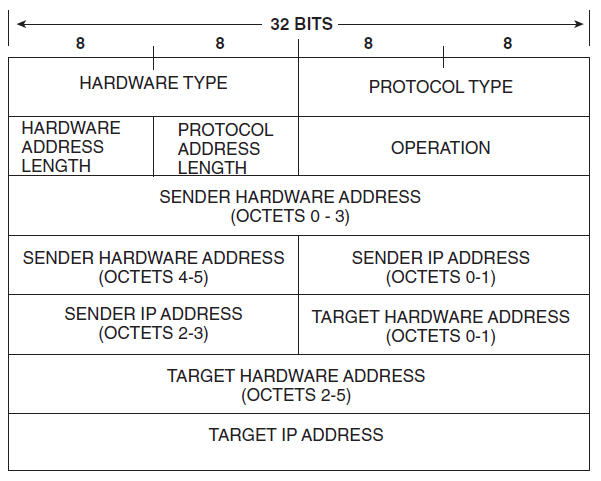


Рисунок 1.1 – Структура полей протокола ARP

Протокол ARP имеет поля:

* Hardware Type - 16-битное поле, определяющее “тип канальной среды”;
* Protocol Type - 16-битное поле, определяющее протокол сетевого уровня, который отправитель связывает с идентификатором канала передачи данных. Для протокола IP версии 4 значение данного поля равно 0x0800
* Hardware Address Length - 8-битное поле, определяющее длину идентификатора канальной среды в байтах. MAC-адреса имеет длину 48 бит или 6 байт.
* Protocol Address Length - 8-битное поле, определяющее длину адреса сетевого уровня в байтах. IP-адреса имеет длину 32 бита или 4 байта.
* Operation - 16-битное поле, которое определяет какой тип пакета ARP используется
  + ARP Request - 1
  + ARP Reply - 2
  + Reverse ARP Request - 3
  + Reverse ARP Reply - 4
  + Inverse ARP Request - 8
  + Inverse ARP Reply - 9
* Последние 20 байт приходятся на адресацию канальной среды и сетевого уровня источника и назначения запроса (MAC-адрес 6 байт \* 2 + IP-адрес 4 байт \* 2 = 20)

Базовый алгоритм работы ARP [3]:

* Запрос ARP (ARP Request): когда устройство хочет отправить пакет другому устройству в той же локальной сети, оно сначала проверяет свою ARP-таблицу, чтобы узнать, связан ли IP-адрес получателя с MAC-адресом. Если соответствующего MAC-адреса в таблице нет, устройство создает запрос ARP, указывая IP-адрес, для которого требуется MAC-адрес. Запрос ARP передается в широковещательном режиме (broadcast) по всей сети, потому что изначально устройство не знает MAC-адреса получателя. MAC-адрес источника указывается в запросе.
* Ответ ARP (ARP Reply): устройство, которое распознает свой IP-адрес в запросе, отвечает ARP-ответом (ARP Reply), в котором указывает свой MAC-адрес. Этот ответ отправляется непосредственно (unicast) на устройство, запросившее ARP. Кроме того, устройство, получившее запрос ARP, может добавить или обновить запись в своей ARP-таблице, связывая MAC-адрес с IP-адресом источника запроса.
* Использование ARP-таблицы: когда ARP-кэш содержит нужную связь между IP-адресом и MAC-адресом, устройство использует эту информацию для отправки пакетов данных по сети. Таблица имеет ограниченное время жизни, после которого записи удаляются, чтобы избежать устаревших данных. Если запись удалена, процесс начинается заново.

**1.2 Постановка задачи**

В рамках курсовой работы необходимо:

* исследовать существующую атаку ARP Spoofing. Провести анализ ее воздействия на работу сети и потенциальные последствия;
* разработать тестовую реализацию атаки. Создать программу, имитирующую атаку ARP Spoofing в контролируемой среде;
* создать локальную сеть, которая позволит безопасно провести тестирование созданной атаки.

**2 Анализ данных**

Для возможности проведения исследования атаки ARP Spoofing, курсовая работа должна включать в себя немало аспектов входных данных.

Требуются знания о протоколе ARP и структуре его пакетов, о типах и кодах этого протокола. Нужно обладание достаточными знаниями и пониманием основных принципов построения локальных сетей, включая сетевую архитектуру, IP-адресацию, маршрутизацию и настройку сетевых устройств.

Реализация программной части атаки будет создана на языке программирования Python с библиотекой Scapy, являющейся мощным инструментом для работы с сетью и проведения исследований в области информационной безопасности. Но т.к. данная библиотека ставит некоторые ограничения на генерацию сетевых пакетов, сам код библиотеки тоже должны быть немного изменен.

С помощью виртуализатора VMware должна быть создана локальная сеть, которая включает виртуальные машины Windows – жертву и хакера.

**3 Программная реализация**

Для тестирования атаки, компьютеры жертвы и хакера были размещены в одной локальной сети.

Для выбора жертвы был написан модуль network\_scanner.py (рисунок 3.1), который при вызове принимает такие аргументы как ip-адрес и маску. С помощью библиотеки scapy отправляется ARP Request на широковещательный адрес. Существующие в локальной сети устройства отвечают на каком MAC-адресе они находятся. После этого выводятся их ip-адреса и их mac-адреса. Из этого списка можно выбрать жертву.

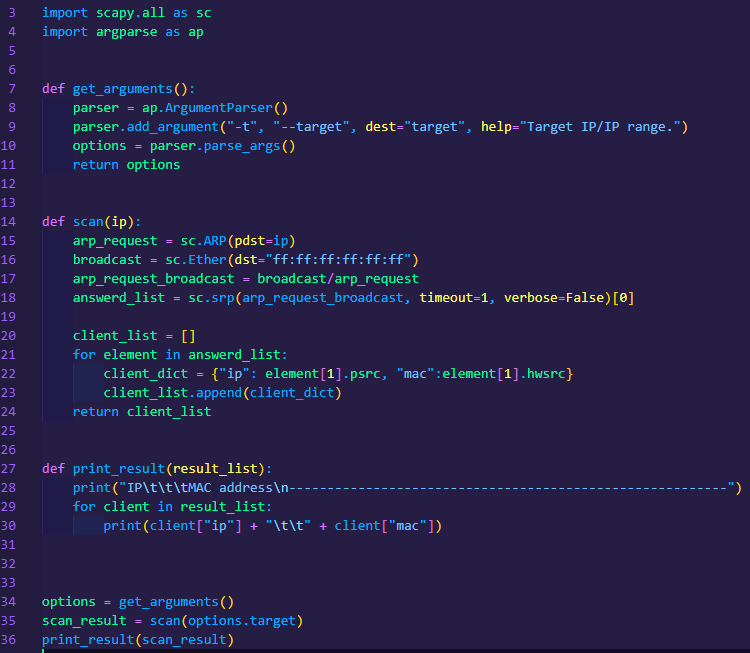


Рисунок 3.1 – Модуль network\_scanner.py

Для реализации атаки был написан модуль arp\_spoofing.py (рисунок 3.2). Сначала находится MAC-адрес жертвы и шлюза. Далее на IP-адрес жертвы отправляется ARP Reply пакет, в котором хакер приписывает шлюзу свой MAC-адрес (рисунок 3.3), и на IP-адрес шлюза отправляется ARP Reply пакет, в котором хакер приписывает жертве свой MAC-адрес (рисунок 3.4). Теперь пакеты от жертвы, отправляемые на роутер, идут через компьютер хакера. Также пакеты от роутера, отправляемые жертве, идут через хакера. Таким образом хакер может просматривать, изменять и уничтожать проходящие через него пакеты. ARP Reply пакеты отправляются каждые 2 секунды.

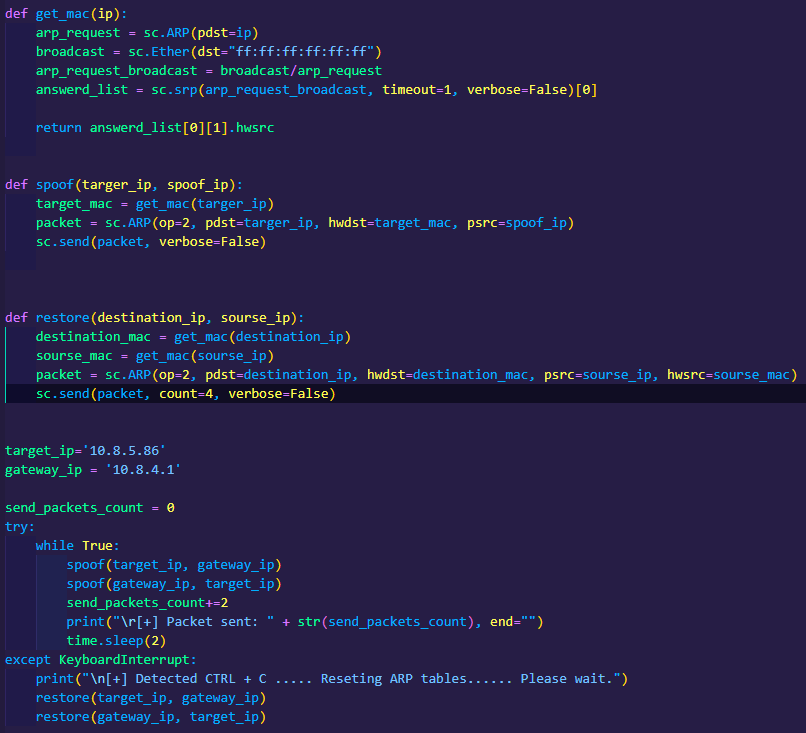


Рисунок 3.2 – Модуль network\_scanner.py

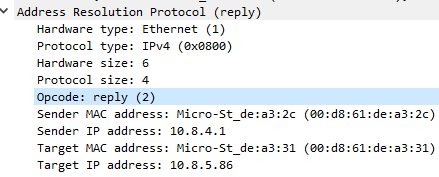


Рисунок 3.3 – ARP reply обманывающий жертву

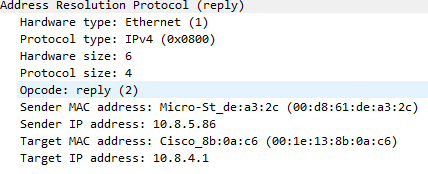


Рисунок 3.4 – ARP reply обманывающий шлюз

После остановки программы отправляются ARP Reply с правильными MAC-адресами жертвы и шлюза.

На рисунке 3.5 представлена ARP таблица жертвы до атаки, белым выделен MAC-адрес шлюза, синим подчеркнуты адреса хакера.

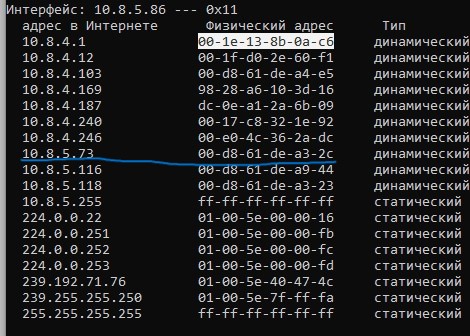


Рисунок 3.5 – ARP таблица до атаки

На рисунке 3.6 представлена ARP таблица жертвы во время атаки, белым выделен MAC-адрес шлюза, синим подчеркнуты адреса хакера. MAC-адреса шлюза и хакера идентичны, значит пакеты, предназначенные для роутера, уходят на компьютер злоумышленника..

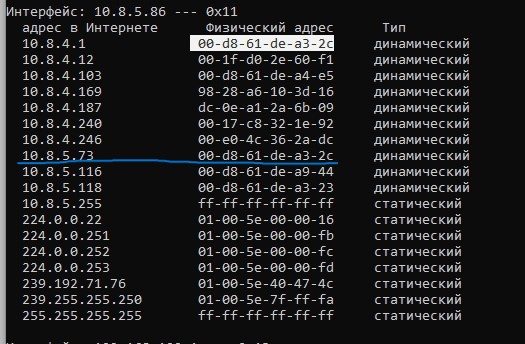


Рисунок 3.6 – ARP таблица во время атаки

После завершения атаки вернулись правильные MAC адреса. Это можно увидеть на рисунке 3.7.

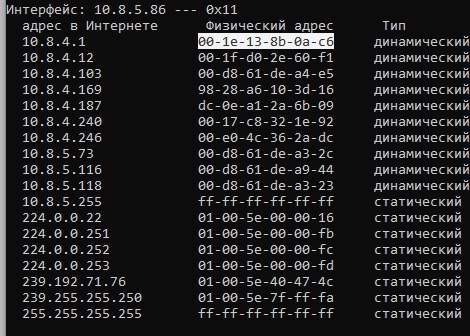


Рисунок 3.1 – ARP таблица после атаки

**4 Руководство пользователя**

Для совершения атаки нужно запустить файл network\_scanner.py дописав аргументы, а именно сеть, адреса которой необходимо узнать (рисунок 4.1).



Рисунок 3.1 – Запуск команды

После выбора жертвы необходимо изменить файл arp\_spoofing.py, вписав IP-адреса жертвы и шлюза (рисунок 3.2)



Рисунок 3.1 – Изменение адресов

Далее необходимо запустить файл arp\_spoofing.py и атака начнется. После остановки программы MAC-адреса восстановятся.

**5 Анализ полученных результатов**

Для реализации ARP Spoofing атаки были разработаны модули, которые были успешно протестированы.

Данная уязвимость может позволяет злоумышленнику пропускать через себя весь трафик жертвы, что за собой ведет риски кражи личных данных.

Тестирование показало, что MAC-адреса в ARP таблицы без проблем меняются после отправки отравленного ARP Reply.

ЗАКЛЮЧЕНИЕ

В рамках данного проекта была проведена успешная атака типа ARP Spoofing, что позволило продемонстрировать уязвимость сетевых устройств к этой форме атаки. Результаты эксперимента подтвердили, что с помощью ARP Spoofing злоумышленник может перехватывать сетевой трафик, изменять его или перенаправлять, создавая серьезные риски для конфиденциальности и целостности данных.

На основе проведенного эксперимента рекомендуется:

* Внедрить средства обнаружения и предотвращения атак ARP Spoofing.
* Использовать шифрование для защиты конфиденциального трафика.
* Проводить регулярное обучение сотрудников по вопросам информационной безопасности, уделяя особое внимание уязвимостям сетевых протоколов.

Таким образом, эксперимент подтвердил важность осведомленности о рисках, связанных с ARP Spoofing, и необходимости принятия соответствующих мер для обеспечения безопасности сетей.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Что такое ARP? Объясняем на пальцах – Текст: электронный // DevRockets — boosting IT perfomance. – 2021. – URL: <https://devrockets.ru/2021/05/23/arp-zapisi-tablicy-maki-dlya-chajnikov/> (дата обращения: 06.03.2023).
2. ARP Spoofing | Отравление ARP. – Текст: электронный // Хабр. – 2023. – URL: <https://habr.com/ru/articles/786038/> (дата обращения: 06.03.2023).
3. Address resolution protocol - что это? – Текст: электронный // MERION. – 2018. – URL: <https://wiki.merionet.ru/articles/address-resolution-protocol-chto-eto> (дата обращения: 06.03.2023).