Аспирант каф. ИЗИ Д.В. Мишин,
студентка гр. КЗИ-108 И.Ю. Богомазова

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ УЯЗВИМОСТИ КОММУТАТОРОВ CISCO К АТАКАМ ТИПА MAC-FLOODING

Данная работа посвящена экспериментальному исследованию подверженности коммутатора Cisco Catalyst Express 500 уязвимости.

Предметом исследования является уязвимость коммутатора Cisco Catalyst Express 500 к атакам MAC-flooding. Под нормальным функционированием будем понимать способность коммутатора выполнять свои функции с требуемым качеством [1].

Атака MAC-flooding [2] является наиболее распространенным видом атак на коммутаторы второго уровня ISO OSI и представляет собой переполнение CAM (Content Addressable Memory) таблицы коммутатора потоком случайных MAC-адресов, что переводит его в режим концентратора (в этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора). CAM таблица — ограниченная по объему таблица во всех моделях коммутаторов, в которую записываются MAC-адрес источника кадра и другая необходимая информация (метка времени, порт получения кадра). На основе поступающих на порты коммутатора данных содержимое этой таблицы обновляется для поддержания наибольшей актуальности и дополняется ранее неизвестными MAC-адресами и сопутствующей информацией.

Гипотеза исследования составила предположение о том, что коммутатор Cisco Catalyst Experss 500 восприимчив к атакам на CAM таблицу.

Экспериментальное исследование нацелено на определение возможности реализации атаки MAC-flooding на коммутатор Cisco Catalyst Experss 500 на примере в КСПД кафедры ИЗИ Владимирского государственного университета.

Для достижения этой цели были поставлены следующие задачи:

- создание экспериментальной установки;
- проведение эксперимента;
- анализ результатов эксперимента и оценка устойчивости современных коммутаторов к атакам рассматриваемого типа.

Суть эксперимента заключается в генерации на атакующем компьютере большого числа кадров с произвольными MAC-адресами отправителя и получателя (вредоносного трафика) с помощью специальной программы. Атаку условимся считать успешной, если удалось перевести коммутатор в режим концентратора за приемлемое время, неуспешной в противоположном случае. Признак успешной атаки определим, как появление у атакующего

возможности видеть данные отправляемые и получаемые другими хостами в сети. Под приемлемым временем будем понимать интервал времени не превышающий одно лабораторное занятие. Будем увеличивать число атакующих машин до тех пор, пока не обнаружим признак успешной атаки или не исчерпаем лимит доступных компьютеров (экспериментальной установки).

Эксперимент проводится на специально созданной экспериментальной установке, которая представляет собой сегмент сети из десяти компьютеров и коммутатора. Схема установки изображена на рис. 1.

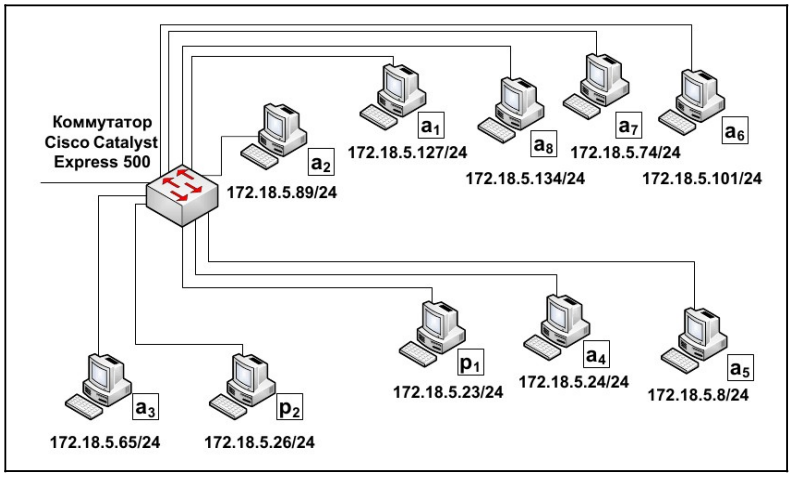

Рис. 1. Схема экспериментальной установки

Обозначим за $A = \{a_1,a_2,\ldots,a_8\}$ множество атакующих компьютеров, которые могут производить генерацию вредоносного трафика, где a_1 – первичная атакующая машина, с которой производится прослушивание сети. Элементы a_2, a_3,…, a_8 – вторичные атакующие машины, которые при необходимости будут последовательно задействованы для реализации атаки. Обозначим за p_1 и p_2 машины, между которыми происходит обмен ICMP (echo) пакетами.

Основные характеристики используемого оборудования представлены в табл. 1.

Таблица 1. Основные характеристики оборудования, используемого в экспериментальной установке

Рабочая станция	2x Intel Pentium 4 class 3400, CPU 2.4 GHz, 512 Mb RAM DDR2, HDD 256Gb, монитор, клавиатура, мышь.
Сетевое оборудование	Коммутатор Cisco Catalyst Express 500 (24 портовый, 10/100BASE-TX; RJ-45; UTP-5, максимум 8000 MAC-адресов, производительность 8,8 Гбит/с).
	Сетевая плата Intel® 82945G Express Chipset Family
Соединительные кабели	Кабель UTP-5e

Условия эксперимента:

- Все компьютеры исследуемой сети работают под управлением ОС Ubuntu 10.10.
- Конфигурации ПО рабочих станций p_1 и p_2 одинаковы.

- На компьютер a_1 установлено все дополнительное ПО, перечисленное в табл. 2.
- На вторичные атакующие компьютеры установлено дополнительное ПО dsniff.

Таблица 2. Дополнительное программное обеспечение

ПО	Тип ПО	Версия	Тип лицензии	Источник
Wireshark	Анализатор трафика с графическим пользовательским интерфейсом	1.4.3	GNU General Public License	Репозитории Ubuntu
dsniff	Пакет программ для сетевого аудита и проверок на возможность проникновения	2.3	Open Source	Репозитории Ubuntu

Схема проведения эксперимента представлена на рис. 2.

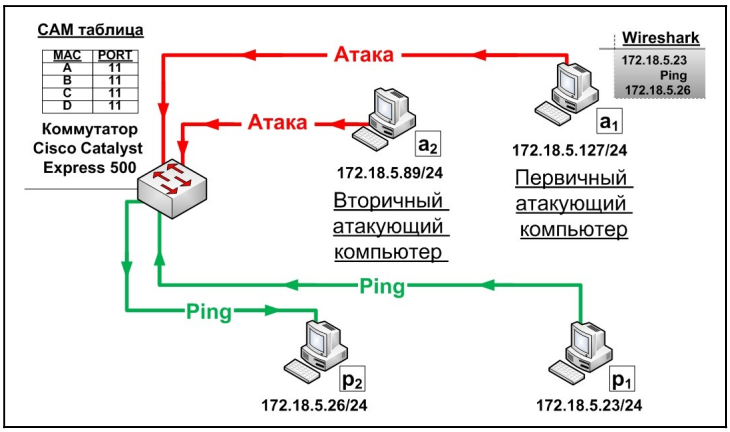

Рис. 2. Схема проведения эксперимента

Эксперимент проводился в 2 этапа.

1 этап. Подготовка к атаке.

Шаг 1. Для обеспечения трафика (который нужно увидеть атакующему) между двумя компьютерами в сети на машине p_1 запущена отправка ICMP (echo) пакетов на адрес 172.18.5.26.

Шаг 2. На компьютере a_1 Wireshark настроен на отображение только ICMP пакетов для облегчения наблюдения за трафиком.

Шаг 3. В дампе анализатора (рис. 3) обнаружен лишь трафик a_1. Коммутатор работает в штатном режиме, так как признак успешной атаки отсутствует.

```
No.     Time        Source                Destination           Protocol Info
1804384 330.275229  172.18.5.127          10.1.11.35            ICMP     Destination unreachable (Port unreachable)
Frame 1804384 (123 bytes on wire, 123 bytes captured)
Ethernet II, Src: AsustekC_53:b8:5e (00:17:31:53:b8:5e), Dst: 3com_32:3b:01 (00:1a:c1:32:3b:01)
Internet Protocol, Src: 172.18.5.127 (172.18.5.127), Dst: 10.1.11.35 (10.1.11.35)
Internet Control Message Protocol
------------------------------------------------------------------------------------------------------------------------
No.     Time        Source                Destination           Protocol Info
1804386 330.275249  172.18.5.127          10.1.11.35            ICMP     Destination unreachable (Port unreachable)
Frame 1804386 (112 bytes on wire, 112 bytes captured)
Ethernet II, Src: AsustekC_53:b8:5e (00:17:31:53:b8:5e), Dst: 3com_32:3b:01 (00:1a:c1:32:3b:01)
Internet Protocol, Src: 172.18.5.127 (172.18.5.127), Dst: 10.1.11.35 (10.1.11.35)
Internet Control Message Protocol
```

Рис. 3. Выписка из файла истории Wireshark.

2 этап. Атака.

Шаг 1. Обеспечена непрерывная генерация вредоносного трафика с помощью утилиты macof (рис. 4) из пакета dsniff.

```
root@vlaizi2427bw01:/home/student/Downloads#: macof
b5:cf:65:4b:d5:59 2c:01:12:7d:bd:36 0.0.0.0.4707 > 0.0.0.0.28005: S 106321318:106321318(0) win 512
68:2a:55:6c:1c:1c bb:33:bb:4d:c2:db 0.0.0.0.44367 > 0.0.0.0.60982: S 480589777:480589777(0) win 512
1e:95:26:5e:ab:4f d7:80:6f:2e:aa:89 0.0.0.0.42809 > 0.0.0.0.39934: S 1814866876:1814866876(0) win 512
51:b5:4a:7a:03:b3 70:a9:c3:24:db:2d 0.0.0.0.41274 > 0.0.0.0.31780: S 527694740:527694740(0) win 512
51:75:2e:22:c6:31 91:a1:c1:77:f6:18 0.0.0.0.36396 > 0.0.0.0.15064: S 1297621419:1297621419(0) win 512
7b:fc:69:5b:47:e2 e7:65:66:4c:2b:87 0.0.0.0.45053 > 0.0.0.0.4908: S 976491935:976491935(0) win 512
```

Рис. 4. Выписка из консоли macof.

Шаг 2. Установлено непрерывное наблюдение за трафиком для обнаружения признака успешной атаки.

Шаг 3. По истечении заданного времени признак успешной атаки не был зафиксирован.

Шаг 4. Увеличено число атакующих компьютеров на 1 (a_2).

Шаг 5. На атакующем компьютере зафиксировано появление ICMP пакетов хостов p_1 и p_2 (рис. 5).

```
No.     Time        Source                Destination           Protocol Info
2576618 672.771578  172.18.5.23           172.18.5.26           ICMP     Echo (ping) reply
Frame 2576618 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Giga-Byt_4a:ab:8a (00:16:e6:4a:ab:8a), Dst: AsustekC_1f:28:7a (00:1f:c6:1f:28:7a)
Internet Protocol, Src: 172.18.5.23 (172.18.5.23), Dst: 172.18.5.26 (172.18.5.26)
Internet Control Message Protocol
------------------------------------------------------------------------------------------------------------------------
No.     Time        Source                Destination           Protocol Info
3133875 895.618650  172.18.5.23           172.18.5.26           ICMP     Echo (ping) reply
Frame 3133875 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Giga-Byt_4a:ab:8a (00:16:e6:4a:ab:8a), Dst: AsustekC_1f:28:7a (00:1f:c6:1f:28:7a)
Internet Protocol, Src: 172.18.5.23 (172.18.5.23), Dst: 172.18.5.26 (172.18.5.26)
Internet Control Message Protocol
```

Рис. 5. Выписка из файла истории Wireshark.

Эксперимент дал следующий результат: признак успешной атаки был обнаружен. Следовательно, таблица коммутатора оказалась переполнена и атака достигла успеха.

По результатам эксперимента можно сделать вывод о том, что коммутатор Cisco Catalyst Express 500 подвержены атакам MAC-flooding.

Список литературы

1. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е изд. С испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 1138 с.: ил.

2. Самойленко Н. Безопасность канального уровня «Linux Vacation / Eastern Europe» / «Международная конференция разработчиков и пользователей свободного программного обеспечения-2009» / Учебный центр «Сетевые технологии», Киев, Украина.