УДК 00

Смирнов Сергей Максимович Баев Азамат Аланович студенты

Российский государственный университет нефти и газа (РФ, г. Москва)

НАСТРОЙКА БЕЗОПАСНОСТИ РЕШЕНИЙ, НА ОСНОВЕ IGMP v1

Аннотация. Данная работа представляет собой практическое исследование по настройке и обеспечению безопасности multicast-сети с использованием протокола IGMP v1. В рамках лабораторного стенда был развернут программный маршрутизатор на базе Linux и настроен коммутатор L2 с функциями IGMP Snooping и Querier. Ключевые этапы работы включали: настройку IP-маршрутизации и отключение Strict Reverse Path Filtering (rp_filter) на интерфейсах маршрутизатора для корректной работы multicast; принудительное выставление версии IGMPv1 через системные параметры ядра (force_igmp_version=1); конфигурацию правил iptables для разрешения multicast-трафика и добавления статического маршрута к группе 224.0.0.0/4.

Ключевые слова:IGMP, IGMP v1, RFC 1112, multicast, многоадресная рассылка, Source-Specific Multicast (SSM), IGMP Snooping, IGMP Querier, безопасность сети, фильтрация трафика, защита от атак, strict reverse path filtering, IPTables, multicast-группа 224.2.2.2.

Протокол IGMP (Internet Group Management Protocol) — это важный инструмент для управления групповой рассылкой в сетях IP. Документ RFC 1112, который называется «Расширения для групповой рассылки IP», содержит описание первой версии IGMP (IGMPv1). Формат пакета IGMPv1 показана на рисунке 1.

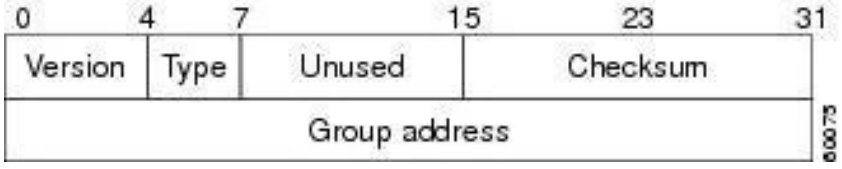

Рисунок 1 — Формат сообщения IGMPv1 В версии 1 существуют только два типа IGMP-сообщений:

- Запрос на членство (Membership Query)

- Отчет о членстве (Membership Report)

Компьютеры отправляют отчеты IGMP для конкретной групповой рассылки, чтобы показать, что хотят получать для нее данные. Программное обеспечение сети на компьютере само отправляет такой отчет, когда приложение начинает работать с групповой рассылкой. Маршрутизатор время от времени отправляет запрос, чтобы проверить, есть ли еще компьютеры, которые хотят получать данные для этой группы. Если после трех запросов никто не ответил, маршрутизатор перестает отправлять данные для этой группы.

IGMPv1 не использует шифрование или проверку подлинности. Это значит, что данные можно перехватить или подделать. Это может быть плохо для приложений, которые передают важные данные через групповую рассылку. Но у протокола есть и положительные стороны для защиты:
Эффективная передача данных — IGMP помогает маршрутизаторам понять, нужно ли отправлять групповой трафик в определенную часть сети. Это предотвращает отправку ненужных данных туда, где их никто не ждет.
Контроль за группами — протокол позволяет маршрутизаторам следить, какие устройства еще хотят получать данные, и убирать те, которые стали неактивны.

Пример топологии эксперимента показан на рисунке 2.

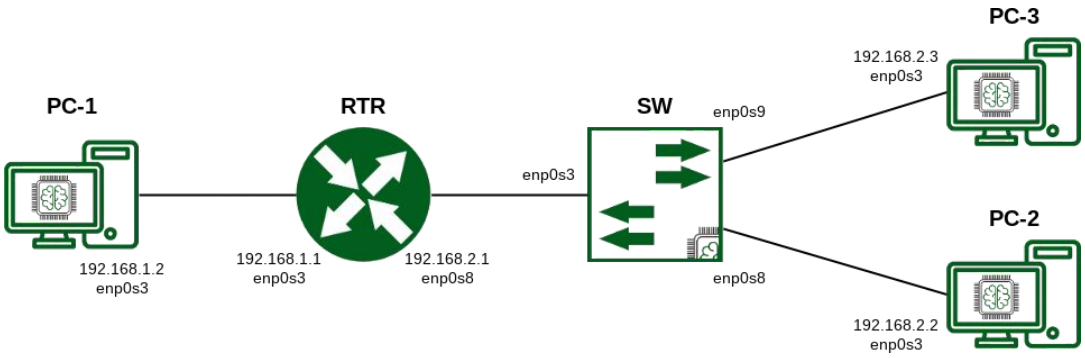

Рисунок 2 – Топология

Включение функции IGMP Snooping на коммутаторах позволяет им следить за служебными сообщениями IGMP. Используя эти данные, коммутатор строит таблицы для группового трафика, отправляя его только на те порты, где есть активные получатели. Этот способ не дает рассылать групповые пакеты на все порты подряд, что снижает риск атак, направленных на перегрузку каналов связи ненужным трафиком.

Настройка IGMP Querier. В сети с работающим IGMP Snooping нужен компонент IGMP Querier, который будет регулярно отправлять запросы о групповых рассылках. Это помогает поддерживать таблицы коммутатора в актуальном состоянии и обеспечивает стабильную работу групповой рассылки.

Регулярный контроль и детальный разбор сетевого трафика. Постоянное наблюдение за IGMP-пакетами помогает быстро находить необычную активность и выявлять попытки атак, такие как подмена групповых сообщений или преднамеренная перегрузка сети групповым трафиком.

Активируем на роуторе маршрутизатор и отключаем strict reverse path filtering, после чего принудительно устанавливаем использование протокола IGMP v1. Действия представлены на рисунке 3:

Рисунок 3 – Установка использования протокола

Включаем на маршрутизаторе работу групповой рассылки и отключаем строгую проверку обратного пути, затем задаем использование IGMP v1. Результат представлен на рисунке 4:

```
[root@vbox ~]# iptables -I INPUT -d 224.0.0.0/4 -j ACCEPT
[root@vbox ~]# iptables -I FORWARD -d 224.0.0.0/4 -j ACCEPT
[root@vbox ~]# router add -net 224.0.0.0/4 dev enp0s8
```

Рисунок 4 – Настройка правил irtables

Настройка IGMP Snooping и Querier на коммутаторе. Результат представлен на рисунке 5:

```
[root@vbox ~]# echo 1 > /sys/dev
dev/     devices/
[root@vbox ~]# echo 1 > /sys/devices/virtual/net/bridge/bridge/multicast_snoo
ping
[root@vbox ~]# echo 1 > /sys/devices/virtual/net/bridge/bridge/multicast_quer
```

Рисунок 5 – Настройка IGMP Snooping и Querier

Проверка настроек

Отправляем эхо-запросы на другие компьютеры, чтобы убедиться, что сеть работает. Результат представлен на рисунке 6:

```
[root@vbox ~]# ping 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 56(84) bytes of data.
64 bytes from 192.168.2.20: icmp_seq=1 ttl=63 time=1.16 ms
64 bytes from 192.168.2.20: icmp_seq=2 ttl=63 time=2.23 ms
64 bytes from 192.168.2.20: icmp_seq=3 ttl=63 time=1.89 ms
^C
--- 192.168.2.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.158/1.757/2.227/0.446 ms
[root@vbox ~]# ping 192.168.2.30
PING 192.168.2.30 (192.168.2.30) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
^C
--- 192.168.2.30 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3059ms
pipe 4
[root@vbox ~]# ping 192.168.2.30
PING 192.168.2.30 (192.168.2.30) 56(84) bytes of data.
64 bytes from 192.168.2.30: icmp_seq=1 ttl=63 time=1.84 ms
64 bytes from 192.168.2.30: icmp_seq=2 ttl=63 time=2.31 ms
```

Рисунок 6 – Проверка связанности

На всех устройствах проверить настройку IGMP v1. Результат представлен на рисунке 7:

Рисунок 7 – Проверка настроек IGMP v1

Запуск сервера на multicast-группе 224.2.2.2. Результат представлен на рисунке 8:

Рисунок 8 – Запуск сервера

Отправка данных. Результат представлен на рисунке 9:

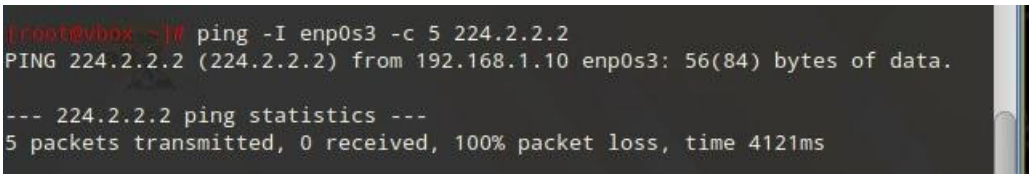

Рисунок 9 – Отправка трафика

Полученные данные. Результат представлен на рисунке 10:

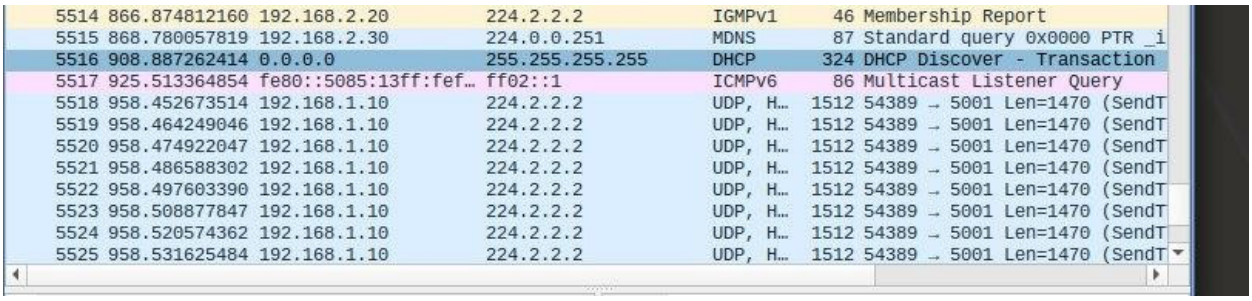

Рисунок 10 – Полученные данные

На втором компьютере запрос на получение данных не отправлялся поэтому трафик не пришёл. Результат представлен на рисунке 11:

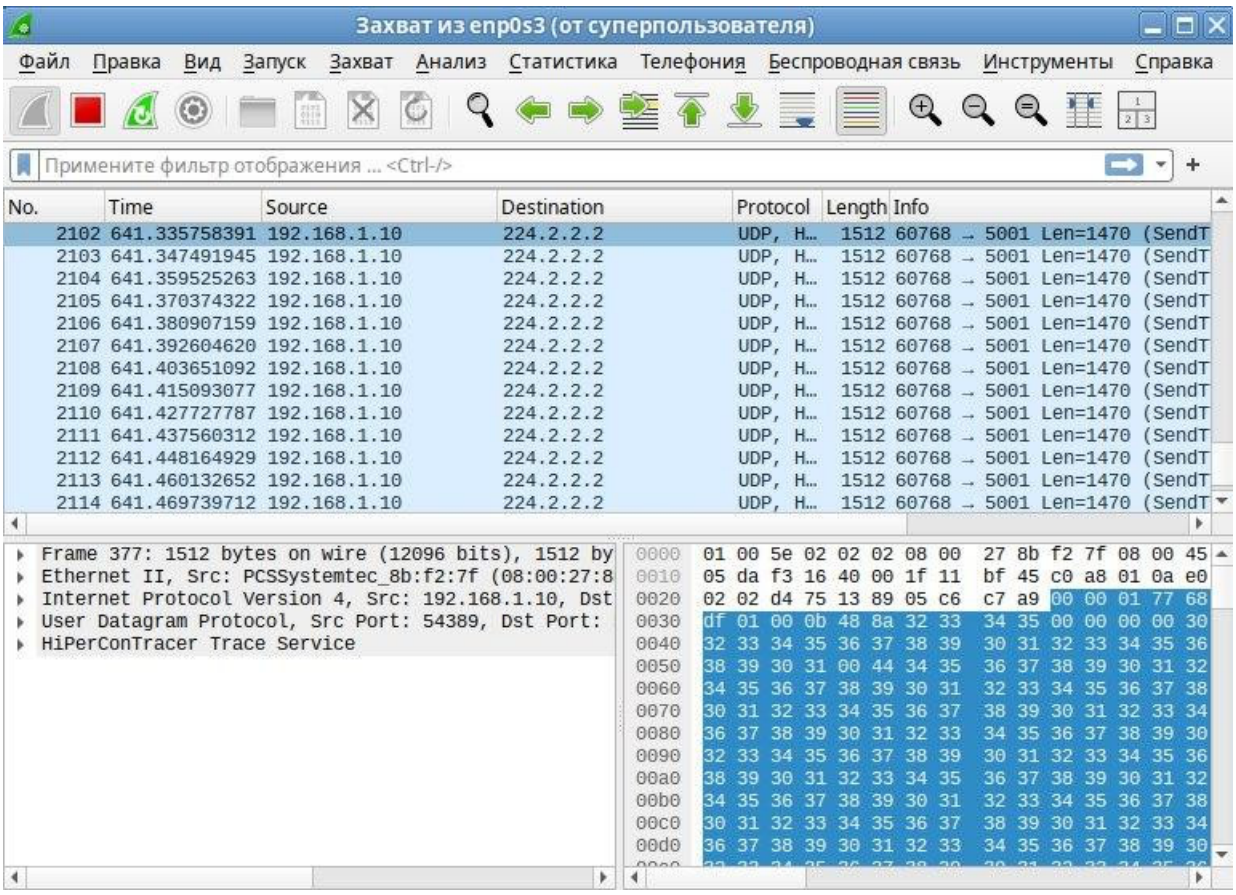

Рисунок 11 – Отсутствие трафика

Простота IGMP v1 и отсутствие в нем шифрования уравновешиваются основным, но работающим способом защиты, который ограничивает трафик только подписанными участниками. Главный результат эксперимента состоит в том, что безопасность групповой рассылки зависит в большей степени от правильной настройки сети, а не от возможностей самого протокола. Совместное использование IGMP Snooping и Querier на коммутаторе, фильтрация на маршрутизаторе и точная настройка ОС Linux вместе предотвращают несанкционированный доступ к групповым потокам и их распространение. Это позволяет безопасно использовать IGMP v1 в контролируемых сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Отечественная ОС «Альт СП» релиз 10 отвечает требованиям ФСТЭК России по защите средств виртуализации и контейнеризации /

KateBasealt [Электронный ресурс] // Хабр: [сайт]. — URL: https://habr.com/ru/news/754012/ (дата обращения: 07.12.2024).

2. Система управления пакетами [Электронный ресурс] // Red-Soft: [сайт] — URL: https://redos.red-soft.ru/base/sup-yum/intro/ (дата обращения: 05.07.2024).

3. Мультивещание. [Электронный ресурс] // Wikipedia: [сайт] – URL: https://ru.wikipedia.org/wiki/Мультивещание (дата обращения: 01.07.2024).

4. Оптимизация передачи multicast-трафика в локальной сети с помощью IGMP snooping. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/cbs/articles/309486/

5. Приручаем multicast. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/icl_group/articles/429062/

6. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 190 с.
— ISBN 978-5-4497-2559-2, 978-5-4488-1745-8.

7. IGMP. [Электронный ресурс] // Wikipedia: [сайт] – URL: https://ru.wikipedia.org/wiki/IGMP (дата обращения: 17.11.2023).

8. Network Storage & Security // официальный блог. – URL: https://networkstoragesecurity.wordpress.com/igmpv1-igmpv2- igmpv3/ (дата обращения: 15.09.2024).

9. Static Multicast Routing. – [электронный ресурс]. – Режим доступа: https://www.altlinux.org/Static_Multicast_Routing

10. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство

"Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ