УДК 004.773:004.056.5

ПЕРЕНАПРАВЛЕНИЕ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ MITM

Т.Б. Русецкая

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В материалах доклада представлены результаты анализа уязвимости ICMP протокола и реализация кибератаки ICMP Redirect в среде виртуализации VirtualBox. Кибератака проведена на виртуальном макете, состоящем из устройств нарушителя, целевого устройства, маршрутизатора и клиентской машины. Исследование включает в себя описание методов эксплуатации уязвимости протокола ICMP, а также последствия кибератаки для безопасности сети. В результате анализа были выявлены основные факторы, способствующие успешному проведению кибератаки, а также предложены рекомендации для повышения уровня защиты информационной системы и минимизации рисков. Полученные данные могут быть полезны для специалистов в области защиты информации и разработки эффективных мер по предотвращению подобных угроз, а также для улучшения безопасности сетевых коммуникаций.

Ключевые слова: MITM; ICMP протокол; ICMP Redirect; сетевые кибератаки; сетевой трафик; VirtualBox; анализ уязвимости; Wireshark; IP-адрес; сетевая инфраструктура.

REDIRECT OF NETWORK TRAFFIC USING MITM ATTACK

T.B. Rusetskaya

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The report presents the findings of an investigation into the vulnerabilities of the ICMP protocol and the ICMP Redirect attack within the VirtualBox virtualization environment. The cyberattack was conducted on a virtual mockup comprising the intruder's devices, the target device, the router and the client machine. The study provides a comprehensive overview of the methods employed to exploit the vulnerabilities of the ICMP protocol, in addition to the repercussions of the attack on network security. The analysis yielded key factors contributing to the success of the attack, and recommendations for enhancing the protection of information systems and mitigating risks were proposed. The findings from this study are likely to be of value to information security specialists in the fields of information protection and the development of effective measures to prevent such threats, as well as to improve the security of network communications.

Keywords: MITM-attack; ICMP protocol; ICMP Redirect; network attacks; network traffic; VirtualBox; vulnerability analysis; Wireshark; IP-address; network infrastructure.

Введение

MITM (man in the middle) – это атака, при которой нарушитель получает доступ к каналу связи между легитимными сторонами (пользователями, приложениями, сетевыми устройствами), что позволяет ему просматривать содержимое всех передаваемых ими сообщений, удалять и изменять их.

ICMP (Internet Control Message Protocol) – это протокол, предназначенный для отправки сообщений об ошибках и передачи служебной информации, которая указывает на успех или неудачу при обмене данными с другим IP-адресом. Обычно ICMP не используется для передачи данных между устройствами, а применяется для проверки связи между двумя узлами с помощью программ, таких как ping или traceroute.

Актуальность проблемы сетевой кибератаки ICMP Redirect сохраняется на сегодняшний момент. ICMP Redirect – это кибератака, основанная на уязвимости передачи ICMP-пакетов. В ходе ее проведения нарушитель использует поддельные ICMP-сообщения для управления маршрутизацией сетевого трафика. Сначала атакующий сканирует сеть, определяет целевое устройство, перехватывает трафик сети, отправляет ICMP Redirect сообщения целевому устройству, перенаправляет трафик через свой узел, анализирует и завершает атаку, восстанавливая нормальную маршрутизацию трафика.

Формат ICMP Redirect сообщения состоит из следующих полей (рис. 1):

– Тип (5);

– Код (0 – перенаправление пакетов для сети, 1 – перенаправление пакетов для узла, 2 – перенаправление пакетов в зависимости от типа службы и сети, 3 – перенаправление пакетов в зависимости от типа службы и узла);

– Контрольная сумма;

– IP-адрес шлюза (адрес шлюза, на который направляется трафик для сети, указанной в поле «Internet destination network»);

– Заголовок IP + 64 бита данных.

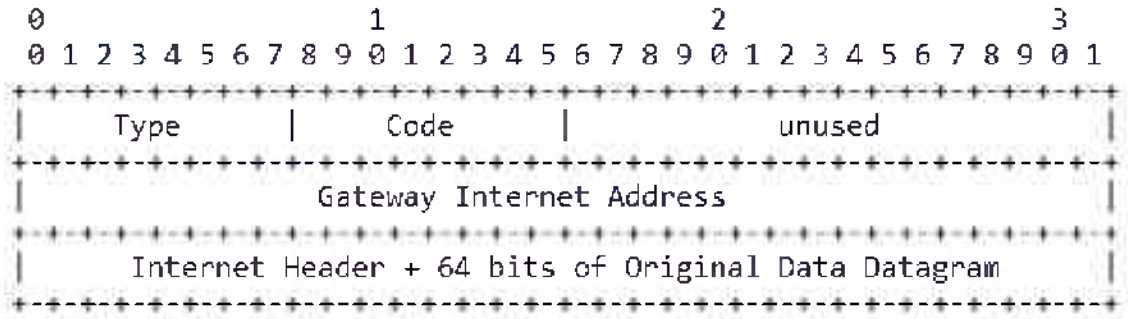

Рис. 1. Формат ICMP Redirect сообщения
Fig.1. Format of ICMP Redirect message

Цель данной работы заключается в рассмотрении проведения кибератаки с использованием ICMP Redirect и анализа перехваченного трафика.

Основная часть

Для проведения MITM кибератаки с использованием ICMP Redirect была использована платформа виртуализации VirtualBox. Создана локальная сеть из 4 виртуальных машин:

– компьютер нарушителя с ОС Kali Linux (attacker);

– компьютер «жертвы» с ОС Ubuntu (victim);
– клиентская машина с ОС Ubuntu (server);
– маршрутизатор Mikrotik (router_mikrotik).

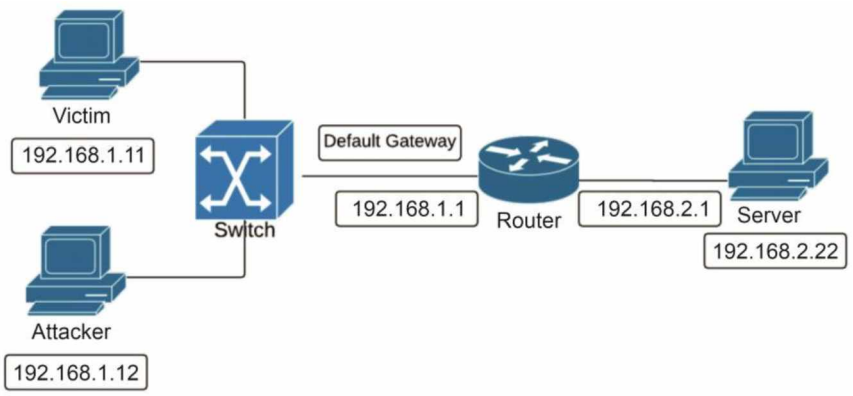

Рис. 2. Топология сети
Fig.2. Network topology

При изучении принципа передачи ICMP пакетов были выявлены несколько уязвимостей. Одной из функций протокола ICMP является управление таблицами маршрутизации на узлах внутри сегмента сети. Сообщения ICMP могут содержать информацию о перенаправлении. Такие сообщения позволяют оптимизировать маршрутизацию пакетов через более эффективные маршруты.

Атака ICMP Redirect заключается в том, что нарушитель отправляет поддельное сообщение ICMP Redirect целевому узлу, указывая предпочтительный маршрут для передачи данных. Цель данной кибератаки – изменить таблицу маршрутизации на целевом узле, чтобы перенаправить трафик через узел нарушителя.

На рисунке 2 показана топология сети в среде виртуализации VirtualBox. Из топологии видно, что виртуальная машина «жертвы» имеет IP-адрес 192.168.1.11/24, нарушитель – 192.168.1.12/24, на интерфейсах маршрутизатора настроены 192.168.1.1/24 и 192.168.2.1/24, на клиентской машине – 192.168.2.22/24.

Далее на устройстве нарушителя происходит сканирование сети с помощью инструмента nmap для обнаружения узлов в сети (рис. 3):

```
/home/kali
nmap -sP 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-20 10:56 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
 specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
MAC Address: 08:00:27:15:3B:3A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.11
Host is up (0.00043s latency).
MAC Address: 08:00:27:68:77:1B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.12
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.96 seconds
```

Рис. 3. Запуск сканирования сети с помощью nmap
Fig.3. Network scan launch using nmap

На рисунке 3 можно заметитить, что в сети 192.168.1.0/24 существует 3 IP-адреса. IP-адрес 192.168.1.11/24 – это адрес целевого устройства.

После этого в Wireshark осуществляем перехват трафика по фильтру ip.add == 192.168.1.11 (рис. 4):

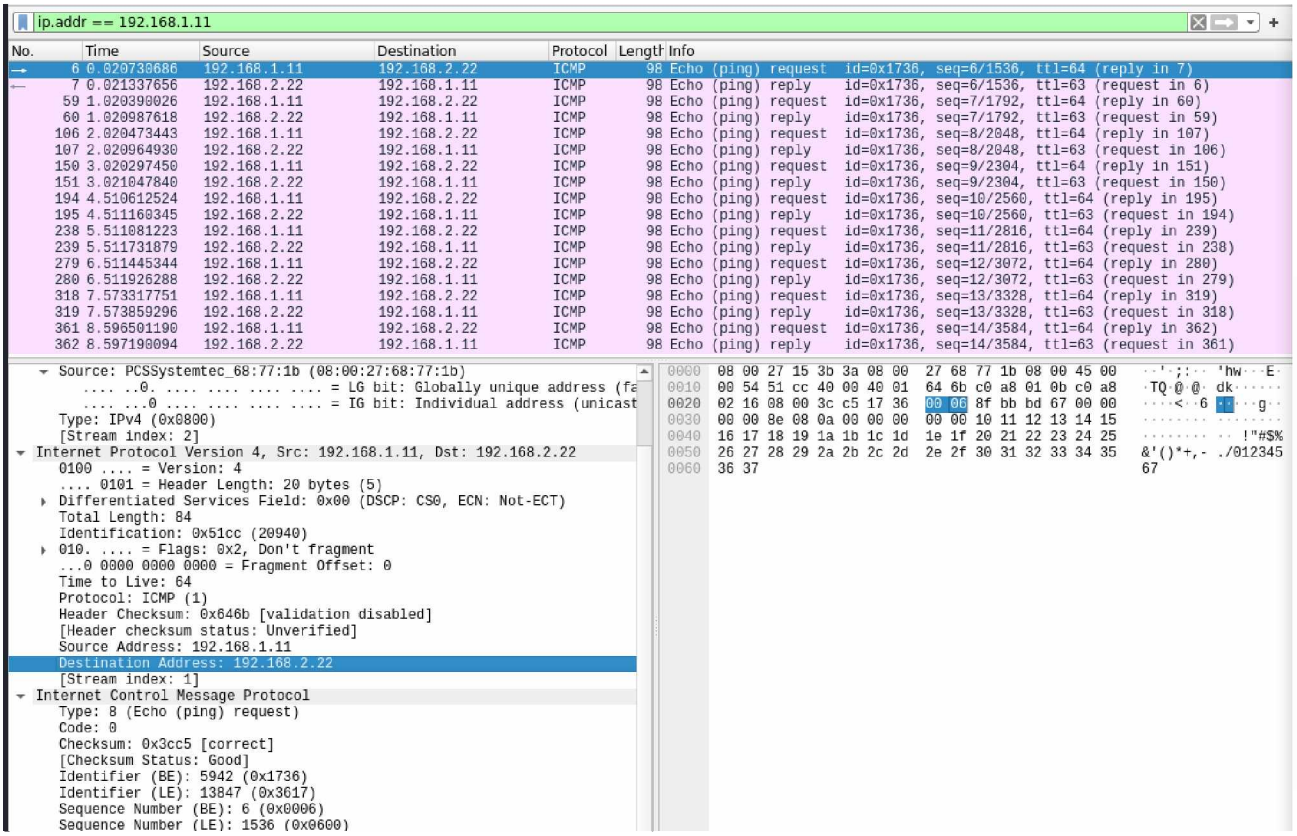

Рис. 4. Перехват сетевого трафика
Fig.4. Interception of network traffic

Из рис. 4 нарушитель получает информацию об IP-адресе клиентской машины. Располагая полученной информацией, можно реализовать кибератаку ICMP Redirect с помощью команды netwox (рис. 5).

Рис. 5. Использование инструмента netwox
Fig. 5. Using the netwox tool

С помощью утилиты netwox нарушитель создает и отправляет поддельные ICMP Redirect сообщения:

1. netwox 86 – предназначен для отправки ICMP Redirect сообщений;
2. -d “eth0” указывает интерфейс, через который будет отправляться трафик;
3. --filter "src host 192.168.1.11" – устанавливает фильтр, чтобы отправлять сообщения только для трафика, исходящего от узла с IP-адресом 192.168.1.11/24;
4. --gw 192.168.1.12 задает IP-адрес шлюза, который будет использоваться для перенаправления трафика;
5. spoofip "raw" – включает подмену IP-адресов в режиме raw, что позволяет изменять IP-адрес источника пакетов;
6. --code 0 – указывает код ICMP-сообщения, что соответствует типу эхо-ответ;
7. --src-ip 192.168.2.22 – указывает IP-адрес, который будет использоваться в качестве источника для поддельных ICMP Redirect-сообщений.

На рисунке 6 видно, что трафик, идущий от устройства victim (IP-адрес 192.168.1.11/24) перенаправлен на узел с IP-адресом 192.168.1.12/24:

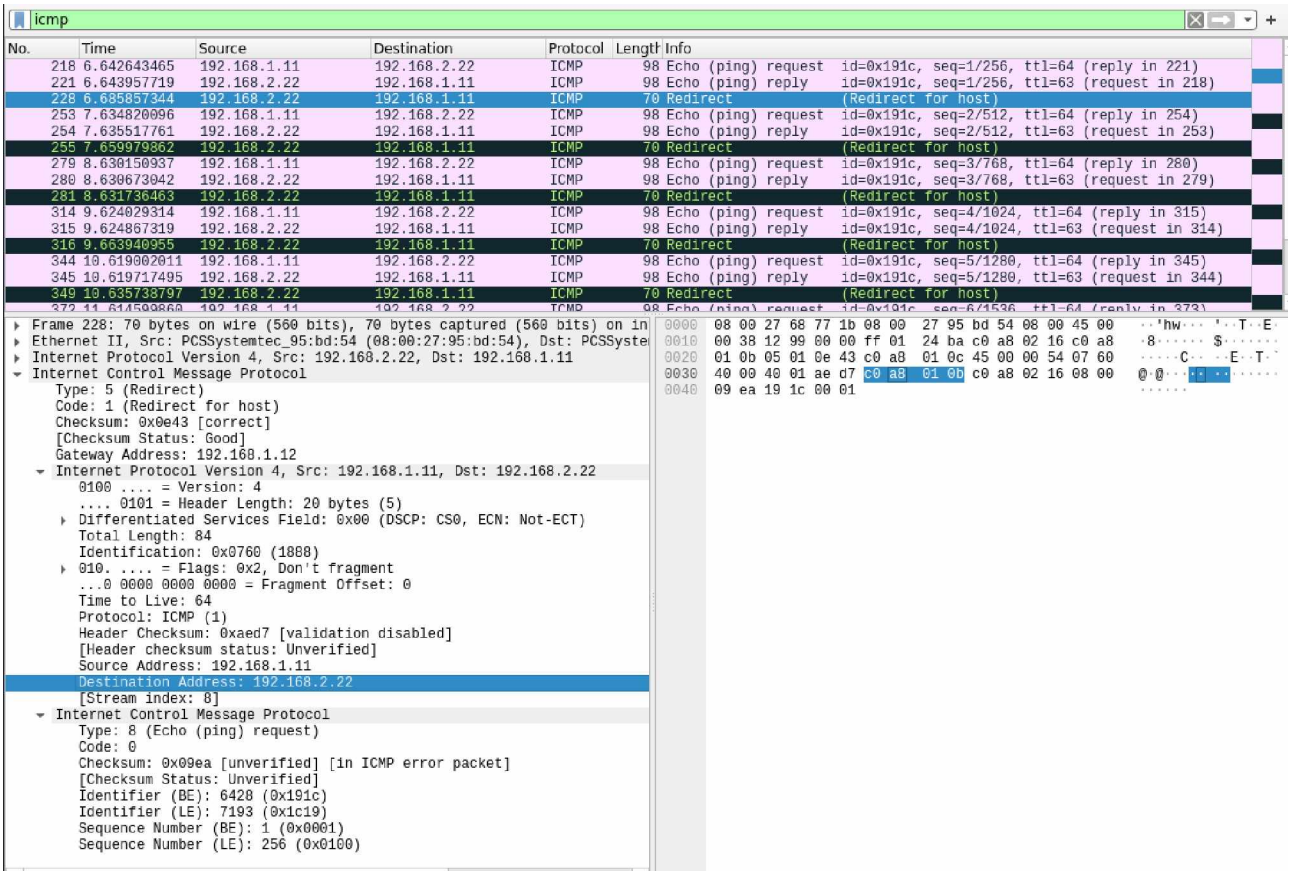

Рис. 6. Анализ трафика в Wireshark
Fig.6. Traffic analysis in Wireshark

Из рис. 6 можно заметить, что тип отправляемого сообщения является 5 или Redirect-сообщение (указывает отправителю на существование более эффективного маршрута для передачи данных).

Заключение

На основе полученных результатов можно сделать вывод что уязвимость протокола ICMP может быть использована для проведения кибератаки Man-in-the-middle, перехвата и изменения сетевого трафика, а также для создания угроз безопасности информации, которые могут привести к нарушению целостности и конфиденциальности данных в компьютерных сетях. Поэтому разработка и внедрение эффективных методов зашиты от таких атак является актуальной задачей для обеспечения устойчивости сетевых инфраструктур.

Список использованных источников

1. Ylli E., Fejzaj J. (2021) Man in the Middle: Attack and Protection. *RTA-CSIT*. 198-204
2. Arkin O. (2000). ICMP Usage in Scanning. *Black Hat Briefings*. 1–6.
3. Waichal S., Meshram B.B. (2013) Router Attacks-Detection And Defense Mechanisms. *International Journal of Scientific & Technology Research. IJSTR*. 2 (6). 1-6.
4. Feng X., Liyx Q., Sunz K., Yang Y., Xu K. (2023) Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. *IEEE Symposium on Security and Privacy (SP). IEEE*. 3162-3177.
5. Postel J. (1981). RFC0777: Internet Control Message Protocol. *RFC*. 1–6.

References

1. Ylli E., Fejzaj J. (2021) Man in the Middle: Attack and Protection. *RTA-CSIT*. 198-204

2. Arkin O. (2000). ICMP Usage in Scanning. *Black Hat Briefings*. 1–6.

3. Waichal S., Meshram B.B. (2013) Router Attacks-Detection And Defense Mechanisms. *International Journal of Scientific & Technology Research. IJSTR*. 2 (6). 1-6.

4. Feng X., Liyx Q., Sunz K., Yang Y., Xu K. (2023) Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. *IEEE Symposium on Security and Privacy (SP). IEEE*. 3162-3177.

5. Postel J. (1981). RFC0777: Internet Control Message Protocol. *RFC*. 1–6.

Сведения об авторе

Русецкая Т.Б., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». flowt10932@gmail.com.

Information about the author

Rusetskaya T., student. Educational Institution "Belarusian State University of Informatics and Radioelectronics". flowt10932@gmail.com.