ПРОФЕССИОНАЛИТЕТ, 2025, № 1 (005)

УДК *004.732:004.056.53*

Л.Г. Хорошилов [1], Н.А. Костин [1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ АТАКИ DOUBLE TAGGING В ГЕТЕРОГЕННЫХ СЕТЯХ (CISCO, MIKROTIK, ELTEX)

Аннотация: *В статье представлен практический анализ атаки класса VLAN Hopping, реализуемой методом Double Tagging, которая позволяет обходить логическую изоляцию виртуальных локальных сетей, построенных на основе стандарта IEEE 802.1Q. Рассматриваются архитектурные особенности технологии VLAN, связанные с механизмом обработки native VLAN на транковых портах коммутаторов, которые создают предпосылки для реализации данной атаки на канальном уровне модели OSI. Подробно описан принцип формирования Ethernet-кадров с двойным тегированием 802.1Q и механизм их обработки сетевыми устройствами, приводящий к несанкционированной передаче трафика между логически изолированными сегментами сети.*

Экспериментальная часть исследования выполнена на специализированном тестовом стенде с использованием реального сетевого оборудования различных производителей, включая Cisco, MikroTik и Eltex, что позволяет оценить особенности реализации атаки в гетерогенной сетевой среде. Для генерации кадров с двойным тегированием применялся инструмент Yersinia, а фиксация результатов атаки осуществлялась с использованием анализатора сетевого трафика tcpdump.

В рамках работы проведено сравнение поведения оборудования при стандартных (дефолтных) конфигурациях и после применения защитных мер. Показано, что использование native VLAN по умолчанию на транковых портах делает сетевую инфраструктуру уязвимой к атаке Double Tagging независимо от производителя оборудования. На основе полученных результатов сформулированы практические рекомендации по защите, включающие изменение идентификатора native VLAN на неиспользуемый, явную настройку режимов портов и отказ от автоматического согласования транковых соединений. Результаты исследования подтверждают критическую важность корректной конфигурации сетевого оборудования для обеспечения безопасности сегментированных корпоративных сетей.

Ключевые слова: *VLAN Hopping, Double Tagging, сетевая безопасность, тестирование на проникновение, native VLAN, IEEE 802.1Q, сегментация сети.*

Введение

Логическая сегментация с помощью виртуальных локальных сетей (VLAN) на основе стандарта IEEE 802.1Q является фундаментальным механизмом для построения безопасных, производительных и управляемых корпоративных сетей [2]. Она позволяет создавать изолированные домены в рамках единой физической инфраструктуры. Однако сама архитектура VLAN содержит фундаментальные уязвимости, которые позволяют злоумышленнику обходить изоляцию сегментов. Наиболее критичной из таких угроз является атака VLAN Hopping, и особенно ее метод Double Tagging [4], который эксплуатирует особенности обработки native VLAN в сетевых устройствах.

Несмотря на то, что фундаментальные принципы атаки VLAN Hopping методом Double Tagging были описаны ещё в начале 2000-х годов, практическая реализация данной угрозы в современных сетях остается актуальной. Это связано с широким распространением гетерогенных сетевых инфраструктур, в которых одновременно используется оборудование различных вендоров, включая зарубежных (Cisco) и отечественных производителей (Eltex), а также популярные решения класса SMB и SOHO (MikroTik).

В условиях импортозамещения и активного внедрения отечественного сетевого оборудования особую значимость приобретает вопрос корректности типовых (дефолтных) конфигураций и их устойчивости к классическим атакам канального уровня. На практике сетевые администраторы часто воспроизводят шаблоны конфигураций, ориентированные на оборудование Cisco, без учета особенностей реализации VLAN-механизмов у других производителей.

Таким образом, научная новизна данного исследования заключается не в повторном описании механики атаки Double Tagging, а в сравнительном практическом анализе её реализации на современном оборудовании различных вендоров (Cisco, MikroTik, Eltex), а также в оценке универсальности защитных мер в гетерогенной сетевой среде.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Объект исследования: безопасность использования технологии виртуальных локальных сетей (VLAN) для логической сегментации сетевой инфраструктуры.

Предмет исследования: механизм атаки VLAN Hopping, реализуемый методом Double Tagging, средства тестирования соответствующей уязвимости, а также оценка эффективности мер защиты от подобных угроз.

Цель исследования: выполнить практический анализ атаки Double Tagging и на основе полученных результатов сформировать комплексный подход к защите сетевой инфраструктуры, предусматривающий методику проверки на уязвимость и практические рекомендации по конфигурации для предотвращения данной угрозы.

Литературный обзор.

Для начала необходимо определить ключевые термины и их значения.

Виртуальная локальная сеть (VLAN) – это логическая группа устройств, объединённых в отдельный широковещательный домен, независимо от их физического расположения. VLAN позволяют сегментировать сеть для повышения безопасности, производительности и управляемости.

Стандарт IEEE 802.1Q – основной протокол, определяющий механизм тегирования трафика для передачи информации о принадлежности кадра к определённому VLAN по магистральным (транковым) соединениям. Тег 802.1Q добавляется в заголовок кадра Ethernet и содержит, среди прочего, 12-битный идентификатор VLAN (VID) [1].

Порт доступа (Access Port) – порт коммутатора, предназначенный для подключения конечных узлов сети, таких как компьютеры или конечные устройства. Эти порты образуют нетегированный поток данных. Каждому порту доступа назначается определённая виртуальная локальная сеть (PVID), и все приходящие кадры с этого порта получают метку этого VLAN. Исходящие кадры покидают порт без метки, так как их направление уже определено VLAN [3].

Транковый порт (Trunk Port) – порт коммутатора, предназначенный для создания линии связи (транка) между двумя коммутаторами или между коммутатором и маршрутизатором. Эта линия транспортирует поток данных от нескольких VLAN. На транковых портах происходит маркировка (тегирование) кадров с метками VLAN, что позволяет принимающей стороне различать кадры для разных VLAN [3].

Native VLAN – специально назначенная VLAN на транковом порту, трафик которой передаётся без тега 802.1Q. По умолчанию на многих устройствах в этой роли выступает VLAN 1.

Атака VLAN Hopping – класс атак, целью которых является обход логической изоляции VLAN для получения несанкционированного доступа к трафику другого сегмента сети. Одним из методов реализации является Double Tagging (двойное тегирование) [4].

Следует отметить, что атаки класса VLAN Hopping включают в себя несколько различных векторов, наиболее известными из которых являются Double Tagging и Switch Spoofing (основанный на эксплуатации протокола DTP). В рамках данного исследования рассматривается исключительно атака Double Tagging. Это обусловлено тем, что на большинстве современных коммутаторов, включая исследуемые модели Cisco, MikroTik и Eltex, протокол динамического согласования транков (DTP) либо отключён по умолчанию, либо не реализован вовсе, что делает атаку Switch Spoofing нерелевантной для рассматриваемых конфигураций.

В то же время механизм обработки native VLAN и тегов IEEE 802.1Q сохраняет свою актуальность независимо от вендора и модели оборудования, что обосновывает фокус исследования именно на методе Double Tagging как наиболее универсальном и воспроизводимом в современных сетях.

Атака Double Tagging – техника, при которой злоумышленник формирует кадр Ethernet с двумя вложенными тегами 802.1Q. Первый (внешний) тег соответствует native VLAN на целевом транковом порту, что приводит к его удалению при обработке. Второй (внутренний) тег указывает на VLAN-жертву, в который кадр в итоге и перенаправляется, что позволяет преодолеть границу сегментации [5].

На основе анализа литературы и понимания указанных терминов можно сформулировать следующие гипотезы данного исследования:

1. H1: Типовая конфигурация коммутаторов различных вендоров является уязвимой к атаке Double Tagging, что позволяет осуществить несанкционированную передачу трафика между логически изолированными VLAN.
2. H2: Практическая методика демонстрации атаки Double Tagging на реальном сетевом оборудовании является эффективным инструментом для наглядного представления данной угрозы и может быть использована в учебном процессе для подготовки специалистов в области информационной безопасности.

Методы исследования

Исследование является экспериментальным и будет проводиться на специализированном тестовом стенде.

Характеристика среды исследования: сеть включает физические коммутаторы различных вендоров.

Узел 1 (жертва) – компьютер с операционной системой Kali Linux.

Узел 2 (атакующий) – компьютер с операционной системой Kali Linux.

Методы сбора данных:

1. Анализ и настройка конфигураций сетевого оборудования (уязвимой и защищённой).
2. Активное тестирование уязвимостей с использованием специализированного инструментария. В ходе эксперимента применялась утилита Yersinia, позволяющая генерировать сетевые кадры с двумя вложенными 802.1Q тегами (Double Tagging).
3. Пассивный мониторинг сетевого трафика с помощью анализатора tcpdump для фиксации этапов атаки и подтверждения её успешности.

Описание процедуры проведения исследования: на узле-жертве, находящемся в целевом VLAN (VLAN 10), запускается инструмент захвата трафика (tcpdump) для мониторинга входящих кадров, в то время как на узле-атакующем, физически подключенном к другому VLAN (VLAN 20), с помощью инструмента Yersinia реализуется атака Double Tagging. Данная атака заключается в отправке сформированных кадров Ethernet с двумя вложенными тегами 802.1Q (внешний — native VLAN, внутренний — целевой VLAN), что приводит к несанкционированной доставке трафика в изолированный VLAN-сегмент.

Эксперимент проводится в несколько этапов. Подготовительный этап направлен на настройку необходимого сетевого оборудования (коммутаторов различных вендоров) с созданием уязвимой конфигурации, при которой native VLAN на транковых портах оставлена равной значению по умолчанию (VLAN 1). Основным этапом является непосредственное проведение атаки Double Tagging и захват её результатов на узле-жертве. Заключительным этапом становится анализ полученных данных, проверка эффективности мер защиты (изменения native VLAN на неиспользуемый идентификатор) и подведение итогов эксперимента.

Методы обработки данных: Сравнительный и качественный анализ, направленный на сопоставление поведения оборудования разных вендоров, интерпретация данных сетевого трафика, обобщение результатов для подтверждения выдвинутых гипотез.

Ход исследования

Для начала необходимо настроить наши коммутаторы. Отметим, что настройка производилась отдельно для каждого этапа эксперимента с участием конкретного коммутатора определенного вендора в рамках топологии, состоящей из двух компьютеров и двух коммутаторов.

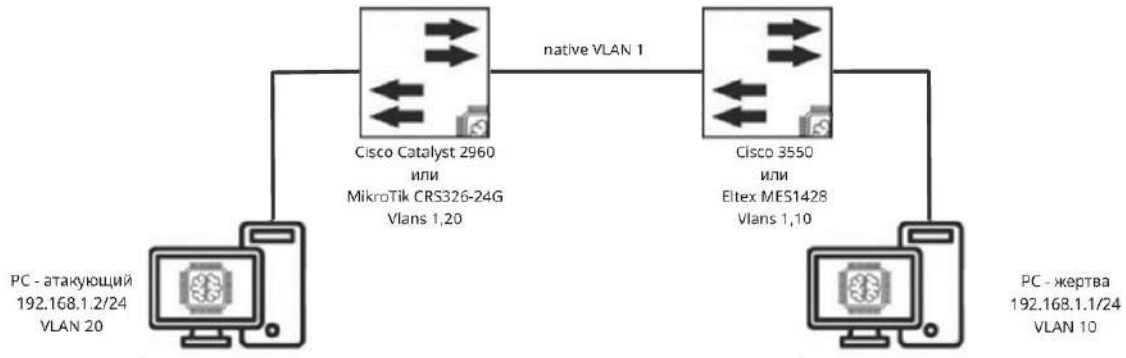

Рис. 1 Топология экспериментального стенда для проверки атаки Double Tagging между VLAN 20 и VLAN 10

Для начала рассмотрим настройку Cisco Catalyst 2960 и Cisco 3550.

Начнём с объяснения настройки коммутатора Cisco Catalyst 2960. Создадим VLAN 20, настроим два порта, один будет в режиме access, так как ведет к конечному узлу атакующего, другой в режиме trunk. Также у транкового порта явно укажем, что в качестве native VLAN берём VLAN 1. Конфигурация приведена в листинге 1.

Листинг 1 – Конфигурация коммутатора Cisco Catalyst 2960

```
conf t
vlan 20
 name VLAN20_V
 exit
int fa0/21
 switchport mode access
 switchport access vlan 20
 no shutdown
 exit
int fa0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan 1,20
 no shutdown
 exit
```

Теперь перейдем к настройке коммутатора Cisco 3550. Аналогично, создадим VLAN 10, настроим два порта, один будет в режиме access, так как ведет к конечному узлу-жертве, другой в режиме trunk. Также, у транкового порта явно укажем, что в качестве native VLAN берём VLAN 1. Конфигурация приведена в листинге 2.

Листинг 2 – Конфигурация коммутатора Cisco Catalyst 3550

```
conf t
vlan 10
 name VLAN10_V
 exit
int fa0/13
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
int fa0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 1
 switchport trunk allowed vlan 1,10
 no shutdown
```

```
exit
```

Теперь после настройки коммутаторов, перейдём к настройке PC. На атакующем PC настроим IP адрес (access порт VLAN 20). Настройка представлена на листинге 3.

Листинг 3 – Настройка IP-адреса на атакующем ПК

```
ip addr flush dev eth0
ip addr add dev eth0 192.168.1.2/24
```

На ПК-жертве настройка IP (VLAN 10) аналогичная, только IP здесь: 192.168.1.1/24.

Для запуска самой атаки потребуется специальная утилита Yersinia (интерфейс представлен на рисунке 2), широко применяемая в практиках тестирования безопасности сетей канального уровня [6].

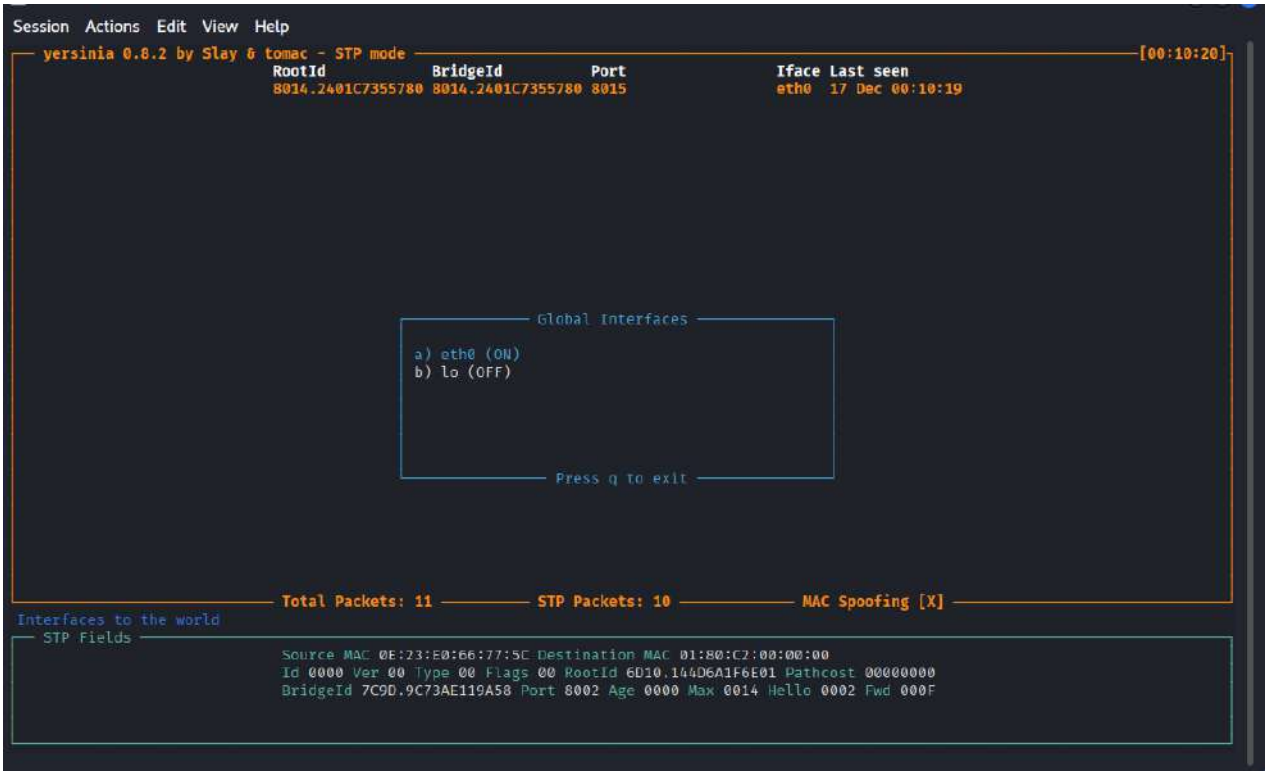

Рис. 2 Интерфейс утилиты Yersinia, используемой для формирования кадров с двойным тегированием 802.1Q

Для её запуска в консоли прописать команду, которая представлена на листинге 4.

Листинг 4 – Запуск приложения Yersinia

```
yersinia -I
```

Прежде чем запускать саму атаку, нужно убедиться, что в качестве интерфейса выбран нужный нам (в данном случае это eth0). Далее, нужно выбрать, какую именно атаку мы хотим совершить. Для этого нажимаем клавишу G и появляется иконка выбора протокола (Рисунок 3). Выбираем 802.1Q и нас перебросит в меню атаки.

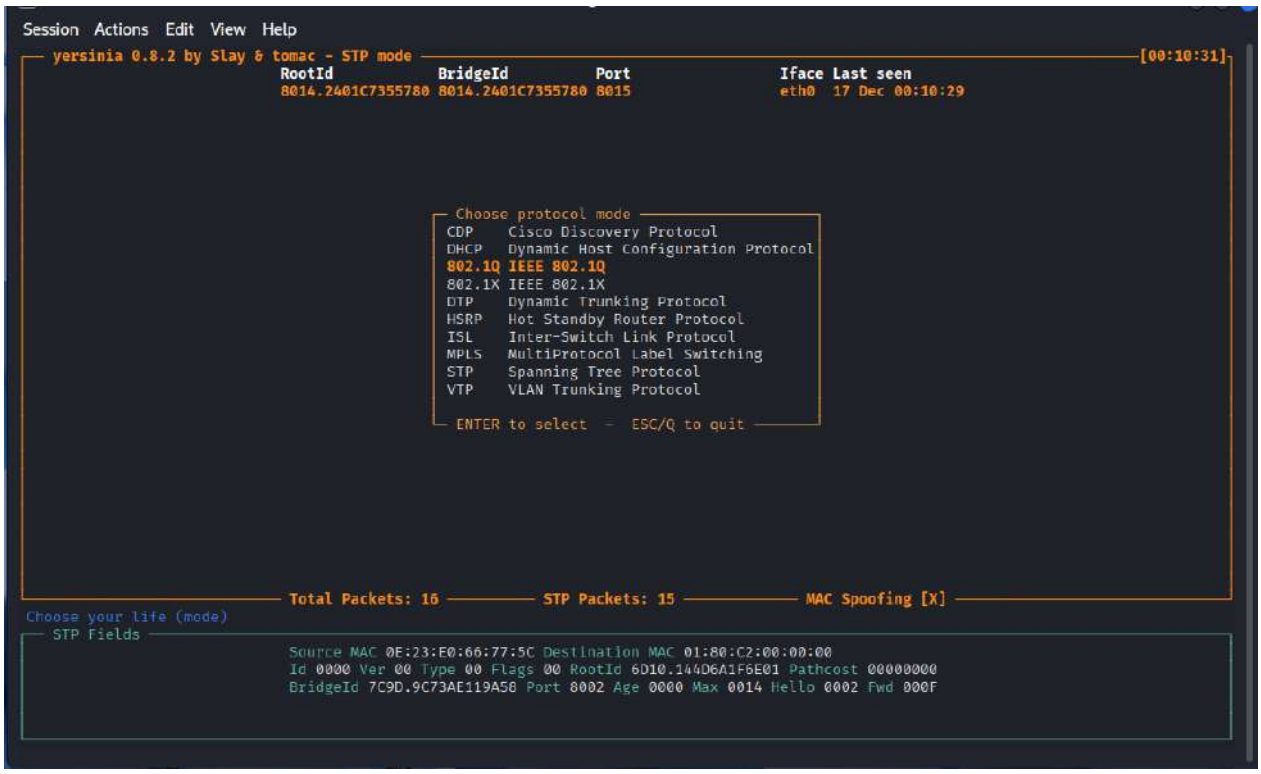

Рис. 3 Выбор протокола 802.1Q в утилите Yersinia для настройки атаки Double Tagging

Теперь, нажимаем клавишу E, чтобы отредактировать поля протокола 802.1Q. В качестве VLAN (внешнего) выбираем наш native VLAN 1, а внутренний VLAN указываем 10. Также важно указать Src IP – 192.168.1.2 (атакующий) и Dst IP – 192.168.1.1 (жертва). После этого выходим из меню настройки нажатием Esc и производим саму атаку. Для этого, нажимаем клавишу x и выбираем нужную нам Double tagging, нажав на 1. Настройка представлена на рисунке 4.

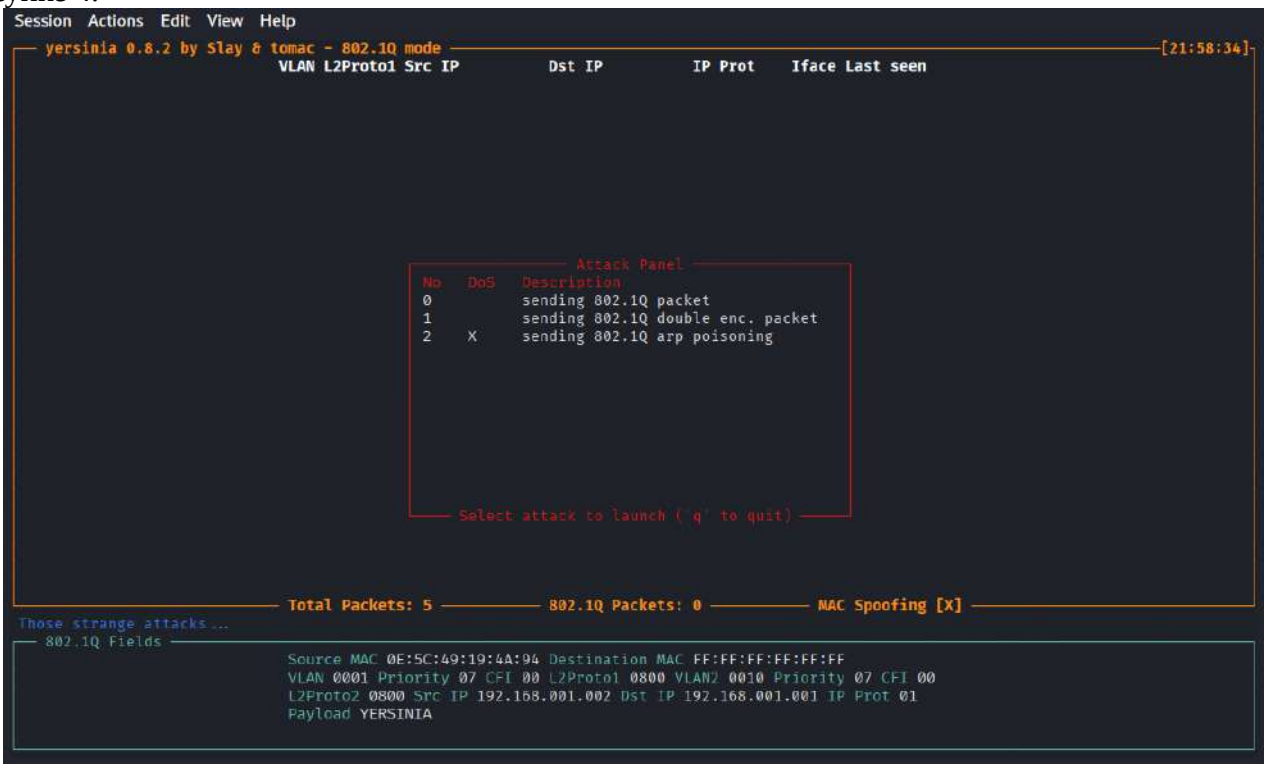

Рис. 4 Настройка полей 802.1Q в Yersinia с указанием внешнего native VLAN 1 и внутреннего целевого VLAN 10

После выполнения предыдущих шагов, мы успешно отправили один пакет, для более детального анализа отправим еще несколько пакетов. Для того, чтобы посмотреть, отправляются ли у нас пакеты, в консоли воспользуемся утилитой tcpdump (Листинг 5).

Листинг 5 – Фиксация отправки кадров с двойным тегированием на атакующем узле

```
tcpdump -i eth0 -e -v vlan
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
192.168.1.2 > 192.168.1.1: ICMP echo request, id 66, seq 66, length 16
12:41:03.112233 0e:5c:49:19:4a:94 (oui Unknown) > Broadcast, ethertype 802.1Q (0x8100), length 58: vlan 1, p 7, ethertype 802.1Q (0x8100), vlan 10, p 7, ethertype IPv4 (0x8000), (tos 0x0, ttl 64, id 66, offset 0, flags [none], proto ICMP (1), length 36)
```

Как видно из представленных данных, пакеты с двойным тегом, где внутренний — VLAN 10, а внешний VLAN 1 успешно отправляются. Теперь, воспользуемся этой же утилитой, чтобы посмотреть доходят ли пакеты до узла-жертвы.

Листинг 6 – Фиксация ICMP-трафика на узле-жертве при успешной атаке

```
tcpdump -i eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:41:03.115678 IP 192.168.1.2 > 192.168.1.1: ICMP echo request, id 66, seq 66, length 16
```

Как видно из представленных данных, пакеты успешно достигают узла-жертвы, что говорит об успешном проведении атаки. Теперь, перейдем к защите. Для этого вернемся к настройкам коммутаторов Cisco и изменим ID native VLAN на неиспользуемый 999 (Листинг 7).

Листинг 7 – Изменение native VLAN на транковом порту Cisco Catalyst 3550

```
conf t
int fa0/21
 switchport trunk native vlan 999
 exit
```

На Cisco Catalyst 2960 аналогичным образом изменим ID native VLAN на неиспользуемый 999. Теперь попробуем снова запустить атаку. Как видно на листинге 8 пакеты не доходят до жертвы, что говорит об успешной защите нашей сети от данного вида атаки.

Листинг 8 – Результат повторной атаки после изменения native VLAN

```
tcpdump -i eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
```

Теперь, проделаем данный эксперимент с коммутаторами MikroTik CRS326-24G и Eltex MES1428.

Начнём с объяснения настройки коммутатора MikroTik CRS326-24G. Создадим bridge – виртуальный коммутатор внутри MikroTik, который объединяет физические порты. И добавим к нему два порта, один из которых находится в VLAN 20 режиме access и другой в режиме trunk. Последнему мы указываем untagged для vlan-ids 1, что делает его native VLAN для этого порта. Конфигурация приведена в листинге 9.

Листинг 9 – Конфигурация VLAN на коммутаторе MikroTik CRS326

```
/int br port add interface=ether16 bridge=test
/int br port add interface=ether21 bridge=test
/int br vlan add bridge=test untagged=ether16,ether21
vlan-ids:1
/int bridge port set [find interface=ether16] pvid=1
/int bridge port set [find interface=ether21] pvid=20
/int bridge set test vlan-filtering=yes
```

Теперь перейдем к настройке коммутатора Eltex MES1428. Аналогично, создадим VLAN 10, настроим два порта, один будет в режиме access, так как ведет к конечному узлу-жертве, другой в режиме trunk. Также, у транкового порта явно укажем, что в качестве native VLAN берём VLAN 1. Конфигурация приведена в листинге 10.

Листинг 10 – Конфигурация VLAN на коммутаторе Eltex MES1428

```
conf t
```

```
vlan 1
 exit
vlan 10
 exit
int fa0/21
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
int fa0/13
 switchport mode general
 switchport general allowed vlan add 1 untagged
 switchport general pvid 1
 no shutdown
 exit
```

После настройки коммутаторов, перейдем на атакующий PC и проведем с него атаку Double Tagging с помощью утилиты Yersinia. Настройки аналогичные, что были на этапе атаки коммутаторов Cisco. Для того, чтобы посмотреть отправляются ли у нас пакеты, в консоли воспользуемся утилитой tcpdump.

Листинг 11 – Фиксация отправки кадров с двойным тегированием на атакующем узле

```
tcpdump -i eth0 -e -v vlan
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
192.168.1.2 > 192.168.1.1: ICMP echo request, id 66, seq 66, length 16
12:57:54.250734 0e:5c:49:19:4a:94 (oui Unknown) > Broadcast, ethertype 802.1Q (0x8100), length 58: vlan 1, p 7, ethertype 802.1Q (0x8100), vlan 10, p 7, ethertype IPv4 (0x8000), (tos 0x0, ttl 64, id 66, offset 0, flags [none], proto ICMP (1), length 36)
```

Как видно из представленных данных, пакеты с двойным тегом успешно отправляются. Также на ПК-жертве посмотрим доходят ли до него пакеты.

Листинг 12 – Фиксация ICMP-трафика на узле-жертве при успешной атаке

```
tcpdump -i eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:57:54.251167 IP 192.168.1.2 > 192.168.1.1: ICMP echo request, id 66, seq 66, length 16
```

Как видно из представленных данных, пакеты успешно достигают узла-жертвы, что говорит об успешном проведении атаки. Теперь, перейдем к защите. Для этого вернемся к настройкам коммутаторов и изменим ID native VLAN на неиспользуемый 999. Настройка MikroTik CRS326-24G приведена на листинге 13.

Листинг 13 – Изменение native VLAN на коммутаторе MikroTik CRS326

```
/interface bridge vlan set [find vlan-ids 1] vlan-ids=999 untagged=ether16,ether21
```

Таким образом, в конфигурации коммутатора MikroTik идентификатор нативной VLAN был изменён со стандартного значения «1» на неиспользуемый «999» для минимизации рисков, связанных с использованием стандартного нативного VLAN. Порт ether16 сконфигурирован как нетегированный (untagged) для VLAN 999, выполняя роль транкового порта (trunk), который передаёт трафик с соответствующими тегами VLAN. Аналогичная процедура была применена к коммутатору Eltex MES1428, где ID нативной VLAN также был заменён на неиспользуемый — 999. Соответствующие настройки для устройства Eltex представлены на листинге 14.

Листинг 14 – Изменение native VLAN на коммутаторе Eltex MES1428

```
int fa0/13
 switchport general pvid 999
 switchport general allowed vlan add 999 untagged
 exit
```

Теперь попробуем снова запустить атаку, но теперь как видно из листинга 15 пакеты не доходят до жертвы, что говорит об успешной защите нашей сети от данного вида атаки.

Листинг 15 – Результат повторной атаки после изменения native VLAN

```
tcpdump -i eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

```
^C
0 packets captured
```

Результаты исследования

Необходимо понять, как именно работает атака Double Tagging: атакующий узел, находящийся в VLAN 20, с помощью инструмента Yersinia отправляет сформированные кадры Ethernet с двойным тегированием 802.1Q. При этом первый (внешний) тег соответствует native VLAN на транковом порту коммутатора (по умолчанию VLAN 1), а второй (внутренний) тег указывает на целевой VLAN (VLAN 10). Первый коммутатор, получив такой кадр с порта доступа, пересылает его на транк, где удаляет внешний тег, так как он совпадает с native VLAN. Следующее устройство получает кадр с единственным тегом VLAN 10 и, считая его легитимным, перенаправляет в целевой сегмент сети.

В процессе тестирования на всех коммутаторах при конфигурации по умолчанию (native VLAN = 1 на транковых портах) атака Double Tagging была успешно реализована. На узле-жертве, расположенном в изолированном VLAN 10, с помощью анализатора трафика tcpdump был зафиксирован ICMP-трафик, отправленный атакующим узлом из VLAN 20. Это прямое доказательство того, что граница логической сегментации была преодолена.

Наиболее эффективной мерой защиты от атаки Double Tagging, проверенной в ходе эксперимента, является изменение идентификатора native VLAN на транковых портах с используемого по умолчанию (VLAN 1) на неиспользуемый (например, VLAN 999). После применения этой настройки на всех тестируемых коммутаторах повторная попытка проведения атаки завершилась неудачей: сформированные кадры с двойным тегом более не достигали узла-жертвы, так как первый коммутатор больше не удалял внешний тег при отправке по транку.

Таким образом, результаты наглядно демонстрируют, что типовая конфигурация оборудования различных производителей не обеспечивает защиту от атаки Double Tagging, однако простая корректировка настройки native VLAN является универсальным и высокоэффективным методом защиты.

Заключение

В рамках исследования был проведён эксперимент, направленный на изучение уязвимости стандартных конфигураций коммутаторов различных вендоров к атаке типа VLAN Hopping (метод Double Tagging). На специализированном тестовом стенде с использованием реального оборудования (Cisco, Eltex, MikroTik) была успешно смоделирована атака с применением инструмента Yersinia. В ходе эксперимента осуществлялся мониторинг сетевого трафика и анализ поведения оборудования, что позволило на практике подтвердить возможность обхода логической изоляции VLAN.

Результат проверки гипотез:

1. Гипотеза H1 подтвердилась полностью. Экспериментально установлено, что типовая конфигурация протестированных коммутаторов (Cisco Catalyst 2960, Eltex MES1428, MikroTik CRS326) является уязвимой к атаке Double Tagging. При стандартных настройках, когда на транковых портах используется native VLAN по умолчанию (VLAN 1), оборудование не препятствует отправке кадров с двойным тегированием, что позволяет злоумышленнику успешно передавать трафик между логически изолированными VLAN.
2. Гипотеза H2 подтвердилась полностью. Разработанная и применённая методика практической демонстрации атаки Double Tagging на реальном сетевом оборудовании показала высокую наглядность и эффективность. Простота воспроизведения атаки в сочетании с убедительностью полученных результатов (прямой перехват трафика между VLAN) делает данную методику ценным инструментом для наглядного представления внутренних угроз информационной безопасности. Это открывает перспективы её использования в учебном процессе для подготовки специалистов.

Направления дальнейшего исследования: разработка автоматизированных систем обнаружения атак VLAN Hopping, анализ устойчивости современных протоколов сетевой виртуализации и программно-определяемых сетей (SDN) к атакам обхода сегментации на канальном

уровне, изучение новых векторов атак, связанных с IPv6 и современными протоколами сетевой виртуализации.

Проведённое исследование подтвердило, что атака VLAN Hopping, реализуемая методом Double Tagging, остается актуальной угрозой, корень которой лежит в ошибках базовой конфигурации, а не в недостатках оборудования. Полученные результаты имеют практическую ценность для системных администраторов и специалистов по безопасности, демонстрируя критическую важность даже простых, но правильных настроек для обеспечения надёжной защиты сетевой инфраструктуры.

Библиографический список

1. 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: 15.12.2025).
2. Cisco Systems, Inc. Understanding and Configuring VLAN Trunk Protocol (VTP) // Cisco Technical Documentation. – 2023. – URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swvtp.html (дата обращения: 15.12.2025).
3. 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. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/135231.html (дата обращения: 13.12.2025).
4. Convery, S. Hacking Layer 2: Fun with Ethernet Switches // Black Hat USA 2002. – 2002. – URL: https://blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (дата обращения: 11.12.2025).
5. Knobbe, F. VLAN Security // SANS Institute InfoSec Reading Room. – 2002. – URL: https://www.sans.org/reading-room/whitepapers/protocols/vlan-security-853 (дата обращения: 12.12.2025).
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: 12.12.2025)
7. MikroTik Documentation. VLAN Security and Bridge Filtering // MikroTik Official Documentation. – 2024. – URL: https://help.mikrotik.com/docs/display/ROS/VLAN (дата обращения: 14.12.2025).

References

1. IEEE Standards Association. *IEEE Standard 802.1Q-2018 — Bridges and Bridged Networks* [Electronic resource]. IEEE Standards Association, 2018. URL: https://standards.ieee.org/standard/802_1Q-2018.html (access date: 15.12.2025).
2. Cisco Systems, Inc. Understanding and Configuring VLAN Trunk Protocol (VTP) // *Cisco Technical Documentation*. 2023. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swvtp.html (access date: 15.12.2025).
3. Uymin, A. G. *Computer Networks. Layer 2 Technologies: Practical Guide for Secondary Vocational Education*. Saratov; Moscow: Profobrazovanie, IPR Media, 2024. 190 p. ISBN 978-5-4497-2559-2. Electronic resource. URL: https://www.iprbookshop.ru/135231.html (access date: 13.12.2025).
4. Convery, S. Hacking Layer 2: Fun with Ethernet Switches // *Proceedings of Black Hat USA 2002*. 2002. URL: https://blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (access date: 11.12.2025).
5. Knobbe, F. VLAN Security // *SANS Institute InfoSec Reading Room*. 2002. URL: https://www.sans.org/reading-room/whitepapers/protocols/vlan-security-853 (access date: 12.12.2025).

6. SANS Institute. Network Penetration Testing Survey 2023 [Electronic resource] // *SANS Survey Report*. 2023. URL: https://www.sans.org/reading-room/whitepapers/survey/network-penetration-testing-survey-2023-39845 (access date: 12.12.2025).
7. MikroTik. VLAN Security and Bridge Filtering // *MikroTik Official Documentation*. 2024. URL: https://help.mikrotik.com/docs/display/ROS/VLAN (access date: 14.12.2025).

Информация об авторах

Хорошилов Лев Геннадьевич — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: levyahorosh@yandex.ru

Костин Никита Андреевич — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: knikita200558@mail.ru

ANALYSIS OF PROTECTION EFFECTIVENESS AGAINST DOUBLE TAGGING ATTACKS IN HETEROGENEOUS NETWORK ENVIRONMENTS (CISCO, MIKROTIK, ELTEX)

Khoroshilov L. G.[1], Kostin N. A.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. This paper presents a practical analysis of a VLAN Hopping attack implemented using the Double Tagging technique, which allows attackers to bypass the logical isolation of virtual local area networks based on the IEEE 802.1Q standard. The study examines architectural characteristics of VLAN technology related to native VLAN processing on trunk ports of Ethernet switches that create conditions for exploiting Layer 2 vulnerabilities. The mechanism of forming Ethernet frames with double 802.1Q tagging is described in detail, along with the frame forwarding logic that allows such packets to be delivered into a target VLAN segment without authorization.

The experimental part of the research was conducted on a dedicated testbed using real network equipment from multiple vendors, including Cisco, MikroTik, and Eltex. This heterogeneous environment allows evaluation of device behavior under identical attack conditions. The Yersinia utility was used to generate Ethernet frames with double tagging, while network traffic was captured and analyzed using the tcpdump tool to confirm successful delivery of traffic to a protected VLAN segment.

The study compares device behavior under default configurations and after applying standard security countermeasures. The results demonstrate that the default native VLAN configuration on trunk ports makes network infrastructures vulnerable to Double Tagging attacks regardless of the equipment vendor. Based on the experimental findings, practical recommendations for improving VLAN-based network segmentation security are proposed, including assigning a non-default native VLAN, explicitly configuring port modes, and disabling automatic trunk negotiation mechanisms. The research highlights the critical importance of correct Layer 2 configuration practices for ensuring secure segmentation in modern heterogeneous network environments.

Keywords: VLAN Hopping, Double Tagging, Network Security, Penetration Testing, native VLAN, IEEE 802.1Q, Network Segmentation.

Information about the authors

Khoroshilov Lev Gennadievich — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: levyahorosh@yandex.ru

Kostin Nikita Andreevich — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: knikita200558@mail.ru