УДК 004.056.53

Ткаченко Андрей Вячеславович
студент
2 курса, факультета «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва

Отмахова Елизавета Павловна
студент
2 курса, факультета «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва

АТАКА ROOT HIJACKING. МЕТОДИКИ ТЕСТИРОВАНИЯ И ЗАЩИТЫ

Аннотация: В статье рассматриваются методики тестирования и защиты атаки Root Hijacking на трёх физических коммутаторах под управлением отечественной операционной системы «Альт». Исследование проводится на физическом оборудовании. Для оптимизации использования ресурсов реализована схема прямого соединения двух коммутаторов и параллельно подключённого к ним третьего, где каждый выполняет ключевую роль в поддержании сети. Приводятся результаты экспериментов по проверке функциональности и устойчивости созданной сети при воздействии Root Hijacking, а также описаны предложенные меры по обеспечению её безопасности и устойчивости к данной атаке.

Ключевые слова: Root Hijacking, BPDU, STP, RSTP, корневой коммутатор, ОС Альт, PortFast, Root Guard, защита сети, BPDU Guard, топология сети, сетевой трафик, Scapy, Yersinia.

ROOT HIJACKING ATTACK. TESTING AND PROTECTION METHODS

Tkachenko Andrey Vyacheslavovich
student
2nd year, Faculty of "Integrated Safety of the Fuel and Energy Complex"
Gubkin Russian State University of Oil and Gas (NIU)
Russia, Moscow

Otmakhova Elizaveta Pavlovna
student
2nd year, Faculty of "Integrated Safety of the Fuel and Energy Complex"
Gubkin Russian State University of Oil and Gas (NIU)
Russia, Moscow

Abstract: The article examines methodologies for testing and protecting against the Root Hijacking attack on three physical switches running the domestic operating system "Alt". The study is conducted on physical hardware. To optimize resource usage, a direct connection scheme between the two switches is implemented, where each plays a key role in maintaining the network. The results of experiments verifying the functionality and stability of the created network under the influence of Root Hijacking are presented, as well as proposed measures to ensure its security and resilience to this attack.

Keywords: Root Hijacking, BPDU, STP, RSTP, root bridge, Alt OS, PortFast, Root Guard, network protection, BPDU Guard, network topology, network traffic, Scapy, Yersinia.

Введение

Актуальность

В настоящее время сетевая архитектура операторов связи и крупных предприятий не может функционировать без реализации технологий, обеспечивающих безопасность, масштабируемость и изоляцию передачи сетевого

трафика. Атака Root Hijacking представляет собой угрозу безопасности на уровне канального протокола STP, при которой злоумышленник может захватить роль корневого коммутатора, нарушая тем самым топологию сети. Эта атака используется для перехвата и перенаправления сетевого трафика с целью получения несанкционированного доступа, нарушения работы или прослушивания передачи данных. Root Hijacking воздействует на передачу BPDU-пакетов, изменяя логику выбора корневого моста в сети, что может привести к дестабилизации маршрутизации и нарушению изоляции трафика. Защита от таких атак реализуется средствами PortFast, Root Guard, BPDU Guard и другими функциями, обеспечивающими правильность и безопасность топологии сети.

В контексте активного развития импортозамещения и технологического суверенитета критически важным становится анализ защищенности отечественных программных платформ от современных сетевых угроз. Операционная система «Альт», как ключевой элемент реестра российского ПО, должна демонстрировать устойчивость к сложным атакам на сетевую инфраструктуру, включая атаки подмены корневого моста в STP-протоколах.

Объект, предмет, цель

Объект исследования: процесс реализации и нейтрализации атак подмены корневого моста (Root Hijacking) в сетях на основе протокола Spanning Tree Protocol (STP).

Предмет исследования: функциональные возможности и эффективность инструментов с открытым исходным кодом (Scapy, Yersinia) для проведения атаки Root Hijacking в среде операционной системы «Альт».

Цель исследования: разработка и экспериментальная проверка методики проведения и защиты атаки Root Hijacking на базе ОС «Альт» с последующей оценкой уязвимости сетевой инфраструктуры.

Обзор и методология исследования

Литературный обзор

Атака Root Hijacking относится к типу кибератаки, которая нацелена на протокол Spanning Tree Protocol (STP), используемый в сетях для предотвращения

петель и обеспечения надежности топологии сети. STP выбирает специальный корневой коммутатор (root bridge), который является центральным узлом в сети и через который проходит основной трафик.

Актуальность исследования атаки Root Hijacking обусловлена критической важностью безопасности канального уровня в корпоративных и операторских сетях, где протокол Spanning Tree Protocol (STP) обеспечивает отказоустойчивость и предотвращение петель. В условиях роста сложности сетевых инфраструктур и увеличения числа угроз, способность злоумышленника перехватывать роль корневого моста представляет серьезную угрозу доступности сетевых сервисов. В 2007 году в книге «**LAN Switch Security: What Hackers Know About Your Switches» авторы Eric Vyncke и Christopher Paggen** детально описали механизмы атак на STP, включая Root Hijacking, а также методы защиты (BPDU Guard, Root Guard). Это произведение раскрыло уязвимости коммутационных инфраструктур и стало основой для современных систем сетевой безопасности. **Работа «Computer Networking: A Top-Down Approach» Куроса и Росса** рассказывает, как атаки канального уровня влияют на вышележащие уровни сетевой модели OSI, что важно для оценки воздействия Root Hijacking на сетевые сервисы. Для тестирования и анализа результатов значение имеет книга «**Python for Network Engineers» Натании Трауба**, которая детализирует использование библиотеки Scapy для создания инструментов сетевой безопасности и диагностики.

В текущем исследовании атака Root Hijacking рассматривается на практике, однако следует отметить, что на сегодняшний день отсутствует отдельный RFC или официальный стандарт, посвящённый именно атаке Root Hijacking. Тем не менее, данная атака связана с уязвимостями в работе протоколов Spanning Tree Protocol (STP) и Rapid Spanning Tree Protocol (RSTP), которые регламентируются стандартами IEEE:

- IEEE 802.1D — Стандарт протокола Spanning Tree Protocol (STP)
- IEEE 802.1w — Стандарт протокола Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1Q — Стандарт VLAN и обработки тегированных кадров в сети

Также, вопросы сетевой безопасности и защиты от атак типа "hijacking" рассматриваются в таких документах, как:

- RFC 4949 — Internet Security Glossary, Version 2 (ограниченное описание hijacking-атак)
- RFC 3552 — Guidelines for Writing RFC Text on Security Considerations (рекомендации по безопасности)

Поскольку атака Root Hijacking по сути является подделкой BPDU и попыткой переопределения ролей корневого моста, её защита опирается на механизмы, предусмотренные в данных стандартах, и реализацию специальных функций безопасности на сетевом оборудовании (Root Guard, BPDU Guard, PortFast).

Основные гипотезы исследования:

- **Гипотеза о реализуемости:** Стандартный сетевой стек ОС «Альт» в связке с инструментами типа Scapy обладает всей необходимой функциональностью для проведения успешной атаки Root Hijacking в коммутируемой сети Ethernet.
- **Гипотеза об эффективности:** Атака Root Hijacking способна привести к изменению топологии Spanning Tree и перехвату роли корневого моста в разумные сроки на коммутационном оборудовании.
- **Гипотеза о детектировании:** Стандартные инструменты мониторинга ОС «Альт» (wireshark) позволяют зафиксировать факт успешной атаки и ее воздействие на сетевую инфраструктуру.
- **Гипотеза о защитных механизмах:** Стандартные механизмы защиты (BPDU Guard, Root Guard) на коммутаторах эффективно блокируют атаку Root Hijacking при их корректной настройке.

Методы исследования

Тип исследования: экспериментальное тестирование атаки Root Hijacking с использованием ОС «Альт» в контролируемой лабораторной среде.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая физические коммутаторы Eltex mes1428, Mikrotik и 2960si, а также два

PC. На двух PC установлена операционная система Альт Линукс, на атакующем PC установлен PyCharm Community Edition 2024.2.4. с библиотекой Scapy.

Методы сбора данных:

- Мониторинг BPDU-трафика с использованием Wireshark для захвата и анализа кадров Spanning Tree Protocol
- Анализ логических данных коммутаторов для документирования реакции оборудования на атаку
- Измерение временных параметров с помощью скриптового мониторинга времени отклика и продолжительности атаки
- Верификация изменения топологии через команду показа spanning-tree (show spanning-tree)

Процедура проведения исследования:

1. **Подготовка тестовой среды:** настройка коммутаторов с STP, конфигурация базовых VLAN, проверка исходной топологии spanning tree
2. **Подготовка инструментов атаки:** установка и настройка ПО для проведения атаки (Scapy) на ОС «Альт», написание скриптов генерации BPDU-пакетов
3. **Проведение атаки:** выполнение Root Hijacking, мониторинг реакции сети
4. **Анализ результатов:** оценка эффективности атаки, времени до смены root bridge, влияния на сетевую производительность, тестирование защитных механизмов

Основные моменты экспериментального исследования

Лабораторная среда эксперимента

Разберемся с тем, что из себя представляет атака Root Hijacking и какие компоненты необходимы для её тестирования. Root Hijacking — это тип атаки на канальном уровне модели OSI, которая направлена на компрометацию протокола Spanning Tree Protocol (STP). Злоумышленник отправляет поддельные BPDU-пакеты с более высоким приоритетом, чтобы стать корневым мостом в сети. Это позволяет перехватывать сетевой трафик, вызывать отказы в обслуживании и проводить атаки.

Принцип работы атаки следующий:

- Атакующая система генерирует BPDU-кадры с наивысшим приоритетом (наименьшим числовым значением)
- Эти кадры отправляются на multicast-адрес 01:80:C2:00:00:00, используемый STP
- Коммутаторы в сети, получившие поддельные BPDU, пересчитывают spanning tree
- Атакующий узел становится новым корневым мостом
- Весь трафик начинает проходить через атакующую систему

Для успешного проведения атаки необходимы следующие компоненты лабораторной среды:

- Минимум два коммутатора с поддержкой STP
- Атакующая система под управлением ОС «Альт»
- Средства мониторинга (Wireshark)
- Сетевое оборудование для анализа реакции защиты (BPDU Guard, Root Guard)

Особенность данной атаки заключается в том, что она эксплуатирует принцип работы STP — выбор корневого моста на основе приоритета, что делает её эффективной против любого оборудования, поддерживающего этот протокол.

Топология сети

Эксперимент был проведён с устройствами в роли L2 коммутатора, поддерживающего trunk-порты. На рисунке 1 представлена используемая топология сети.

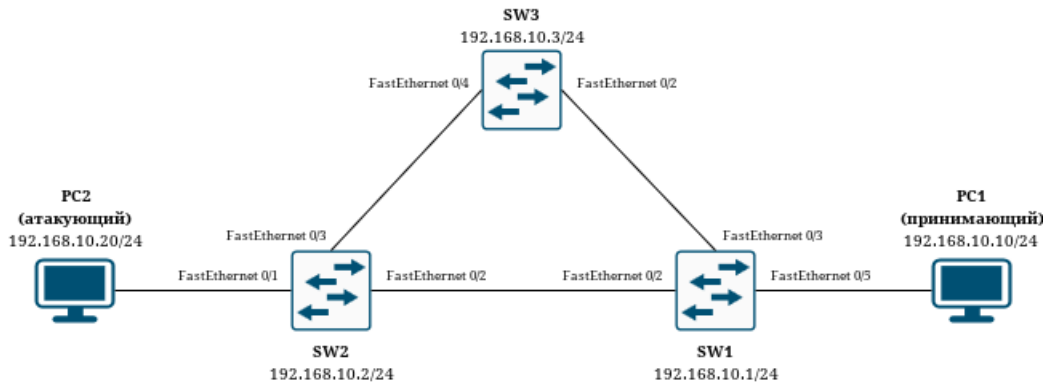

Рисунок 1. Топология сети для эксперимента

Далее мы будем с ней работать. В следующем пункте представлена настройка всех машин.

Подготовка и конфигурация машин

1. Подготовим оборудование, а именно:

- Коммутаторы: Cisco 2960si, Eltex mes1428, Mikrotik.
- ПК2 (атакующий) — Linux с интерфейсом eth0.
- ПК1 (принимающий) — любая ОС с интерфейсом eth0.
- Кабели: Ethernet для подключения ПК к коммутаторам.

2. Произведем настройку оборудования.

2.1. Подключаем ПК2 злоумышленника к порту коммутатора Cisco 2960si. Соединяем коммутаторы Cisco 2960si и Eltex mes1428, Mikrotik транком. Подключаем принимающий ПК1 к коммутатору Eltex mes1428. Команды, используемые в ходе настройки представлены ниже.

Таблица 1.

Настройка коммутаторов

Eltex mes1428	**Cisco 2960si**	**Mikrotik**
enable configure terminal vlan 10 exit interface Fa 0/5 switchport mode access	enable configure terminal vlan 10 exit interface FastEthernet0/1 switchport mode access	/interface bridge add name= bridge1 vlan-filter- ing=yes /interface bridge port add bridge= bridge1 inter- face=ether2

switchport access vlan 10 no shutdown exit interface Fa 0/2 switchport mode general switchport general allowed vlan add 10 switchport general pivd 10 no shutdown exit interface Fa 0/3 switchport mode general switchport general allowed vlan add 10 switchport general pivd 10 no shutdown exit interface vlan 10 ip address 192.168.10.1 255.255.255.0 no shutdown exit spanning-tree priority 4096 end write memory	switchport access vlan 10 no shutdown exit interface FastEthernet0/2 switchport mode trunk no shutdown exit interface FastEthernet0/3 switchport mode trunk no shutdown exit interface vlan 10 ip address 192.168.10.1 255.255.255.0 no shutdown exit spanning-tree vlan 10 priority 8192 end write memory	/interface bridge port add bridge= bridge1 inter- face=ether4 /interface bridge vlan add bridge= bridge1 tagged=ether2, ether4 vlan-ids=10 /interface bridge set bridge1 protocol- mode=stp /interface bridge set bridge1 priority=8192 ip address add ad- dress=192.168.10.3/24 in- terface=bridge1

Используем Wireshark для отслеживания трафика на ПК злоумышленника и жертвы. С помощью программы PyCharm Community Edition 2024.2.4. с установленной библиотекой Scapy напишем программу для формирования поддельных BPDU-пакетов. Цель — совершить атаку Root Hijacking, сделать коммутатор Cisco 2960si

корневым. После запустим написанную программу и отправим поддельные BPDU пакеты на с адреса 192.168.10.20 атакующего ПК2 на принимающий ПК1 с адресом 192.168.10.10.

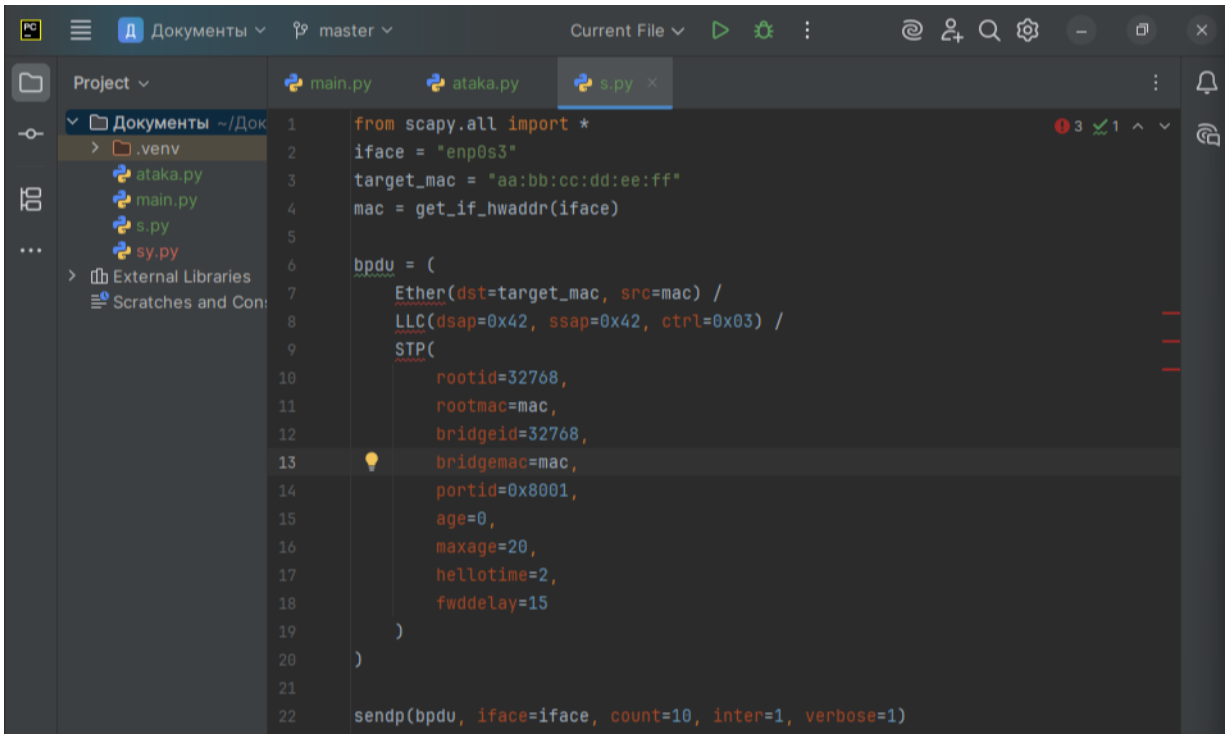

Рисунок 2. Код программы для формирования поддельных BPDU пакетов

Методы защиты от атаки на коммутаторе Cisco 2960si:

1. Включение функции Root Guard на портах, к которым подключены конечные устройства (потенциальные источники атаки).

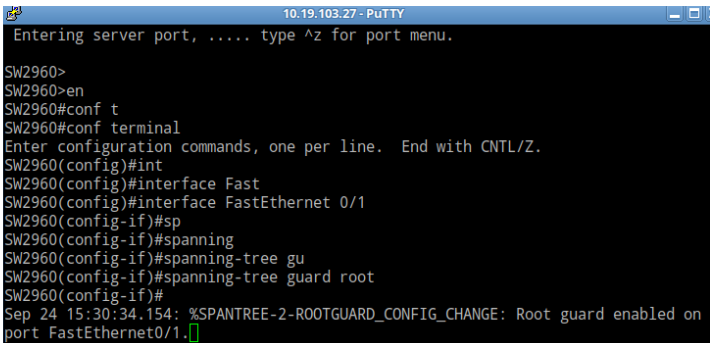

Рисунок 3. Метод №1

2. Включение BPDU Guard на портах доступа (access ports), чтобы отключить порт при получении BPDU.

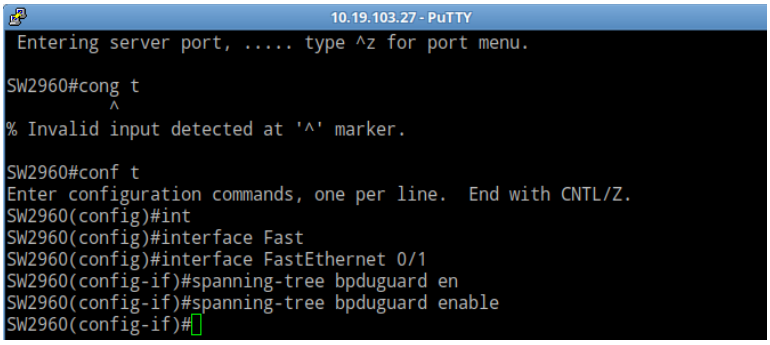

Рисунок 4. Метод №2

3. Для портов, подключенных к конечным устройствам, включается PortFast для быстрой активации порта без ожидания протоколов STP.

Рисунок 5. Метод №3

4. Также для снижения временного интервала, в течение которого может успешно нарушить топологию, повышения общей безопасности и устойчивости сети можно включить RSTP

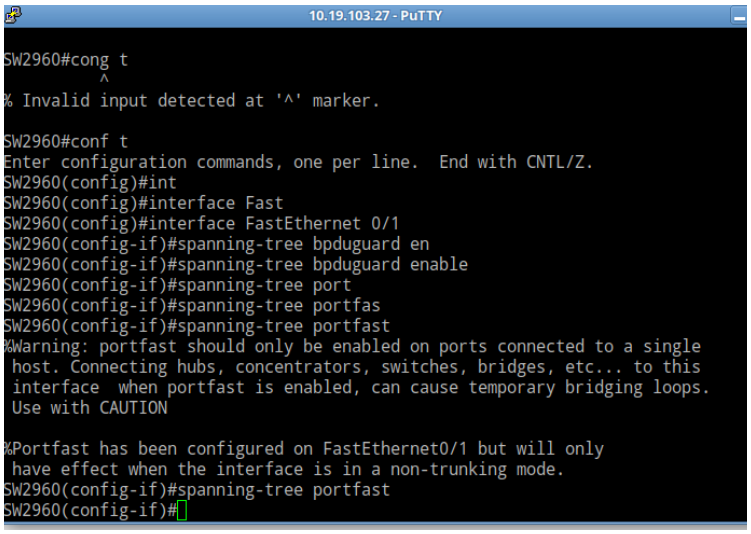

Рисунок 6. Метод №4

Методы защиты от атаки на коммутаторе Mikrotik:

1. По аналогии включим те же методы что и на Cisco 2960si.

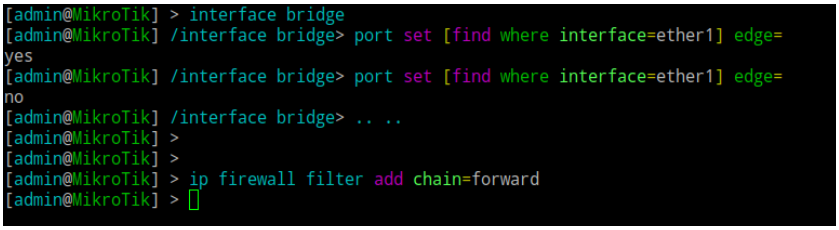

Рисунок 7. Настройка методов защиты на Mikrotik

Методы защиты от атаки на коммутаторе Eltex mes1428:

1. По аналогии включим те же методы что и на Cisco 2960si.

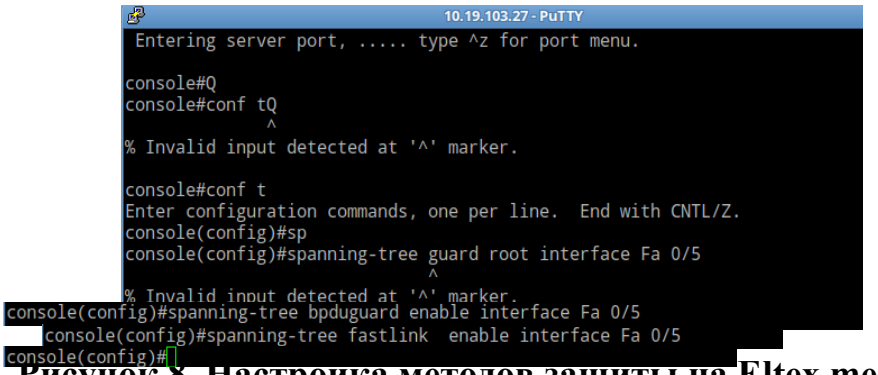

Рисунок 8. Настройка методов защиты на Eltex mes1428

Таблица 2.

Описание методов защиты

Метод	**Команда**	**Значение**
Root Guard	interface <порт> spanning-tree guard root	Позволяет блокировать прием BPDU с возможностью назначения роли корня с этих портов.
BPDU Guard	interface <порт> spanning-tree bpduguard enable	Предотвращает появление нежелательных коммутаторов и подделки BPDU.
PortFast	interface <порт> spanning-tree portfast	Вместе с BPDU Guard повышает защиту от атак.
RSTP	interface <порт> spanning-tree mode rapid-pvst	Снижение временного интервала, в течение которого может успешно нарушить топологию, повышает общую безопасность и устойчивость сети.

Мониторинг и логирование	show spanning-tree	Непрерывный мониторинг состояния STP, Логирование изменений корня и аномалий в топологии.

Результаты исследования

В ходе исследования была выполнена атака типа Root Hijacking на базе ОС «Альт» и на коммутаторах Cisco, Eltex, Mikrotik. Для атаки был использован способ создания поддельных BPDU-пакетов, реализованный на языке Python при помощи библиотеки Scapy. Стоит отметить, что в качестве альтернативы был рассмотрен инструмент Yersinia, однако мы были вынужденны отказаться от него из-за несовместимости программы с использованной нами ОС «Альт» 10.4. При помощи созданных BPDU-пакетов с более низким приоритетом удалось изменить корневой коммутатор. Без использования методов защиты топология, построенная с помощью двух персональных компьютеров и коммутаторов Cisco, Eltex, Mikrotik, успешно поддаётся атаке.

Для противодействия атаке были протестированы следующие методы защиты:

1) Включение функций Bridge и BPDU Guard на коммутаторах.

2) Использование настройки PortFast.

3) Активирование протокола Rapid Spanning Tree Protocol (RSTP).

4) Ручной мониторинг трафика с помощью анализатора пакетов Wireshark.

Ниже, на рисунках 11-13, можно увидеть, как в Wireshark выглядят основные этапы работы.

1. Правильная работа STP.

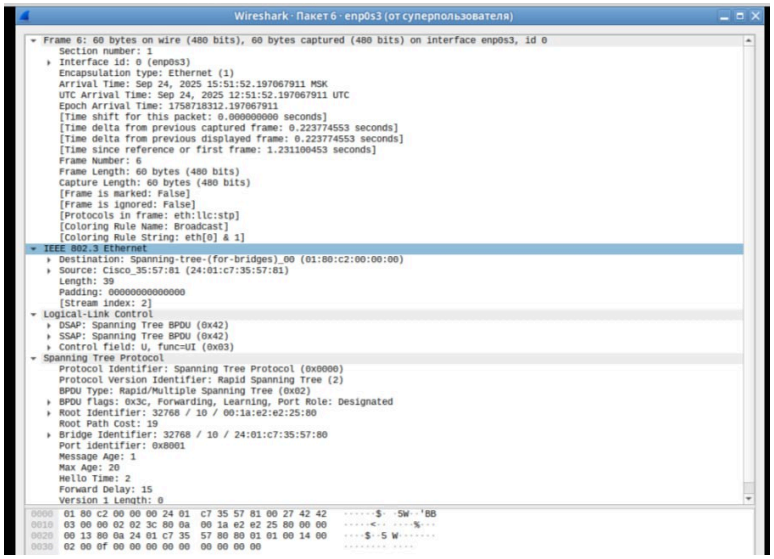

Рисунок 9. Работа STP

2. Атака Root Hijacking.

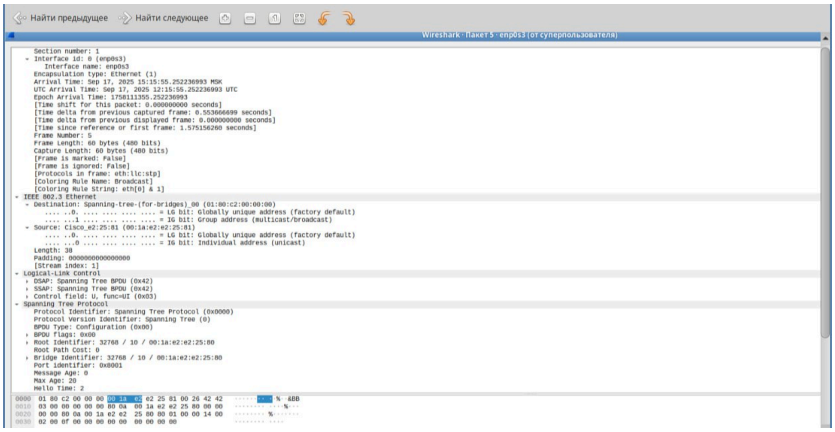

Рисунок 10. Атака Root Hijacking.

3. Атака Root Hijacking при настроенной защите.

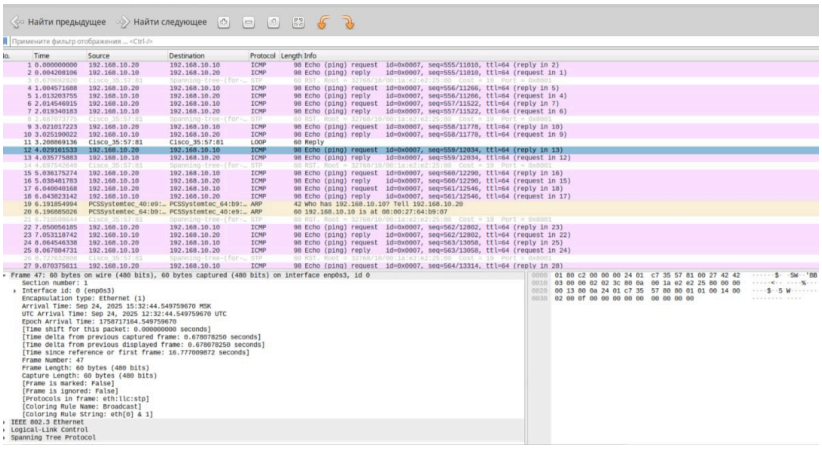

Рисунок 11. Неудавшаяся попытка атаки

После проведения каждого из описанных методов была совершена проверка содержимого файлов с помощью Wireshark и был осуществлён просмотр состояния

коммутатора. Все методы подтвердили свою работоспособность против описанной нами атаки.

Анализ содержимого файлов

1.До атаки (рисунок9)

- Стабильная работа сети
- STP трафик: стабильные BPDU пакеты
- Multicast адрес: 01:80:c2:00:00:00 (нормальный STP)
- Состояние: Сеть стабильна, топология определена

2. Во время атаки (рисунок10)

- Появились поддельные BPDU с нашим MAC адресом
- Изменение Root Bridge: наш MAC стал root
- Path Cost: коммутатор показывает стоимость пути 19 до нашего устройства
- Признаки успеха: Root Identifier: 0 / Your:mac:ad:dr, коммутатор принял наши BPDU

3. После блокировки (рисунок11)

- Атака заблокирована системой защиты
- Восстановление нормальной работы:
  - ICMP ping: 192.168.10.20 ↔ 192.168.10.10 (нормальный обмен)
  - ARP запросы: Разрешение MAC адресов
  - STP восстановил оригинальную топологию

Заключение

Исследование показало, что топология, включающая коммутаторы Cisco, Eltex, Mikrotik уязвима к атаке Root Hijacking, что подчёркивает важность применения мер защиты. Методы Bridge и BPDU Guard, PortFast, а также RSTP подтвердили свою работоспособность в противодействии данной атаке. Метод ручного мониторинга трафика рассматриваем как возможный способ выявления атак, однако считаем его неэффективным из-за необходимости постоянного мониторинга и риска пропуска

злоумышленных пакетов в условиях большой сетевой нагрузки или сложной топологии

Использованные источники

1. 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: 2.04.2025)
2. Vyncke E., Paggen C. LAN Switch Security: What Hackers Know About Your Switches [Электронный ресурс] / E. Vyncke, C. Paggen. – Cisco Press, 2007. – 312 с. – Режим доступа: https://www.ciscopress.com/9781587052569 – Загл. с экрана. – ISBN 978-1587052569. – (дата обращения: 11.04.2025).
3. Kerrisk M. The Linux Programming Interface: A Linux and UNIX System Programming Handbook [Электронный ресурс] / M. Kerrisk. – No Starch Press, 2010. – 1552 с. – Режим доступа: https://nostarch.com/linuxprogramming – Загл. с экрана. – ISBN 978-1593272203. – (дата обращения: 15.04.2025).
4. Traub N. Python for Network Engineers [Электронный ресурс] / N. Traub. – Independently published, 2021. – 298 с. – Режим доступа: https://www.pythonfornetworkengineers.com – Загл. с экрана. – ISBN 979-8745422397. – (дата обращения: 23.04.2025).
5. Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach [Электронный ресурс] / J.F. Kurose, K.W. Ross. – 8-е изд. – Pearson, 2020. – 848 с. – Режим доступа: https://www.pearson.com/networking – Загл. с экрана. – ISBN 978-0135928615. – (дата обращения: 2.05.2025).
6. Clark K., Hamilton K. Cisco LAN Switching [Электронный ресурс] / K. Clark, K. Hamilton. – Cisco Press, 1999. – 500 с. – Режим доступа: https://www.ciscopress.com/lan-switching – Загл. с экрана. – ISBN 978-1578700940. – (дата обращения: 12.05.2025).
7. McNab C. Network Security Assessment: Know Your Network [Электронный ресурс] / C. McNab. – 3-е изд. – O'Reilly Media, 2016. – 514 с. – Режим доступа: https://www.oreilly.com/library/view/network-security-assessment – Загл. с экрана. – ISBN 978-1491910955. – (дата обращения: 7.06.2025).

8. Scapy Documentation [Электронный ресурс] // Scapy.net – 2024. – URL: https://scapy.net/documentation/ (дата обращения: 19.06.2025)

9. FRRouting Documentation [Электронный ресурс] // FRRouting.org – 2024. – URL: https://docs.frrouting.org/ (дата обращения: 28.06.2025)

10. RFC 4949 — Internet Security Glossary, Version 2 [Электронный ресурс] // IETF – 2006. – URL: https://datatracker.ietf.org/doc/html/rfc4949 (дата обращения: 30.09.2025).

11. RFC 3552 — Guidelines for Writing RFC Text on Security Considerations [Электронный ресурс] // IETF – 2002. – URL: https://datatracker.ietf.org/doc/html/rfc3552 (дата обращения: 30.09.2025).