к.т.н., доцент каф. ИЗИ Д.В. Мишин, магистрант гр. ИСмб-213 И.Ю. Богомазова

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ УЯЗВИМОСТИ КОММУТАТОРОВ D-LINK МОДЕЛЕЙ DES-1016D, DES-3526, DES-3828 К АТАКАМ ТИПА MAC-FLOODING

Данная работа посвящена экспериментальному исследованию подверженности коммутаторов D-Link моделей DES-1016D, DES-3526, DES-3828 уязвимости связанной с возможностью проведения атаки MAC-flooding. Коммутаторы рассматриваемых моделей наиболее распространены в инфраструктуре корпоративной сети передачи данных ВлГУ. Для обеспечения сетевой безопасности необходимо знать об уязвимостях применяемого оборудования, что позволит применить адекватные механизмы защиты.

Предметом исследования является уязвимость коммутаторов D-Link моделей DES-1016D, DES-3526, DES-3828 к атаке 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.

Гипотезы исследования составили предположения о том, что

- коммутатор D-Link DES-1016D восприимчив к атакам на CAM таблицу (MAC-flooding).
- коммутатор D-Link DES-3526 восприимчив к атакам MAC-flooding.
- коммутатор D-Link DES-3828 восприимчив к атакам MAC-flooding.

Экспериментальное исследование нацелено на определение возможности реализации атаки MAC-flooding на коммутаторы D-Link моделей DES-1016D, DES-3526, DES-3828 на примере в КСПД кафедры ИЗИ Владимирского государственного университета.

Для достижения этой цели были поставлены следующие задачи:

- Провести анализ предметной области.

- Выдвинуть гипотезу об уязвимости коммутаторов D-Link моделей DES-1016D, DES-3526, DES-3828 в заданных условиях.
- Разработать методику эксперимента.
- Собрать экспериментальную установку.
- Провести эксперименты.
- Оценить полученные результаты.

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.

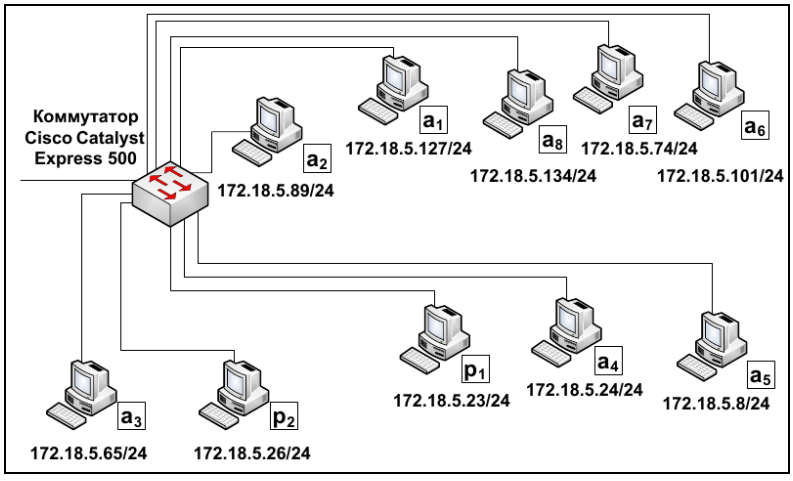

Рис. 1. Схема экспериментальной установки

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.

Краткое описание каждой из рассматриваемых моделей коммутаторов содержится таблице 1.

Таблица 1. Основные характеристики рассматриваемых коммутаторов

D-Link DES-1016D	неуправляемый, 2 уровня, 16 портов, 10/100Base-TX; максимум 8Кб записей в CAM таблице на устройство, время старения MAC-адресов 300 с, производительность 3,2 Гбит/с
D-Link DES-3526	управляемый, 2 уровня, 24 порта, 10/100Base-TX+2 комбо-порта 1000Base-T/ Min-GBIC; максимум 8Кб записей в CAM таблице на устройство, время старения MAC-адресов 300 с, производительность 8,8 Гбит/с; по умолчанию функции Port security и IP-MAC-Port Binding отключены
D-Link DES-3828	управляемый, 3 уровня, 24 порта, 10/100Base-TX+2 комбо-порта 1000Base-T/SFP+2 порта 1000Base-T; максимум 16Кб записей в CAM таблице на устройство, время старения MAC-адресов 300 с, производительность 12,8 Гбит/с; по умолчанию функции Port security и IP-MAC-Port Binding отключены, есть управление широковещательным штормом

Основные характеристики другого используемого оборудования представлены в таблице 2.

Таблица 2. Основные характеристики другого оборудования, используемого в экспериментальной установке

Рабочая станция	HP Compaq 8000 Elite, Intel Core 2 Duo E8400, CPU 3.0 GHz, 1.25 Gb RAM, HDD 80Gb, NIC Intel® 82578 GbE, монитор, клавиатура, мышь.
Соединительные кабели	UTP cat.5e

Условия эксперимента:

- Все компьютеры исследуемой сети работают под управлением ОС Kali Linux 3.7.2.
- Конфигурации ПО рабочих станций p_1 и p_2 одинаковы.
- На компьютер a_1 установлено все дополнительное ПО, перечисленное в таблице 3.
- На вторичные атакующие компьютеры установлено дополнительное ПО macof из пакета dsniff.

Таблица 3. Дополнительное программное обеспечение

ПО	**Тип ПО**	**Версия**	**Тип лицензии**	**Источник**

ПО	Тип ПО	Версия	Тип лицензии	Источник
Wireshark	Анализатор трафика с GUI	1.8.5	GNU GPL	В составе Kali Linux
macof	Создание лавины пакетов со случайными MAC-адресами	2.4	Open Source	В составе пакета dsniff в Kali Linux

Схема проведения эксперимента представлена на рис. 2.

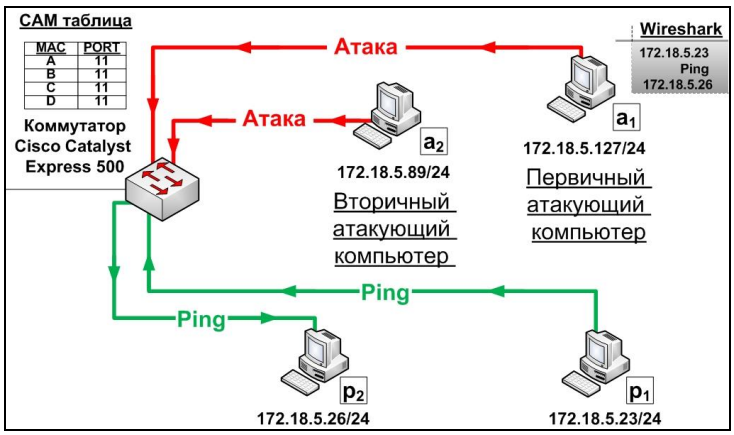

Рис. 2. Схема проведения эксперимента

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
-------------------------------------------------------------------------------------------------
```

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) и т.д.

Шаг 5.

На атакующем компьютере зафиксировано появление ICMP пакетов хостов p1 и p2 (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
--------------------------------------------------------------------------------------------------------------
```

Рис. 5. Выписка из файла истории Wireshark.

- D-Link DES-1016D: При атаке с 3 станций (a_1, a_2, a_3) на a1 зафиксирован перехват ICMP-пакетов хостов p1 и p2. Атака успешно проведена. Конец.
- D-Link DES-3526: При атаке с 4 станций (a_1, a_2, a_3, a_4) на a1 зафиксирован перехват ICMP-пакетов хостов p1 и p2. Атака успешно проведена. Конец..
- D-Link DES-3828: При атаке с 6 станций (a_1, a_2, a_3, a_4, a_5, a_6) признак успешной атаки за приемлемое время обнаружен не был. Атака неуспешна. Конец.

Через некоторый промежуток времени коммутатор D-Link DES-3526 восстановил нормальный режим функционирования за счет наличия времени старения записей в CAM таблице.

По результатам эксперимента можно сделать следующие выводы:

- D-Link DES-3828 при заводских настройках устойчив к атаке MAC-flooding.
- Коммутаторы D-Link DES-1016D и DES-3526 с заводскими настройками подвержены атакам MAC-flooding. Таким образом, необходимо применение механизмов защиты (изменение заводских настроек) или замена оборудования. Уязвимость может быть устранена путем использования функций: Port security и IP-MAC-Port Binding.

Основные результаты работы:

- Проведен обзор характеристик коммутаторов D-Link моделей DES-1016D, DES-3526, DES-3828 и порядка осуществления атак.
- Выдвинуты гипотезы об уязвимости коммутаторов D-Link DES-1016D, DES-3526, DES-3828 с заводскими настройками к атаке MAC-flooding.
- Разработана методика проведения эксперимента для проверки гипотезы.
- Собрана экспериментальная установка на базе лаборатории кафедры ИЗИ ВлГУ.
- Проведены эксперименты.
- Полученные результаты подтвердили гипотезы об уязвимости коммутаторов D-Link DES-1016D, DES-3526 к атакам типа MAC-flooding и опровергли гипотезу об уязвимости D-Link DES-3828.

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.