УДК 069.271.2 – 021.131:044.056.5

МАКЕТ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ PNETLAB ДЛЯ ИЗУЧЕНИЯ КИБЕРАТАКИ ARP-SPOOFING

Иванов А.П., Кисель А.В.

гр.161402

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С. – доцент кафедры ЗИ, кандидат технических наук, доцент.

Аннотация. В материалах доклада представлены результаты анализа уязвимости ARP-протокола и реализация кибератаки ARP-spoofing в смоделированной локальной сети в виртуальной лаборатории PnetLAB. Предлагается разработанный макет виртуальной лаборатории использовать для развития знаний и навыков у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

Ключевые слова: сетевые кибератаки, ARP-spoofing, PnetLab

Введение. ARP (Address Resolution Protocol) был разработан Лораном Джонсоном в начале 1980-х годов с целью решения проблемы сопоставления IP-адресов узлов с их физическими MAC-адресами в компьютерных сетях. Протокол был впервые определен в RFC 826 в 1982 году. Он стал ключевым элементом современных компьютерных сетей, обеспечивая эффективную коммуникацию и обмен данными между устройствами в локальных сетях.

Актуальность проблемы сетевых атак, таких как ARP-spoofing, становится все более критичной в условиях большого использования локальных сетей в различных сферах жизни. ARP-spoofing это кибератака, основанная на влиянии на передачу ARP-кадров. В ходе кибератаки нарушитель сканирует сеть и подменяет MAC-адреса. Это позволяет ему подделывать и перенаправлять сетевой трафик, что приводит к серьезным последствиям, таким как перехват информации, ее подмена или нарушение нормального функционирования сети.

Цель данной научной работы заключается в разработке эффективных методов защиты от кибератак на основе изучения сценариев ARP-spoofing. Результаты этого

исследования могут стать основой для разработки политик безопасности и обеспечить устойчивость к подобным угрозам в локальных сетях.

Основная часть. Для изучения принципов передачи ARP-кадров и уязвимостей ARP-протокола была создана локальная сеть в виртуальной лаборатории PnetLab, которая предоставляет возможности проектирования локальных сетей на базе устройств различных производителей в режиме реального времени.

Построенная виртуальная лаборатория в PnetLab приведена на рисунке 1. В нее входит следующее оборудование:

– шлюз подключения к внешней сети (Network);
– маршрутизатор Cisco c7200 (Router);
– коммутатор Cisco IOS L2 (Switch);
– компьютер нарушителя с ОС Linux (Ubuntu);
– компьютер жертвы с ОС Linux (Ubuntu_victim);
– компьютер с ограниченной ОС (VPC).

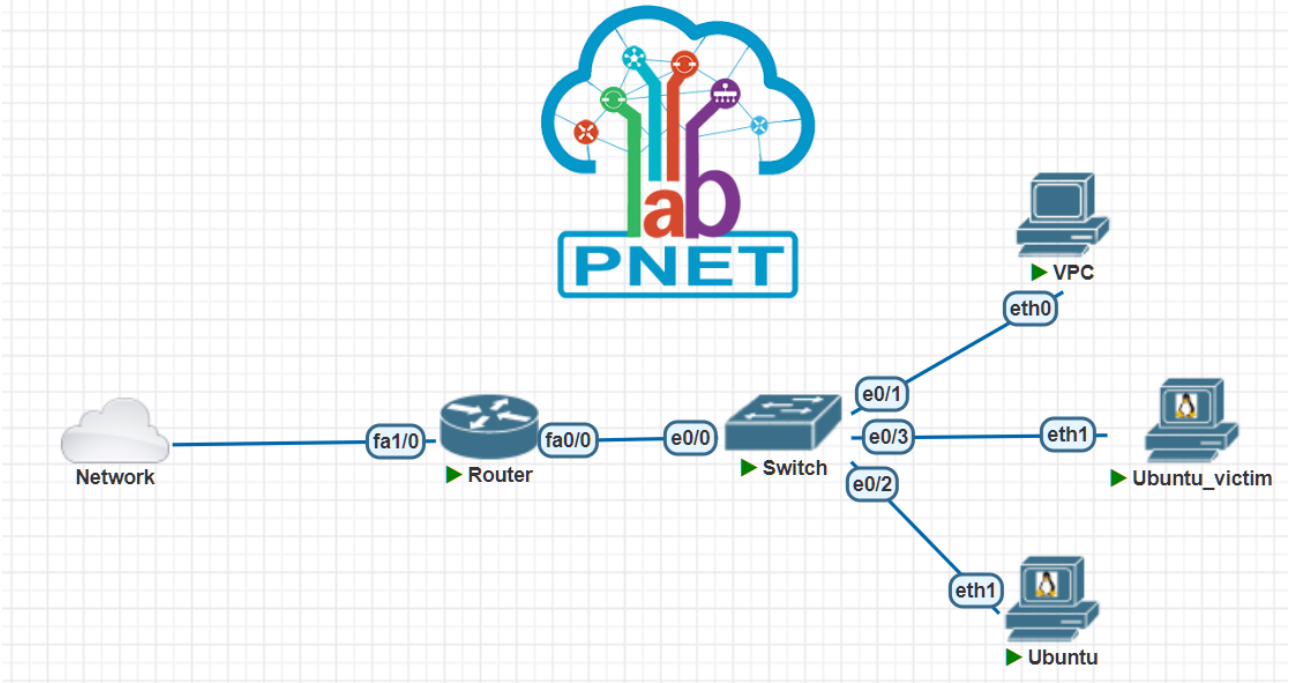

Рисунок 1 – Топология локальной сети в виртуальной лаборатории PnetLab

На основе изучения принципа передачи ARP-кадров были выявлены несколько уязвимостей. В связи с тем, что ARP-запрос содержит широковещательный MAC-адрес, то такой ARP-кадр может получить любое устройство в широковещательном сегменте. Поэтому возникает один из вариантов кибератаки – постоянная отправка ARP-кадров с модифицированным MAC-адресом. Устройство Ubuntu_victim получает ARP-ответ от устройства нарушителя. Далее происходит перенаправление трафика на устройство нарушителя. Второй вариант атаки – реализация кибератаки «человек-посередине» с помощью подмены MAC-адреса порта маршрутизатора на MAC-адрес устройства-нарушителя в таблице ARP Ubuntu_victim. Было принято решение изучения второго варианта реализации кибератаки ARP-spoofing.

В топологии топология локальной сети в виртуальной лаборатории PnetLab (рисунок 1) устройство Ubuntu_victim (MAC-адрес 50:00:00:24:00:01) получило по DHCP IP-адрес 192.168.50.4/24, а устройство Ubuntu (MAC-адрес 50:00:00:37:00:01) – 192.168.50.2/24.

Далее на устройстве Ubuntu был установлен инструмент arp-scan для обнаружения IP- и MAC-адреса всех устройств в локальной сети с помощью команды:

admin@Ubuntu:~$ sudo apt install arp-scan –interface=eth1 --localnet

В результате нарушитель получает информацию о MAC- и IP-адресах всех устройств. Располагая полученной информацией, нарушитель реализует кибератаку ARP-spoofing с помощью команды:

root@Ubuntu:/home/admin# arpspoof -i eth0 -t 192.168.50.4 192.168.50.1

На рисунке 2 представлена ARP-таблица на устройстве Ubuntu_victim до и после реализации команды arpspoof.

а б

Рисунок 2 – Содержимое ARP-таблицы на устройстве Ubuntu_victim до (а) и после (б) реализации кибератаки ARP-spoofing

Таким образом, можно сделать вывод, что была проведена успешная замена MAC-адреса маршрутизатора на физический адрес устройства нарушителя. Для проверки перенаправления трафика использовалась программа Wireshark (рисунок 3).

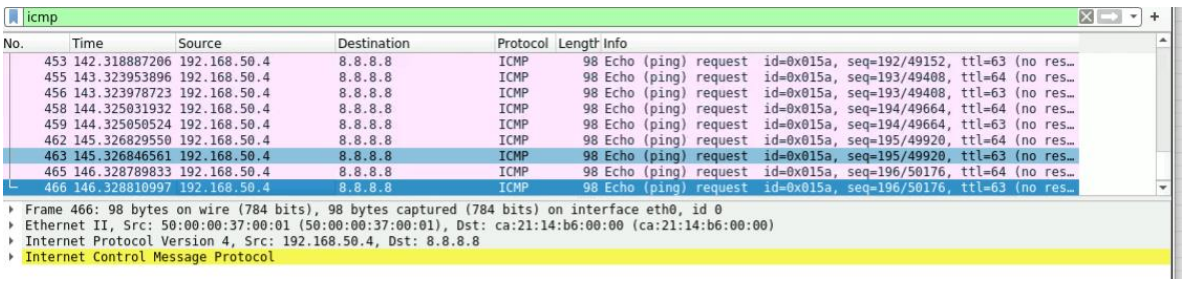

Рисунок 3 – Анализ трафика Wireshark

На рисунке 3 видно, что трафик, идущий от устройства Ubuntu_victim (IP-адрес 192.168.50.4/24) перенаправлен на устройство с MAC-адресом 50:00:00:37:00:01, что соответствует устройству нарушителя Ubuntu.

На основе полученных результатов, можно сделать вывод о том, что несмотря на актуальность и значимость протокола ARP в современных локальных сетях он легко может быть использован для реализации кибератак и перенаправления трафика. Поэтому следует использовать необходимые средства защиты на сетевом оборудовании.

Возможны несколько вариантов защиты от атаки ARP-spoofing:

1. Статические ARP-таблицы.
2. Защита коммутатора. Большинство управляемых коммутаторов оснащены функциями предотвращения кибератак ARP Poisoning, динамической проверки ARP (Dynamic ARP Inspection, DAI).

Заключение. На основе проведенных исследований предлагается реализовать макет виртуальной лаборатории на основе платформы PnetLab для изучения уязвимостей ARP-протокола, реализации кибератаки ARP-spoofing, конфигурации функций предотвращения кибератак. Такой макет позволит развивать знания и навыки у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

Список литературы

7. Бабин С. А. Инструментарий хакера. / Бабин С. А. – Санкт-Петербург, 2014. – 240 с.

8. Отравление ARP: что это такое и как предотвратить ARP-спуфинг [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/varonis/articles/562144/. – Дата доступа: 02.02.2024.

UDC 069.271.2 – 021.131:044.056.5

THE LAYOUT OF THE NETLAB VIRTUAL LABORATORY TO STUDY THE ARP-SPOOFING CYBERATTACK

Ivanov A.P., Kisel A.V.

gr.161402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department

Annotation. The report presents the results of an analysis of the vulnerability of the ARP protocol and the implementation of the ARP-spoofing cyberattack in a simulated LAN in the virtual laboratory PnetLAB. It is proposed to use the developed layout of the virtual laboratory to develop knowledge and skills among students of various specialties, including 1-98 01 02 "Information security in telecommunications".

Keywords: network attacks, ARP-spoofing, PnetLab.