МОДЕЛЬ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ ARP-ПРОТОКОЛА

Самаке Б.А., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.А. – канд. техн. наук

Аннотация. В данной статье рассматривается уязвимость протокола ARP с помощью атаки ARP spoofing в модели сети, спроектированной в программном эмуляторе GNS3.

Ключевые слова. ARP, ARP-spoofing, MAC-адрес, IP-адрес, локальная сеть, уязвимость.

В данной работе рассмотрена уязвимость протокола ARP (Address Resolution Protocol), который используется для идентификации MAC-адреса устройства по его IP-адресу, а также для формирования таблиц MAC-адресов на коммутаторах и ARP-таблиц на оконечных устройствах в сети. Уязвимость данного протокола заключается в попытке перехвата широковещательной рассылки ARP-пакетов, в которых есть IP и MAC-адреса устройств в сети. Таким образом, нарушитель может получить данные об устройствах в сети и реализовать атаку ARP spoofing [1].

Рассмотрим сценарий атаки, во первых необходимо провести сбор данных для получение информации (например, IP-адреса пользователя), с помощью анализатора трафика, после чего нарушитель реализует IP-адреса на своем устройстве и добавит его в таблицу MAC адресов коммутаторов. Таким образом, нарушитель сможет подключиться к сети в качестве авторизованного пользователя.

Для проверки уязвимости ARP-протокола необходимо было смоделировать локальную сеть. Для этого был произведен сравнительный анализ несколько средств моделирования такие как Cisco Packet Tracer и GNS3. Обе прогаммы эмулируют реальные сетевые устройства, различные оконечные и промежуточные устройства. Разница между рассмотренными средствами моделирования заключается в том что, Cisco Packet Tracer эмулирует устройства внутри программы, из-за чего выбор устройства ограничен несколькими сериями маршрутизаторов и коммутаторов компании Cisco. GNS3 основан на Qemu и Dynamips и является графическим интерфейсом для создания локальных сетей с использованием Qemu. В GNS3 устройства разных производителей можно добавлять самостоятельно. Также GNS3 предоставляет более точную представление в настройки оборудований [2].

На рисунке 1 представлена модель локальной сети в программном эмуляторе сети GNS3. В смоделированной сети выделено четыре виртуальные сети (VLAN), для каждой из которых настроен DHCP сервер.

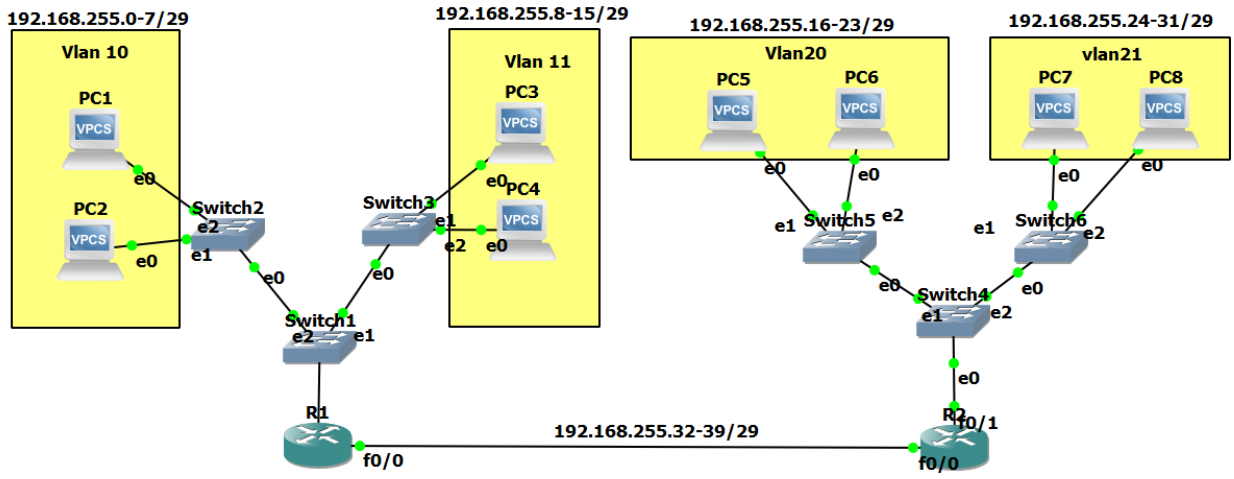

Рисунок 1 – Модель локальной сети для моделирования атаки

На рисунке 2 представлена возможность перехвата нарушителем ARP-пакета во время получение адреса с DHCP-сервера, что можно реализовать посредством использования программного сниффера Wireshark. Как видно из рисунка 2 при перехвате данного пакета нарушитель может получить информацию об адресах устройств в сети, а также информацию о номерах VLAN.

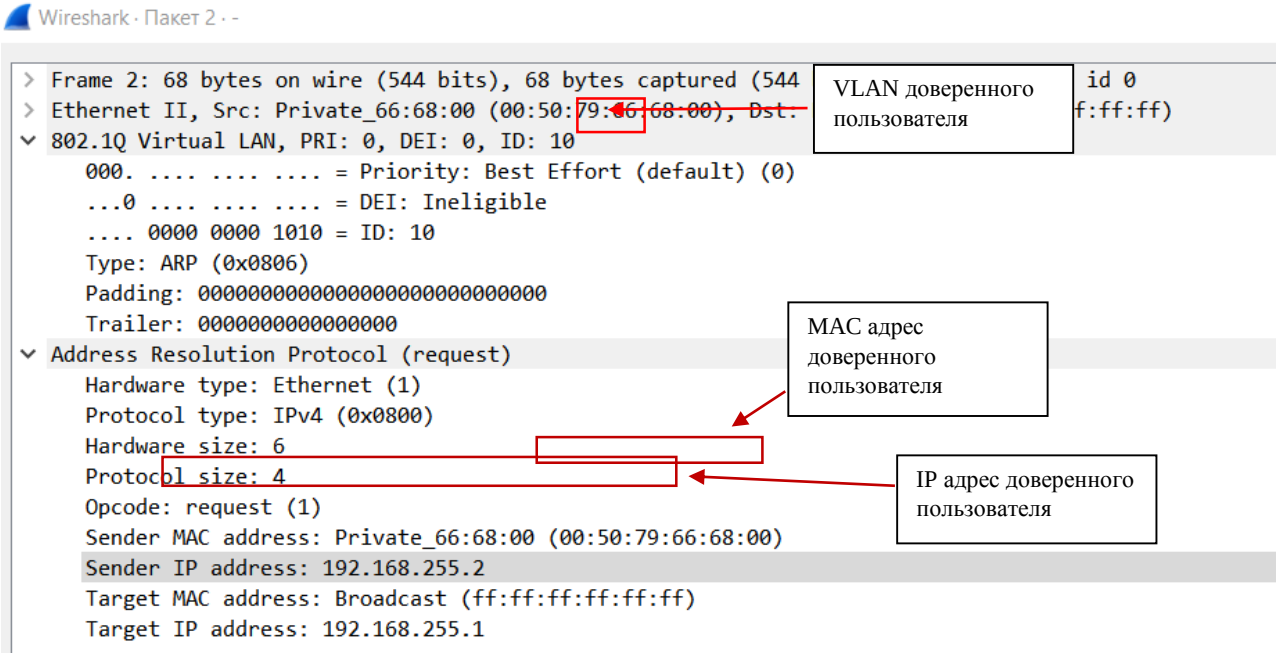

Рисунок 2 – Результат перехвата ARP-рассылки в смоделированной локальной сети

Далее нарушитель может произвести подмену записей в таблицах ARP других устройств в сети путем изменения на своем устройстве IP-адреса на адрес 192.168.255.2, полученный в перехваченном ARP-пакете. Для внесения неверной записи в таблицы ARP устройств в сети, нарушитель производит отправку ICMP пакетов, реализуя команду ping 192.168.255.26. Как видно из рисунка 3 MAC-адрес пользователя изменился на адрес нарушителя без изменение IP-адреса.

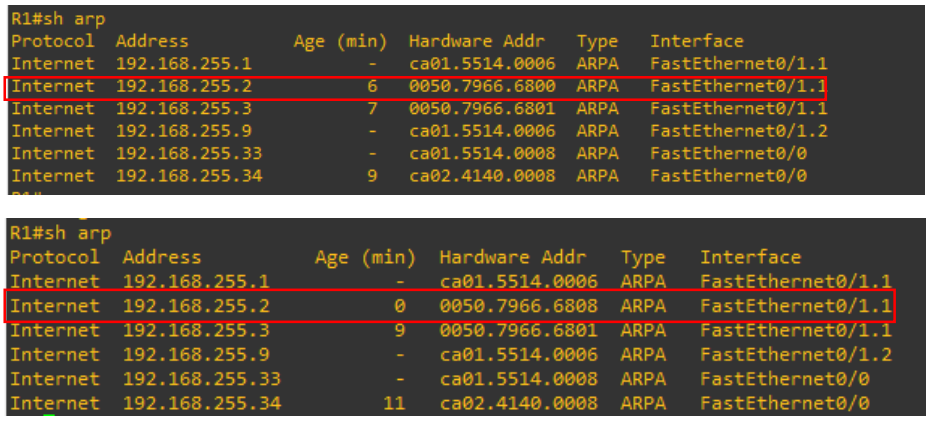

Рисунок 3 – Результат подмены записей в таблице ARP таблицах маршрутизатора до и после реализации атаки ARP-spoofing

После подмены нарушитель сможет перехватывать трафик предназначены для доверенного пользователя. На рисунке 4 видно, что замена записей в таблице ARP привела к возможности нарушителем получать все пакеты в сети.

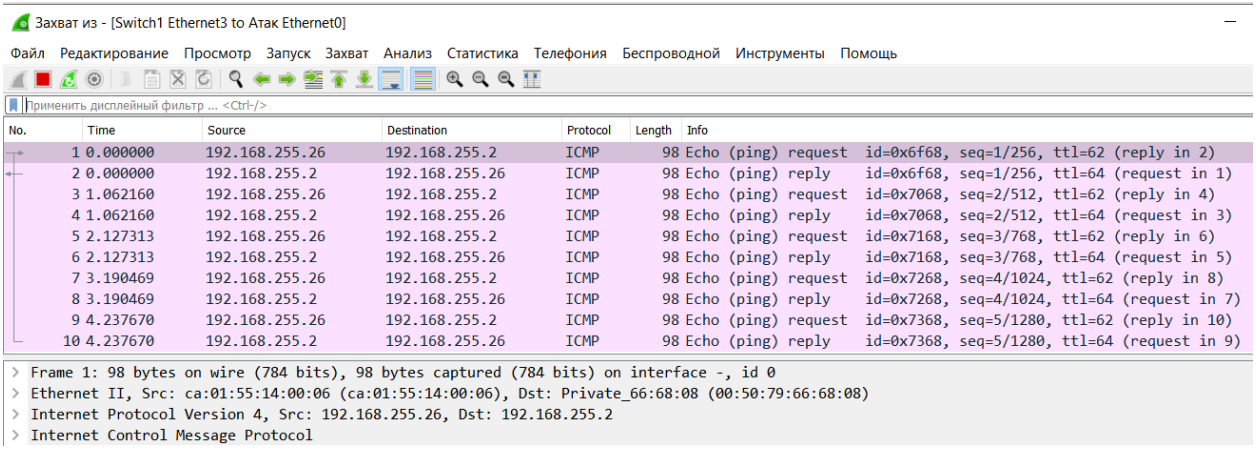

Рисунок 4 – Результат перенаправления пакетов в локальной сети

Таким образом, в работе смоделирована атака ARP-spoofing, проанализированы действия нарушителя и продемонстрированы последствия атаки. В продолжении данной работы планируется разработать комплекс мер по защите устройств локальной сети от атаки ARP-spoofing.

Список использованных источников:

1. Что такое ARP-спуфинг и как от него защититься – режим доступа: Что такое ARP-спуфинг и как от него защититься? (securitylab.ru). – Дата доступа: 25.03.2023.

2. Кулябов Д. С. Средства моделирования сетей для целей обучения– режим доступа: Средства моделирования сетей для целей обучения | Д. С. Кулябов (yamadharma.github.io). – Дата доступа: 25.03.2023.