УДК 00 – 004.7:004.738.5

Бутаков Л.О.
Студент
Морозов Т.А.
студент
Научный руководитель: Павловский В.В.,
Старший преподаватель кафедры БИТ РГУ нефти и газа (НИУ) имени И.М. Губкина

Butakov L.O.
Student
Morozov T.A.
Student
Scientific supervisor: Pavlovskiy V.V.,
Senior Lecturer at the Department of BIT of Gubkin Russian State University of Oil and Gas (NRU)

МЕТОДЫ ТЕСТИРОВАНИЯ И ЗАЩИТЫ ОТ АТАКИ VLAN HOPPING

METHODS OF TESTING AND PROTECTION AGAINST VLAN HOPPING ATTACKS

Аннотация: В статье рассматриваются основные принципы и механизмы атаки VLAN Hopping — способа обхода сетевой изоляции, предоставляемой виртуальными локальными сетями (VLAN), с целью получения несанкционированного доступа к ресурсам других VLAN. Описаны наиболее распространённые техники реализации атак Switch Spoofing и Double Tagging. Приведены практические методики

тестирования сетевой инфраструктуры на уязвимость к этим атакам с использованием специализированного инструментария. Представлены рекомендации по эффективным мерам защиты, включающим правильную настройку портов коммутаторов, отключение автоматического согласования транковых соединений и использование нестандартных VLAN ID для native VLAN. Результаты исследования показывают критическую важность комплексного подхода к конфигурации сетевого оборудования для обеспечения надежной защиты от атак VLAN Hopping.

Ключевые слова: VLAN Hopping, Switch Spoofing, Double Tagging, сетевая безопасность, тестирование на проникновение, DTP, IEEE 802.1Q, коммутаторы, сегментация сети.

Abstract: The article discusses the basic principles and mechanisms of VLAN Hopping attacks, a method of bypassing network isolation provided by virtual local area networks (VLANs) in order to gain unauthorized access to resources of other VLANs. The most common techniques for implementing Switch Spoofing and Double Tagging attacks are described. Practical methods of testing network infrastructure for vulnerability to these attacks using specialized tools are presented. Recommendations on effective protection measures are presented, including proper configuration of switch ports, disabling automatic trunk connection negotiation, and using non-standard VLAN IDs for native VLANs. The results of the study show the critical importance of an integrated approach to network equipment configuration to ensure reliable protection against VLAN Hopping attacks.

Keywords: VLAN Hopping, Switch Spoofing, Double Tagging, Network Security, Penetration Testing, DTP, IEEE 802.1Q, Switches, Network Segmentation.

Современные корпоративные сети характеризуются высокой степенью сложности и разнородности подключенных устройств, что требует эффективных механизмов сегментации для обеспечения безопасности и управляемости сетевой инфраструктуры. Виртуальные локальные сети (VLAN) стали стандартным решением для логической сегментации сетевого трафика, позволяя создавать изолированные домены безопасности в рамках единой физической инфраструктуры.

Исследования в области безопасности VLAN ведутся с момента появления технологии в середине 1990-х годов. Значительный вклад в изучение уязвимостей VLAN внесли такие исследователи, как Frank Knobbe, который в 2002 году описал основные принципы атак VLAN Hopping, и David Convery, автор фундаментальной работы "Hacking Layer 2". Современные исследования фокусируются на анализе новых векторов атак, связанных с эволюцией сетевых протоколов и появлением программно-определяемых сетей.

На сегодняшний день хорошо изучены основные механизмы работы протоколов IEEE 802.1Q и Dynamic Trunking Protocol, разработаны стандартные меры защиты от классических атак VLAN Hopping. Однако остается недостаточно исследованным вопрос адаптации существующих методик тестирования к современным гибридным сетевым архитектурам и оценки эффективности защитных мер в условиях использования различных производителей сетевого оборудования.

Объект исследования: безопасность виртуальных локальных сетей в контексте атак обхода сетевой изоляции.

Предмет исследования: методики реализации атак VLAN Hopping, инструментарий для тестирования уязвимостей и эффективность защитных мер против данного типа угроз.

Цель исследования: разработка комплексного подхода к выявлению уязвимостей VLAN Hopping и формирование практических рекомендаций по защите сетевой инфраструктуры от данного типа атак. Практические

рекомендации будут представлены в отельном разделе, который наглядно будет показывать настройку всех устройств, которые участвуют в эксперименте.

Основные гипотезы исследования:

1. Автоматизированные инструменты тестирования могут эффективно выявлять потенциальные точки атак;
2. Комплексный подход к защите обеспечивает значительное снижение рисков компрометации.

Тип исследования: прикладное исследование с элементами экспериментального тестирования.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая физические коммутаторы Cisco Catalyst серии 2960, Eltex MES1428, MikroTik (CRS326-24G-25+RM), а также два PC с операционными системами Linux.

Методы сбора данных:

1. Анализ конфигураций сетевого оборудования;
2. Автоматизированное тестирование с использованием инструментов Yersinia и Scapy;
3. Мониторинг сетевого трафика с применением Wireshark;
4. Анализ логов коммутаторов и систем обнаружения вторжений.

Процедура проведения исследования:

1. Настройка тестовой среды с различными конфигурациями VLAN;
2. Реализация атак Switch Spoofing и Double Tagging;
3. Тестирование эффективности защитных мер;
4. Анализ результатов и формирование рекомендаций.

Методы обработки данных: качественный анализ эффективности защитных мер, сравнительный анализ поведения различных моделей коммутаторов.

Прежде всего следует разобраться с тем, что такое атака VLAN Hopping. Атака VLAN Hopping представляет собой сложную и многофакторную угрозу кибербезопасности, направленную на нарушение изоляции виртуальных локальных сетей (VLAN) и получение несанкционированного доступа к сетевым ресурсам. Данная атака эксплуатирует фундаментальные механизмы функционирования VLAN-технологий, включая процессы тегирования трафика по стандарту IEEE 802.1Q и динамическое формирование магистральных соединений между коммутаторами. Основными векторами реализации VLAN Hopping являются атака подмены коммутатора (Switch Spoofing) и атака двойного тегирования (Double Tagging), каждая из которых использует различные уязвимости в конфигурации сетевого оборудования для преодоления границ VLAN.

Switch Spoofing – атака подмены коммутатора представляет собой изощренный метод компрометации VLAN-сегментации, при котором злоумышленник эмулирует поведение легитимного сетевого коммутатора для принуждения целевого устройства к созданию магистрального соединения. Данная атака эксплуатирует механизмы автоматического согласования trunk-портов, основанные на протоколе DTP, который предназначен для упрощения администрирования сети путем автоматической настройки межкоммутаторных соединений. Злоумышленник настраивает свое устройство на отправку специально сформированных DTP-пакетов, имитирующих запросы на создание магистрального соединения от имени коммутатора, что приводит к неправильной интерпретации целевым коммутатором роли атакующего устройства в сетевой топологии.

Double Tagging – атака двойного тегирования представляет собой более сложную и технически изощренную разновидность VLAN Hopping, которая эксплуатирует особенности обработки VLAN-тегов коммутаторами в магистральных соединениях. Данная атака основана на

манипулировании механизмом обработки множественных VLAN-тегов в сетевых кадрах, позволяя злоумышленнику обходить стандартные механизмы изоляции VLAN и доставлять трафик в целевые сегменты сети, к которым у него нет непосредственного доступа. Концептуальной основой атаки является создание Ethernet-кадра с двумя VLAN-тегами: внешним тегом, соответствующим VLAN, к которому подключен злоумышленник, и внутренним тегом, указывающим на целевую виртуальную сеть.

Таким образом, Switch Spoofing возможен только на Cisco Catalyst 2960, где возможен DTP. Double Tagging работает на всех трёх коммутаторах при наличии native VLAN 1 на trunk-портах.

На рисунке 1 представлена используемая топология сети.

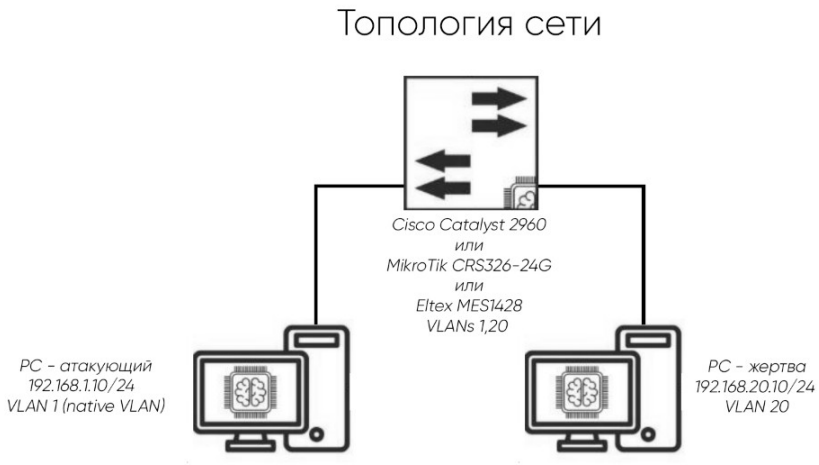

Рисунок 1 – Топология сети для эксперимента

Далее представлена настройка всех машин. Эксперимент был проведён несколько раз с различным устройствами в роли L2 коммутатора, поддерживающего VLAN и trunk-порты.

Для того, чтобы переходить к настройке физических устройств стоит воспользоваться специальным приложением – PuTTY, которое позволит подключиться к коммутаторам (Cisco Catalyst 2960 и Eltex MES1428) для того, чтобы настроить их изнутри. Само приложение представлено на рисунке 2.

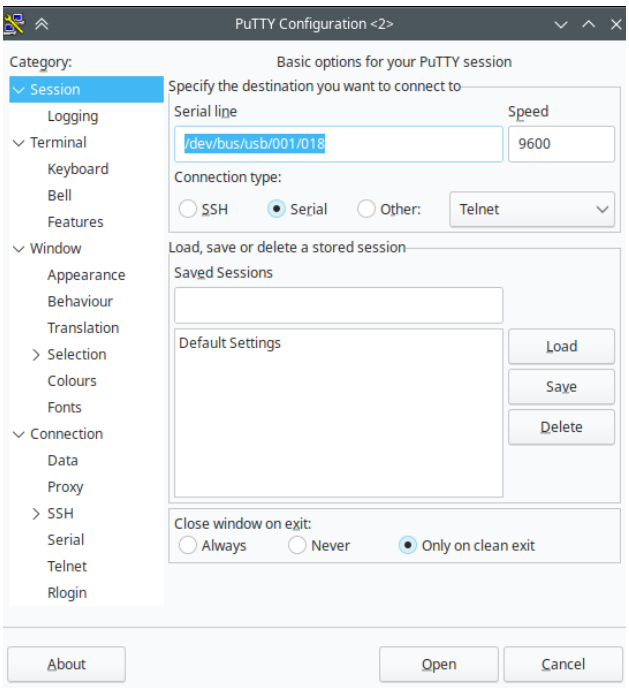

Рисунок 2 –Приложение PuTTY для настройки коммутаторов

Рассмотрим настройку конкретных машин. Для начала покажем настройку Cisco Catalyst 2960 и Eltex MES1428. Стоит понимать, что настройка производилась по отдельности каждый раз для каждого нового состава топологии, ведь в эксперименте участвуют три устройства: два PC и один коммутатор.

Начнём с объяснения настройки коммутатора Cisco Catalyst 2960. Создадим VLAN, настроим trunk-порт, настроим порты двух ПК (у одного – динамический режим, у другого – порт access). Данная настройка показана на рисунке 3. Для удобства присвоим разные hostname для коммутаторов (Switch – Cisco Catalyst 2960; Switch2 – Eltex MES1428).

```
Switch#configure terminal
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20_V
Switch(config-vlan)#exit
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 1
Switch(config-if)#switchport trunk allowed vlan 1,20
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode dynamic desirable
Switch(config-if)#switchport trunk encapsulation
Switch(config-if)#switchport trunk native vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface FastEthernet0/10
Switch(config-if)#switchport mode dynamic desirable
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk native vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
```

Рисунок 3 – Настройка Cisco Catalyst 2960

Теперь покажем настройку для Eltex MES1428. Создадим VLAN 1 (native) и VLAN 20. Настроим порт для атакующего ПК (PC1) в режиме general (для trunk) interface GigabitEthernet 0/1. Настроим порт для жертвы (PC2) в VLAN 20. Данная настройка показана на рисунке 4.

```
Switch2#configure terminal
Switch2(config)#vlan 1
Switch2(config-vlan)#exit
Switch2(config)#vlan 20
Switch2(config-vlan)#exit
Switch2(config)#interface GigabitEthernet 0/1
Switch2(config-if)#switchport mode general
Switch2(config-if)#switchport general allowed vlan add 1 untagged
Switch2(config-if)#switchport general pvid 1
Switch2(config-if)#no shutdown
Switch2(config-if)#exit
Switch2(config)#interface GigabitEthernet 0/2
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#no shutdown
Switch2(config-if)#exit
Switch2(config)#exit
```

Рисунок 4 – Настройка Eltex MES1428

Также продемонстрируем настройку MikroTik. Осуществим подключение через ssh, и введём команды, которые представлены на рисунке 5.

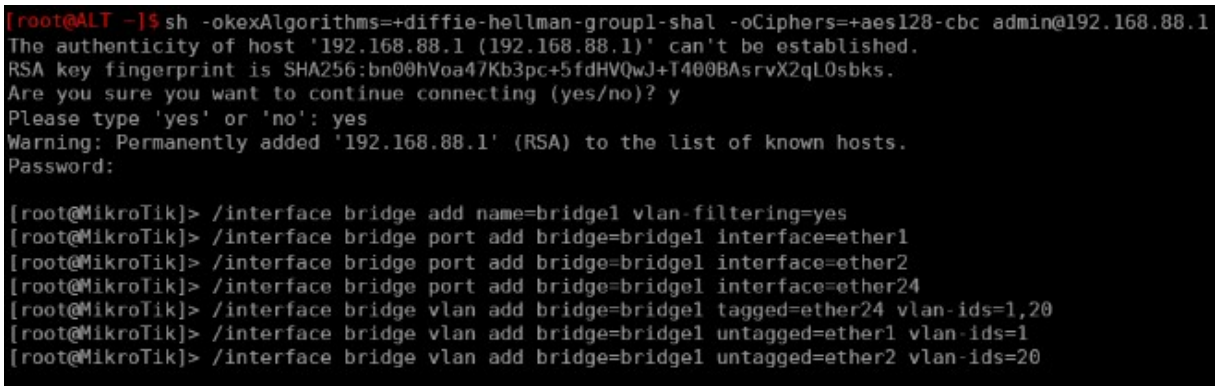

Рисунок 5 – Настройка MikroTik

Далее перейдём к настройке PC. Покажем настройку атакующего PC. Сначала настроим IP адрес (access порт VLAN 1). Настройка представлена на рисунке 6.

Рисунок 6 – Настройка IP на атакующем PC

На PC жертве настройка IP (VLAN 20) аналогичная, только IP здесь: `192.168.20.10/24`.

Для того, чтобы осуществить атаку Switch Spoofing нужно включить поддержку VLAN-тегов на атакующем PC (рисунок 7).

Рисунок 7 – Включение VLAN-тегов

Для запуска самой атаки потребуется специальная утилита Yersinia (интерфейс представлен на рисунке 9). Для её запуска в консоли прописать команду, которая представлена на рисунке 8.

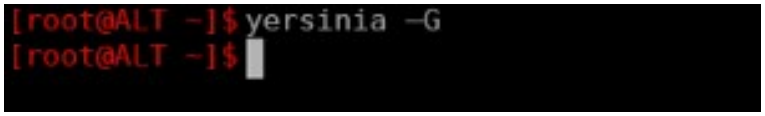

Рисунок 8 – Запуск приложения Yersinia

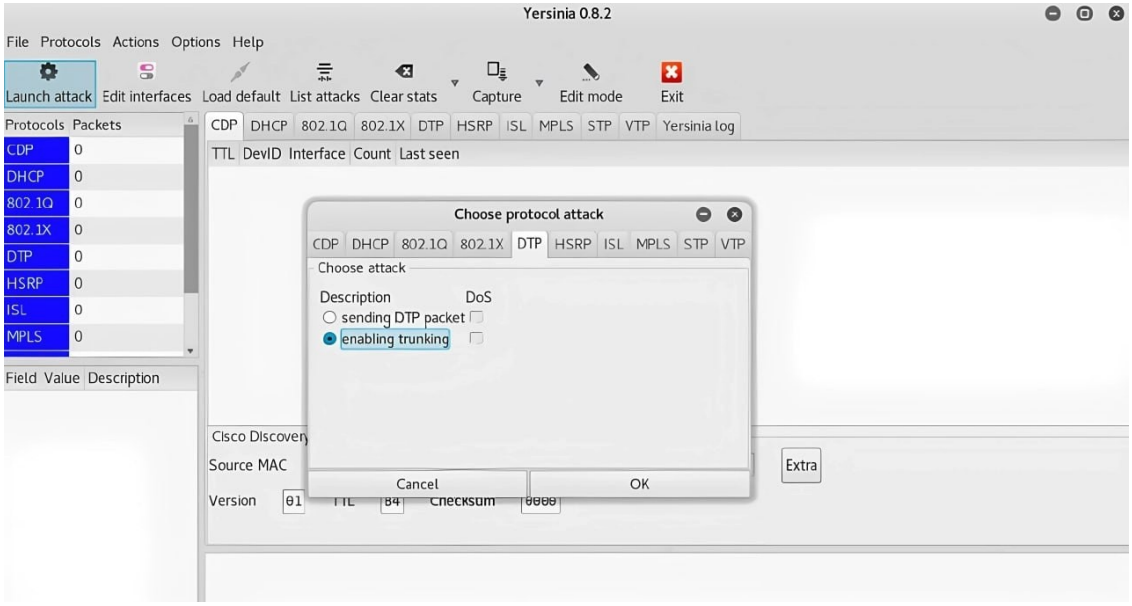

Рисунок 9 – Интерфейс приложения Yersinia

Для запуска атаки внутри приложения Yersinia нужно нажать следующую последовательность кнопок: "DTP" → "Enabling trunking" → "Атака на eth0".

Для того, чтобы осуществить атаку Double Tagging создадим двойной VLAN интерфейс на атакующем PC (рисунок 10).

```
[root@ALT ~]$ip link add link eth0 name eth0.1 type vlan id 1
[root@ALT ~]$ip link add link eth0.1 name eth0.1.20 type vlan id 20
[root@ALT ~]$ip addr add 192.168.20.100/24 dev eth0.1.20
[root@ALT ~]$ip link set eth0.1.20 up
[root@ALT ~]$
```

Рисунок 10 – Создание двойного VLAN интерфейса

А для проведения самой атаки потребуется следующая команда на PC: `ping 192.168.20.10`. Применение команды – на рисунке 11.

```
[root@ALT ~]$ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=64 time=0.474 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=64 time=0.442 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=64 time=0.220 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=64 time=0.220 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=64 time=0.223 ms
64 bytes from 192.168.20.10: icmp_seq=7 ttl=64 time=0.415 ms
```

Рисунок 11 – Запуск атаки Double Tagging

Защита от атак VLAN Hopping требует реализации комплексного подхода к настройке сетевого оборудования и применения множественных уровней безопасности для минимизации рисков компрометации VLAN-сегментации. Первичной мерой защиты от атак Switch Spoofing является

отключение автоматического согласования магистральных портов путем деактивации протокола DTP на всех портах коммутаторов, которые не предназначены для межкоммутаторных соединений. Это достигается использованием команды `switchport nonegotiate`, что полностью исключает возможность динамического создания trunk-портов. Дополнительно необходимо явно настраивать все порты конечных устройств в режиме `access` с помощью команды `switchport mode access`, что гарантирует их функционирование исключительно в качестве портов доступа.

Предотвращение атак двойного тегирования требует более сложных конфигурационных изменений, направленных на устранение уязвимостей в обработке нативного VLAN. Ключевой мерой защиты является изменение нативного VLAN с используемого по умолчанию VLAN 1 на неиспользуемый идентификатор, что исключает возможность подключения конечных устройств к нативному VLAN. Эта мера должна применяться последовательно на всех магистральных портах в сетевой инфраструктуре для поддержания целостности конфигурации. Дополнительно рекомендуется использование явного тегирования для всех VLAN, включая нативный, что может быть достигнуто настройкой vlan dot1q tag native на магистральных портах Cisco коммутаторов.

Перейдём обеспечению защиты устройств. Для того, чтобы осуществить защиту на Cisco Catalyst 2960, отключим DTP на порту PC1. Изменим native VLAN на trunk-порту. Включим Port Security. Данная настройка представлена на рисунке 9.

```
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 999
Switch(config-if)#switchport nonegotiate
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface GigabitEthernet0/24
Switch(config-if)#switchport trunk native vlan 999
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#end
Switch#
```

Рисунок 9 – Настройки для защиты для Cisco Catalyst 2960

Теперь осуществим защиту на Eltex MES1428. Переведём порт PC1 в access-режим. Изменим native VLAN на trunk-порту. Настройка представлена на рисунке 10.

```
Switch2#configure terminal
Switch2(config)#interface GigabitEthernet0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 999
Switch2(config-if)#no switchport general allowed vlan
Switch2(config-if)#no shutdown
Switch2(config-if)#exit
Switch2(config)#interface GigabitEthernet0/24
Switch2(config-if)#switchport trunk native vlan 999
Switch2(config-if)#exit
Switch2(config)#exit
Switch2#
```

Рисунок 10 – Настройки для защиты для Eltex MES1428

Для защиты MikroTik заходим на него через ssh и делаем настройку, которая представлена на рисунке 11.

```
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.88.1' (RSA) to the list of known hosts.
Password:

[root@MikroTik]> /interface bridge vlan set [find vlan-ids=1] vlan-ids=999
[root@MikroTik]> /interface bridge vlan add bridge=bridge1 tagged=ether24 vlan-ids=999,20
[root@MikroTik]> /interface bridge port set ether1 pvid=999
```

Рисунок 11 – Настройки для защиты для MikroTik

Таким образом, в настройке MikroTik CRS326 native VLAN изменяется с 1 на 999, чтобы снизить риски атак, связанных с использованием стандартного нативного VLAN. Порт ether24 настроен как tagged для VLAN 999 и VLAN 20 — это trunk-порт, передающий трафик с

VLAN тегами. Порт ether1 назначен с PVID 999, что соответствует неиспользуемому VLAN, и служит как access-порт для устройства PC1, изолируя его от основных VLAN. Такая конфигурация обеспечивает разделение трафика и предотвращает несанкционированный доступ между VLAN. В MikroTik CRS326 настройка VLAN осуществляется через виртуальный мост (bridge), который объединяет физические порты и управляет передачей трафика с учётом VLAN-тегов. При этом протокол DTP отсутствует, и все trunk-порты настраиваются вручную, что повышает безопасность и исключает возможность динамического согласования trunk. Назначение IP-адреса на интерфейс моста (bridge) позволяет управлять устройством и обеспечивать маршрутизацию трафика через него. Таким образом, мы создаём виртуальный коммутатор с поддержкой VLAN, который эффективно разделяет трафик между VLAN и объединяет физические интерфейсы в единую управляемую сетевую структуру.

В ходе проведённого исследования была подтверждена уязвимость сетевого оборудования к атакам VLAN Hopping при некорректной конфигурации портов. Эксперименты, выполненные на трёх различных коммутаторах — Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326 — показали, что атаки типа Switch Spoofing и Double Tagging могут быть реализованы при неправильной настройке портов, в частности, при использовании динамического согласования trunk (DTP) на Cisco или при наличии незащищённого trunk/наличия стандартного native VLAN на всех устройствах. Это свидетельствует о том, что основная причина уязвимости связана с ошибками конфигурирования, а не с аппаратными ограничениями устройств.

Особенно эффективно атака Switch Spoofing проявилась на коммутаторе Cisco Catalyst 2960, где реализован протокол DTP: злоумышленник может эмулировать поведение коммутатора и перевести порт в режим trunk, получая доступ к трафику всех VLAN, проходящих через данный порт. На MikroTik CRS326 и Eltex MES1428 данный вектор

атаки невозможен, поскольку эти устройства не поддерживают DTP, и trunk-порты настраиваются только вручную. Успешная реализация этой атаки на Cisco подчёркивает необходимость отключения протокола DTP и жёсткой настройки портов в режиме access для конечных устройств, что значительно снижает риски.

Атака Double Tagging была успешно реализована на всех трёх моделях коммутаторов, однако с определёнными ограничениями. Она позволила получить односторонний доступ к VLAN, обходя стандартные механизмы сегментации. На MikroTik CRS326, Eltex MES1428 и Cisco Catalyst 2960 при использовании нативного VLAN 1 атака прошла успешно, но её эффективность ограничена односторонним характером связи и требует точного знания топологии VLAN. Это важно учитывать при оценке угроз и планировании мер защиты.

Практические результаты исследования подтвердили, что рекомендуемые меры безопасности — отключение DTP (для Cisco), явное задание режимов портов (access или trunk), изменение нативного VLAN с VLAN 1 на другой идентификатор, а также внедрение механизмов Port Security и 802.1Q — существенно снижают риск успешного проведения атак VLAN Hopping. Регулярный аудит конфигураций и соблюдение этих рекомендаций являются ключевыми элементами защиты сетевой структуры.

Наконец, несмотря на общую уязвимость, различия в реализации и поведении коммутаторов MikroTik CRS326, Eltex MES1428 и Cisco Catalyst 2960 влияют на нюансы проведения атак и их обнаружения. Эти особенности необходимо учитывать при проектировании комплексных мер безопасности и при оценке потенциальных рисков для корпоративных сетей.

Таким образом, проведённое исследование подтвердило, что атаки VLAN Hopping остаются актуальной и серьёзной угрозой при неправильной конфигурации сетевого оборудования. Для обеспечения

надёжной защиты необходимо строгое соблюдение рекомендаций по настройке VLAN и trunk-портов, а также регулярный мониторинг и аудит сетевой инфраструктуры.

Проведенное исследование подтвердило актуальность угроз VLAN Hopping для современных сетевых инфраструктур. Экспериментальное тестирование показало высокую эффективность атак Switch Spoofing и Double Tagging против оборудования с конфигурациями по умолчанию, что подтверждает основную гипотезу о связи уязвимостей с неправильной настройкой сетевого оборудования.

Результаты проверки гипотез:

1. *Гипотеза 1 подтверждена:* автоматизированные инструменты показали эффективность выявления уязвимостей;
2. *Гипотеза 2 подтверждена:* комплексная защита обеспечила полное предотвращение протестированных атак.

Практические рекомендации:

1. Обязательная настройка всех портов доступа в режим access с отключением DTP;
2. Использование нестандартных VLAN ID для native VLAN на транковых портах;
3. Активация тегирования native VLAN для полной защиты от Double Tagging;
4. Внедрение специализированных правил мониторинга для обнаружения атак VLAN Hopping.

Направления дальнейшего исследования:

1. Анализ уязвимостей VLAN в программно-определяемых сетях (SDN);
2. Разработка автоматизированных систем обнаружения атак VLAN Hopping;
3. Изучение новых векторов атак, связанных с IPv6 и современными протоколами сетевой виртуализации.

Использованные источники:

1. Convery D., Choe J. Network Security Architectures [Электронный ресурс] // Cisco Press. - 2004. - URL: https://www.ciscopress.com/articles/article.asp?p=102157 (дата обращения: 03.04.2025)
2. Уймин А.Г. Компьютерные сети. L2-технологии [Электронный ресурс] // Ай Пи Ар Медия – Москва. - 2024. - URL: https://www.iprbookshop.ru/epd-reader?publicationId=135231 - ISBN 978-5-4497-2539-4 - (дата обращения: 02.04.2025)
3. Knobbe F. VLAN Security [Электронный ресурс] // SANS Reading Room. - 2002. - URL: https://www.sans.org/reading-room/whitepapers/protocols/vlan-security-853 (дата обращения: 03.04.2025)
4. IEEE Standard 802.1Q-2018 - Bridges and Bridged Networks [Электронный ресурс] // IEEE Standards Association. - 2018. - URL: https://standards.ieee.org/standard/802_1Q-2018.html (дата обращения: 05.04.2025)
5. Cisco Security Response Team. VLAN Hopping Attack Prevention [Электронный ресурс] // Cisco Security Advisory. - 2023. - URL: https://tools.cisco.com/security/center/resources/vlan_hopping (дата обращения: 05.04.2025)
6. SANS Institute. Network Penetration Testing Survey 2023 [Электронный ресурс] // SANS Survey Report. - 2023. - URL: https://www.sans.org/reading-room/whitepapers/survey/network-penetration-testing-survey-2023-39845 (дата обращения: 12.04.2025)