АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОТ УГРОЗ IP SPOOFING С ИСПОЛЬЗОВАНИЕМ GNS3

Русецкая Т.Б.[1], студент гр.261401

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Научный руководитель: Бойправ О.В. – кандидат технических наук, заведующий кафедрой защиты информации, доцент

Аннотация. В материалах доклада представлены результаты анализа угроз IP Spoofing, проведенного с использованием симулятора GNS3. Для проведения указанного анализа был разработан виртуальный макет, состоящий из устройств нарушителя, целевого устройства и маршрутизатора. Исследование состояло из описания проведения IP Spoofing, а также последствия кибератаки для безопасности сети. В результате анализа были предложены рекомендации для повышения уровня защищенности информационных систем. Полученные результаты 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. Сетевые кибератаки, IP Spoofing, GNS3, VMware, iptables, Wireshark.

Введение. Протокол IP предназначен для обеспечения соединения хостов. Протокол обеспечивает передачу блоков данных, называемых дейтаграммами между отправителем и получателем, узлы которых идентифицируются адресами фиксированной длины. На рисунке 1 показан формат заголовка пакета IP.

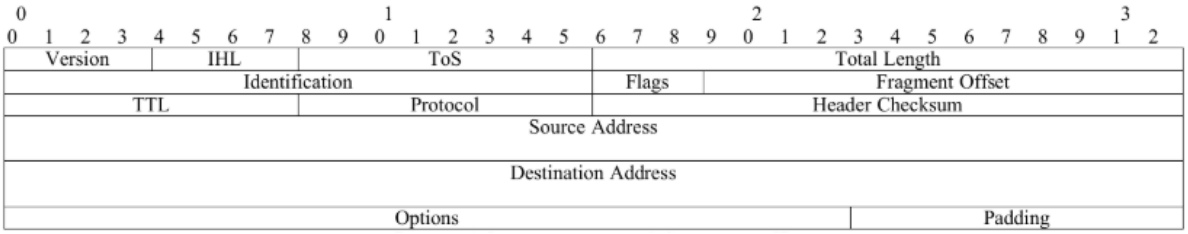

Рисунок 1 – Формат заголовка пакета IP

В полях Source Address и Destination Address указываются адреса источника и назначения.

Актуальность проблемы сетевой атаки IP Spoofing остается высокой из-за использования нарушителями для онлайн-мошенничества, кражи личных данных и нарушения работы корпоративных веб-сайтов и серверов. Также такая атака является основой других атак (DDoS, MITM и маскировка ботнет-устройств). В ходе проведения IP Spoofing адрес источника нарушителя меняется на поддельный, чтобы скрыть реальный IP-адрес и создать видимость легитимного подключения к сети.

Цель данной научной работы состояла в анализе эффективности методов защиты от угроз IP Spoofing. Практическая значимость результатов данного исследования состоит в возможности их применения в целях повышения эффективности алгоритмов фильтрации пакетов и создания современных систем предотвращения атак.

Основная часть. Для изучения принципов передачи IP-пакетов была создана локальная сеть в виртуальной лаборатории, построенной с использованием симулятора GNS3.

Схема виртуальной лаборатории, построенной в GNS3, приведена на рисунке 2. В ее состав входит следующее оборудование:

– маршрутизатор Cisco c7200;

– коммутатор (Swith1);

– компьютер нарушителя с ОС Alpine Linux (AlpineLinux);

– компьютер жертвы с ОС Alpine Linux (AlpineLinux-victim);

– компьютер с ограниченной ОС (VPCS).

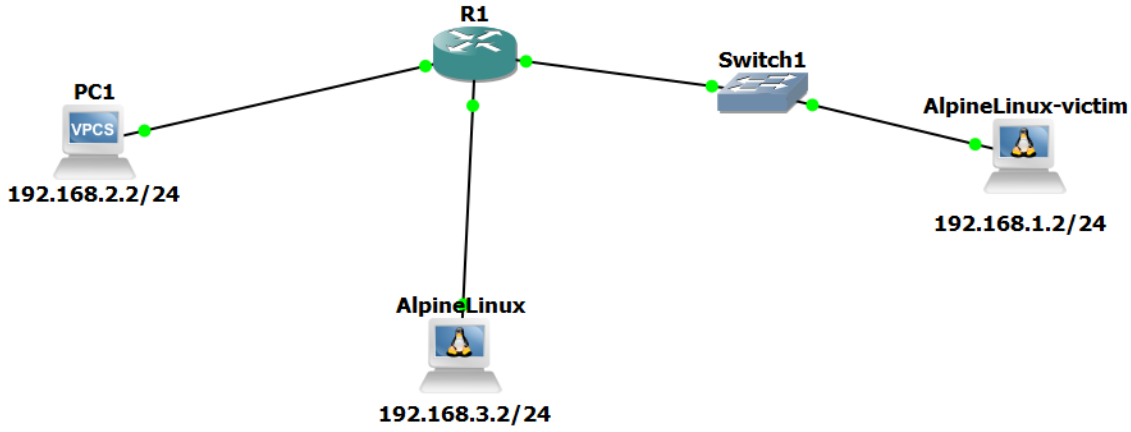

Рисунок 2 – Схема виртуальной лаборатории, построенной с использованием симулятора GNS3

В рамках исследования был рассмотрен сценарий с подменой IP-адреса и проведением DDoS-атаки на устройство с ограниченной ОС. Для проведения кибератаки необходимо изменить IP-адрес через изменение значения поля Source Address в заголовке IP-пакета. В топологии локальной сети в GNS3 определены следующие IP-адреса:

1) 192.168.1.2 – устройство жертвы (AlpineLinux-victim);
2) 192.168.3.2 – устройство нарушителя (AlpineLinux);
3) 192.168.2.2 – устройство с ограниченной ОС (VPCS).

На устройствах нарушителя и целевой машины был установлен инструмент iptables. На устройстве AlpineLinux с помощью команды, представленной на рисунке 3, был изменен IP-адрес источника в IP-пакетах.

```
/ # iptables -t nat -A POSTROUTING -p icmp -j SNAT --to-source 192.168.5.2
```

Рисунок 3 – Команда для изменения адреса источника в IP-пакете

На рисунке 4 приведены полученные с помощью анализатора трафика Wireshark сведения о пакетах, отправленных в ходе реализации успешной DDoS-атаки, при которой была осуществлена замена адреса источника при отправке пакетов с устройства нарушителя.

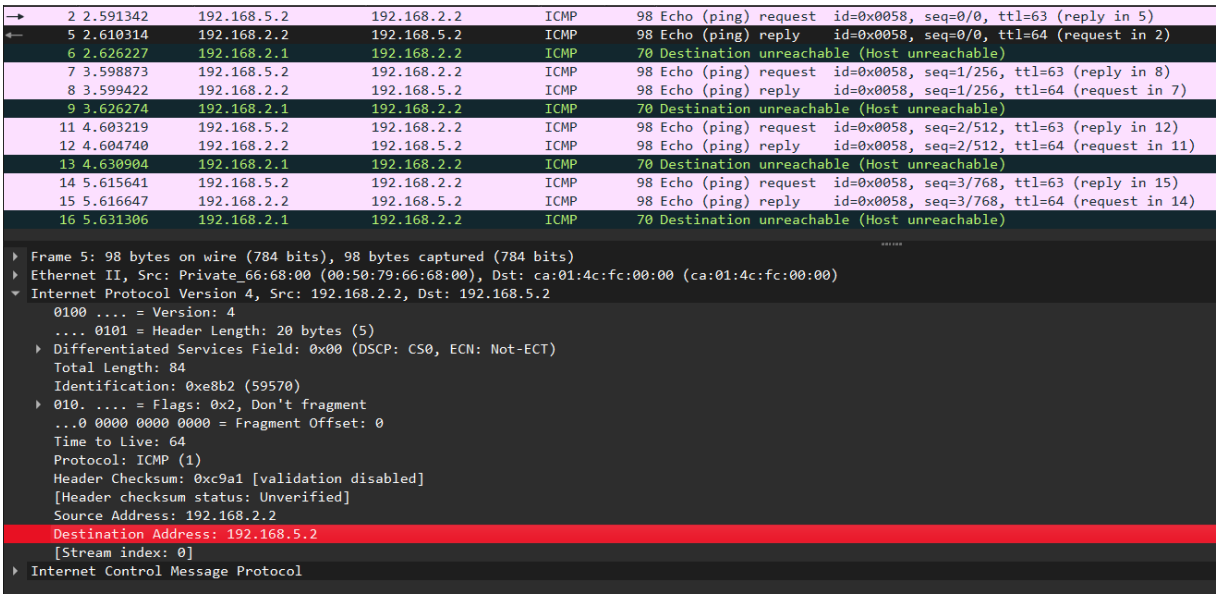

Рисунок 4 – Сведения о пакетах, отправленных в ходе реализации успешной DDoS-атаки

Методы защиты от угроз IP Spoofing включают:

– мониторинг сетей на предмет подозрительной активности;

– использование аутентификации;

– использование межсетевого экрана;

– включение Unicast Reverse Path Forwarding (uRPF) на маршрутизаторах для поиска обратного маршрута пакетов;

– ограничение доступа к сетевым ресурсам (настройка access-list).

Подход к защите от угроз IP Spoofing, основанный на использовании access-list и uRPF на маршрутизаторах для фильтрации трафика, приведен на рисунке 5.

```
R1#sh access-list
Extended IP access list FILTER_TRAFFIC
    10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 (4 matches)
    20 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 (12 matches)
    30 deny ip any any (19 matches)
```

```
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip access-group FILTER_TRAFFIC in
 ip verify unicast reverse-path
 duplex half
!
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group FILTER_TRAFFIC in
 ip verify unicast reverse-path
 duplex half
!
interface FastEthernet2/0
 ip address 192.168.3.1 255.255.255.0
 ip verify unicast reverse-path
 duplex half
```

Рисунок 5 – Настройка access-list и проверка маршрута пакета

Механизм работы Unicast Reverse Path Forwarding включает в себя проверку маршрута пакета в таблице маршрутизации, если адрес источника входящего пакета существует, то осуществляется поиск обратных маршрутов к адресу источника, если найден интерфейс, который соответствует интерфейсу получения, то пакет пропускается, в ином случае отбрасывается.

Результаты анализа трафика при включенной фильтрации пакетов приведен на рисунке 6.

2 3.896275	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=0/0, ttl=63 (reply in 5)
5 3.927704	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=0/0, ttl=64 (request in 2)
6 3.974412	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
7 4.915986	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=1/256, ttl=63 (reply in 8)
8 4.915986	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=1/256, ttl=64 (request in 7)
9 4.959386	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
10 5.916578	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=2/512, ttl=63 (reply in 11)
11 5.916578	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=2/512, ttl=64 (request in 10)
12 5.932204	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
14 11.128433	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x008a, seq=0/0, ttl=63 (reply in 15)
15 11.128433	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x008a, seq=0/0, ttl=64 (request in 14)
16 11.156775	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
17 12.151722	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x008a, seq=1/256, ttl=63 (reply in 18)
18 12.152712	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x008a, seq=1/256, ttl=64 (request in 17)
19 12.166758	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)

Рисунок 6 – Результаты анализа трафика при фильтрации пакетов

Заключение. На основе проведенных исследований можно сделать следующие выводы.

1. Регулярное проведение анализа эффективности методов защиты от угроз информационной безопасности является важным мероприятием, направленным на повышение защищенности информационных систем.

2. Применение таких технологий, как фильтрация трафика, Unicast Reverse Path Forwarding, а также списков контроля доступа обеспечивает эффективное выявление и блокировку поддельных пакетов, что способствует защите данных. Настройка этих инструментов предоставляет возможность анализировать сетевую активность и разрабатывать эффективные меры защиты от угроз кибератаки IP Spoofing.

Список использованных источников:

1. IP Spoofing: что это и как работает [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/ip-spoofing – Дата доступа: 07.04.2025.

2. Черкасов Д. Ю., Иванов В. В. IP-spoofing // Евразийский научный журнал. – 2017. – №. 6. – С. 197-200.

3. Предотвращение подделки адресов через Unicast Reverse Path Forwarding [Электронный ресурс] – Режим доступа: https://www.opennet.ru/base/cisco/unicast_reverse_path_forwarding.txt.html – Дата доступа: 07.04.2025.

4. Бобов М. Н., Мохаммед Ф. О. Методы использования механизма поиска обратного маршрута для защиты локальных сетей от атаки спуфинга //Доклады БГУИР. – 2010. – №. 5 (51). – С. 72-75.

ANALYSIS OF PROTECTION METHODS AGAINST IP SPOOFING THREATS USING GNS3

Rusetskaya T.B.[1], gr.261401

Belarusian State University of Informatics and Radioelectronics[1],
Minsk, Republic of Belarus

Boiprav O.V. – PhD in Technical Sciences, Head of the Department of Information Security, Associate Professor

Annotation. The article presents the results of an IP Spoofing threat analysis performed using GNS3 simulator. For this analysis, a virtual mockup consisting of the intruder's devices, target device and router was developed. The study consisted of a description of IP Spoofing as well as the effects of the cyber-attack on network security. The study's findings yielded recommendations to enhance the security level of information systems. The results obtained may be of use to information protection specialists, in order that they might develop effective measures to prevent such threats, as well as for improving the security of network communications.

Keywords. Network cyber-attack, IP Spoofing, GNS3, VMware, iptables, Wireshark.