УДК 004.725.5

Стрельцов Д.С
Бутенко Е.А
студенты специалитета
Российский государственный университет нефти и газа (НИУ) имени И.М Губкина, г.Москва

VLAN ID ENUMERATION. МЕТОДЫ ЗАЩИТЫ.

Аннотация: Статья посвящена анализу методов защиты при использовании VLAN (Virtual Local Area Network). Рассматриваются основные угрозы безопасности, связанные с управлением VLAN, а также способы их минимизации. Особое внимание уделено методам защиты от атак, использующих подмену тегов и перехват данных. Представлены разные подходы к защите и предложены рекомендации по предотвращению атак и повышению устойчивости сетей к угрозам.

Ключевые слова: VLAN, атака, защита, VLAN_ID

UDC 004.725.5

Streltsov D. S.
Butenko E.A.
students of the specialty
Gubkin Russian State University of Oil and Gas, Moscow

VLAN ID ENUMERATION. PROTECTION METHODS.

Abstract: The article is devoted to the analysis of protection methods when using VLAN (Virtual Local Area Network). The main security threats related to VLAN management are considered, as well as ways to minimize them. Special attention is paid to methods of protection against attacks using tag substitution and data interception. Different approaches to protection are presented and

recommendations for preventing attacks and increasing the resilience of networks to threats are proposed.

Key words: VLAN, attack, protection, VLAN_ID

ВВЕДЕНИЕ

С развитием технологий виртуализации и сегментации сетевой инфраструктуры с использованием VLAN, проблема обеспечения безопасности становится все более важной. VLAN позволяет разделить физическую сеть на несколько логических сегментов, что помогает улучшить управление трафиком, повысить безопасность и снизить нагрузку на сеть. Однако, несмотря на множество преимуществ, VLAN создаёт новые возможности для атак, с помощью которого злоумышленники могут выявить все существующие VLAN в сети. Тема защиты от атак с использованием остаётся актуальной для обеспечения безопасности в современных сетях, что делает её важной как для теоретического изучения, так и для практического применения в реальных условиях.

Стоит сразу отметить, что использование VLAN возможно только на управляемых коммутаторах. VLAN служат для эффективного разделения сетей, что приводит к возникновению определенного идентификатора, используемого для маркировки трафика различных подсетей на коммутаторе. Для этой цели применяется стандарт 802.1q, который определяет процедуру маркировки или тегирования кадров.

Объект исследования: Сетевые инфраструктуры, использующие VLAN (в данной статье рассмотрены коммутаторы cisco, eltex, mikrotik).

Предмет исследования: Методы защиты VLAN от угроз и атак.

Цель исследования: Разработка рекомендаций и анализ методов защиты по обеспечению безопасности при использовании VLAN.

IEEE 802.1Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. В кадр Ethernet вставляется маркер (tag), в котором указывается идентификатор VLAN, принимающий значение от 1 до 4094 (номера 0 и 4095 зарезервированы для специальных целей). Такой кадр называется маркированным (или тегированным, tagged). Тег занимает 4 байта. Он состоит из TPID (Tag Protocol Identifier, 2 байта), 802.1p (поле приоритета – 3 бита, также называемое Priority Code Point (PCP)), CFI (1 бит) и VID (идентификатор VLAN – 12 бит).

RFC 5517

«Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment». Документ описывает механизм изоляции устройств с помощью специальных ограничений пересылки на втором уровне. Такой механизм позволяет конечным устройствам использовать одну и ту же подсеть IP, будучи изолированными на втором уровне, что позволяет сетевым инженерам использовать более крупные подсети и снижать затраты на управление адресами. В данном RFC описан механизм Q-in-Q VLAN stacking — технология вложенных VLAN, также известная как Provider Bridging или Stacked VLANs.

RFC 3069

Это документ, который вводит концепцию агрегации VLAN в контексте распределения адресов IPv4. В нём описан механизм, при котором хосты, находящиеся в одной физической инфраструктуре, но в разных виртуальных широковещательных доменах, адресуются из одной подсети IPv4 и имеют общий IP-адрес шлюза по умолчанию, что устраняет

необходимость в отдельной подсети IP для каждой виртуальной локальной или metropolitan area network (MAN).

RFC 7348

Документ не описывает напрямую VLAN, в нем представлен протокол VXLAN, который используется для создания виртуальных сетей поверх IP-инфраструктуры, часто в дата-центрах.

VLAN

Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса (индивидуального, группового или широковещательного). В то же время внутри виртуальной сети кадры передаются по технологии коммутации, т. е. только на тот порт, который связан с адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими следствий, которые могут приводить к широковещательным штормам и существенно снижать производительность сети.

VLAN обладают следующими преимуществами:

1. гибкость внедрения — VLAN являются эффективным способом группировки сетевых узлов в виртуальные рабочие группы независимо от их физического размещения в сети;
2. ограничивают распространение широковещательного трафика, что увеличивает полосу пропускания, доступную для пользователя;
3. позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

VLAN ID Enumeration

Нумерация делится на два диапазона:

1. Нормальный диапазон. Используется в малых, средних и больших сетях. Нумерация начинается от 1 до 1005. Идентификаторы с 1002 до 1005 зарезервированы для устаревших сетей (Token Ring, FDDI).

2. Расширенный диапазон. Используется провайдерами и очень большими компаниями. Нумерация начинается с 1006 по 4094.

Порты VLAN

1. Access-порты предназначены для подключения конечных узлов в сети, таких как компьютеры или конечные устройства. Эти порты образуют нетегированный поток данных, что означает, что кадры, проходящие через них, не содержат информации о VLAN.

2. Trunk-порты обеспечивают линию связи между двумя коммутаторами или между коммутатором и маршрутизатором. Эта линия, называемая транком, транспортирует поток данных от нескольких VLAN. На транковых портах происходит тегирование кадров с метками VLAN ID, что позволяет принимающей стороне различать.

Native VLAN

Понятие в стандарте 802.1Q, которое обозначает VLAN на коммутаторе, где все кадры идут без тэга, то есть трафик передаётся нетегированным. По умолчанию это VLAN 1. Нужен он для совместимости с устройствами, незнакомыми с инкапсуляцией 802.1q.

Атаки на VLAN

1. VLAN-spoofing или атака на DTP-протокол. Данная атака работает на коммутаторах Cisco с поддержкой протокола DTP (Dynamic Trunking Protocol) могут автоматически согласовывать тип порта в режим trunk. Используя протокол DTP и «недонастроенный» коммутатор, атакующий ПК может получить доступ ко всем VLAN, присутствующим на коммутаторе.
2. Атака при помощи Native VLAN. Эта атака связана с тем, что коммутатор «из коробки» сконфигурирован так — видя, что к нему пришёл нетегированный фрейм, помещает его автоматически в Native VLAN и далее передаёт его в место назначения. Попадая на другой коммутатор, фрейм без тега помещается в его Native VLAN и так далее. Таким образом возможно получить доступ к ряду хостов. По умолчанию Native VLAN – это VLAN 1. Защититься можно следующим образом: назначаем на всех trunk-портах неиспользуемый VLAN в качестве native:
   SW(config-if)# switchport trunk native vlan 999
   Теперь атака неосуществима, так как VLAN 999 не относится ни к одному из access-портов.
3. Атака с двойным тэгированием. Связана с уязвимостью многих коммутаторов, которые поддерживают стандарт 802.1Q. Механизм данной атаки заключается в том, что на access-порт приходит фрейм с двумя тегами, один из которых соответствует Native VLAN данного коммутатора, а другой тег соответствует VLAN, в которую хочет попасть атакующий. И если в trunk-соединение между коммутаторами включен Native VLAN (по умолчанию он, как правило, включен), то коммутатор передаст данный пакет со вторым тегом, отбросив первый.

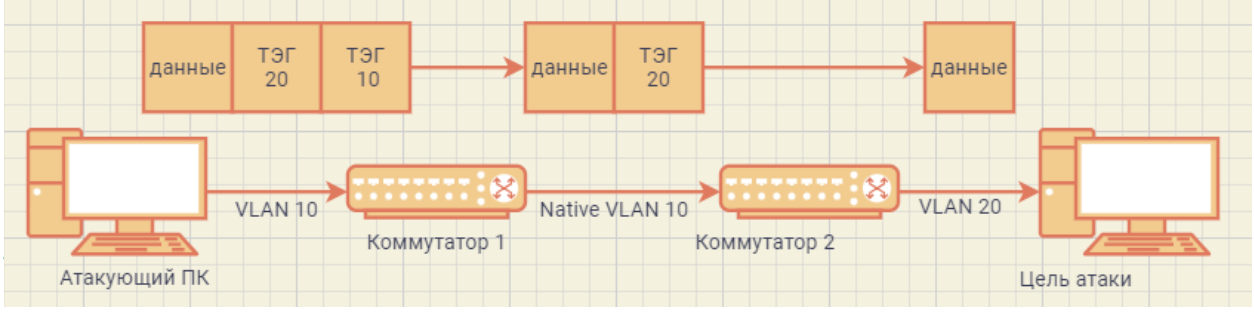

Рис. 1. Пример атаки типа с двойным тегированием

АТАКА НА НЕНАСТРОЕННОМ КОММУТАТОРЕ CISCO SYSTEMS CATALYST 2960 SERIES.

Описание эксперимента

Гипотеза эксперимента:

Если на коммутаторе Cisco Catalyst 2960 Series VLAN не настроен должным образом, а порты находятся в режиме динамического согласования, принимают DTP (Dynamic Trunking Protocol, DTP), злоумышленник сможет инициировать атаку VLAN Hopping и получить доступ ко всем VLAN на устройстве.

Методика эксперимента:

1. Подключается ПК злоумышленника к порту коммутатора.
2. Анализ трафика на ПК злоумышленника.
3. Злоумышленник отправляет DTP-пакеты, убеждая коммутатор перевести порт в режим транка.
4. В режиме транка злоумышленник получает доступ ко всем VAN, что позволяет ему перехватывать или генерировать трафик для любого VLAN.

Порядок эксперимента:

Используется коммутатор Cisco Catalyst 2960 Series с заводскими настройками**.** Атака проводится с помощью ПК с установленным приложением Yersenia. ПК злоумышленника подключён к порту коммутатора, находящемуся в режиме dynamic auto или dynamic desirable Анализ трафика будет производиться с помощью Wireshark. На порт, настроенного в режиме согласования посылаются DTP пакеты для настройки порта в режим транк, что даст злоумышленнику доступ ко всем VLAN. ПК жертвы находится во VLAN 20, ПК злоумышленника во VLAN 10. Цель – получить доступ к трафику ПК жертвы.

В утилите выберем DTP протокол.

Рис. 2. Статус порта в программе атакующего ПК

Как мы видим, пока DTP пакеты не посланы, мы не видим трафик жертвы, так как ПК находятся в разных VLAN. Жертва создаёт трафик, пингуя порт коммутатора с ip-адресом 192.168.20.1

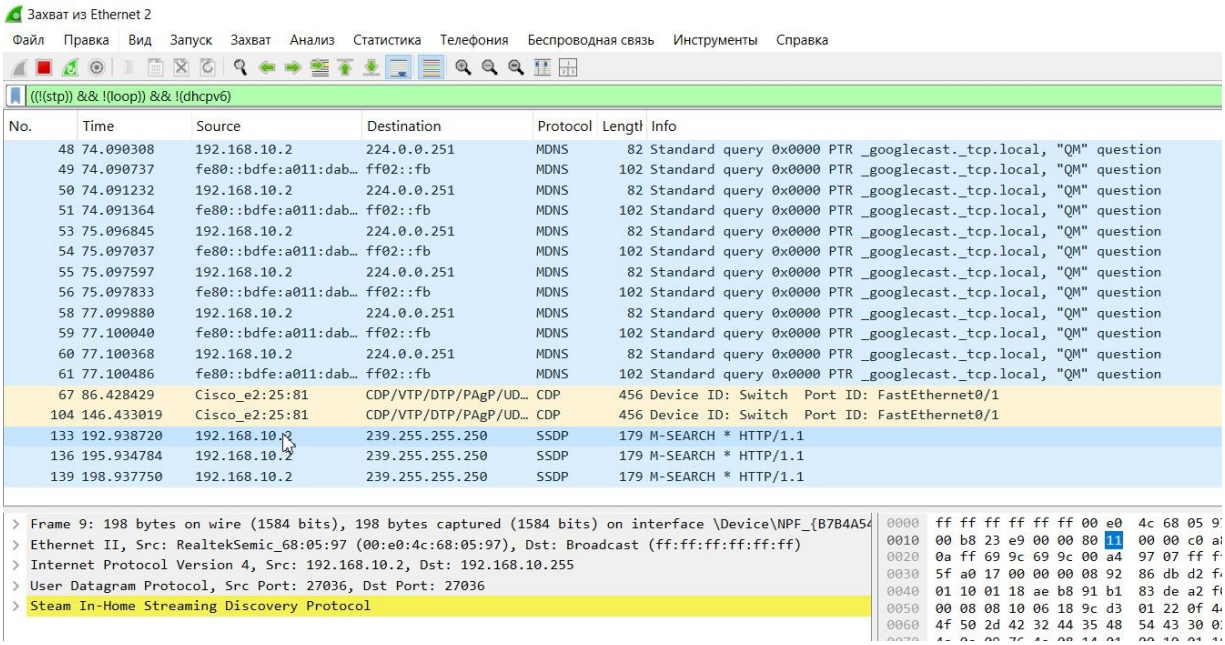

Рис. 3. Отслеживание трафика до атаки

Сейчас мы видим только CDP пакеты. Далее включим отсылку DTP пакетов и увидим, что порт перешёл в режим trunk.

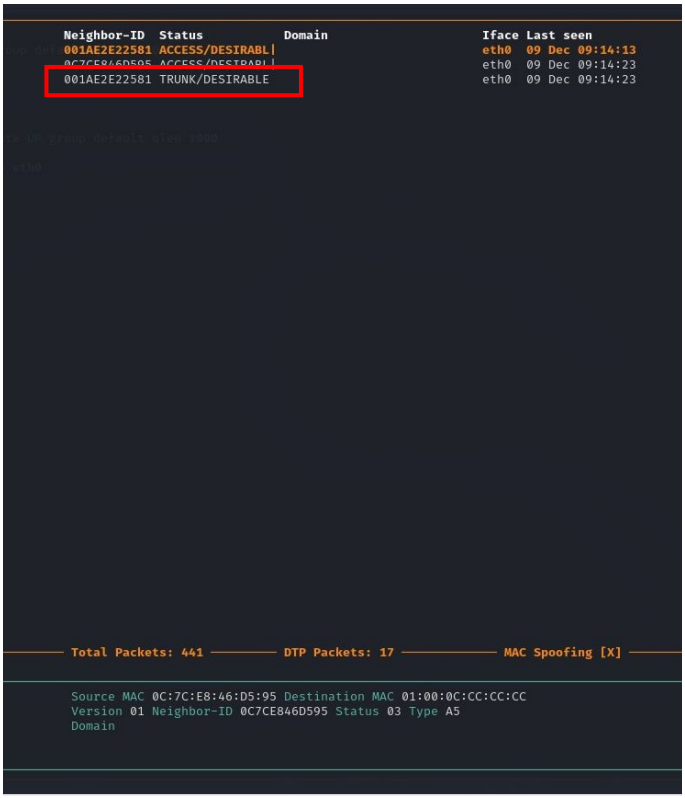

Рис. 4. Статус порта в программе атакующего ПК

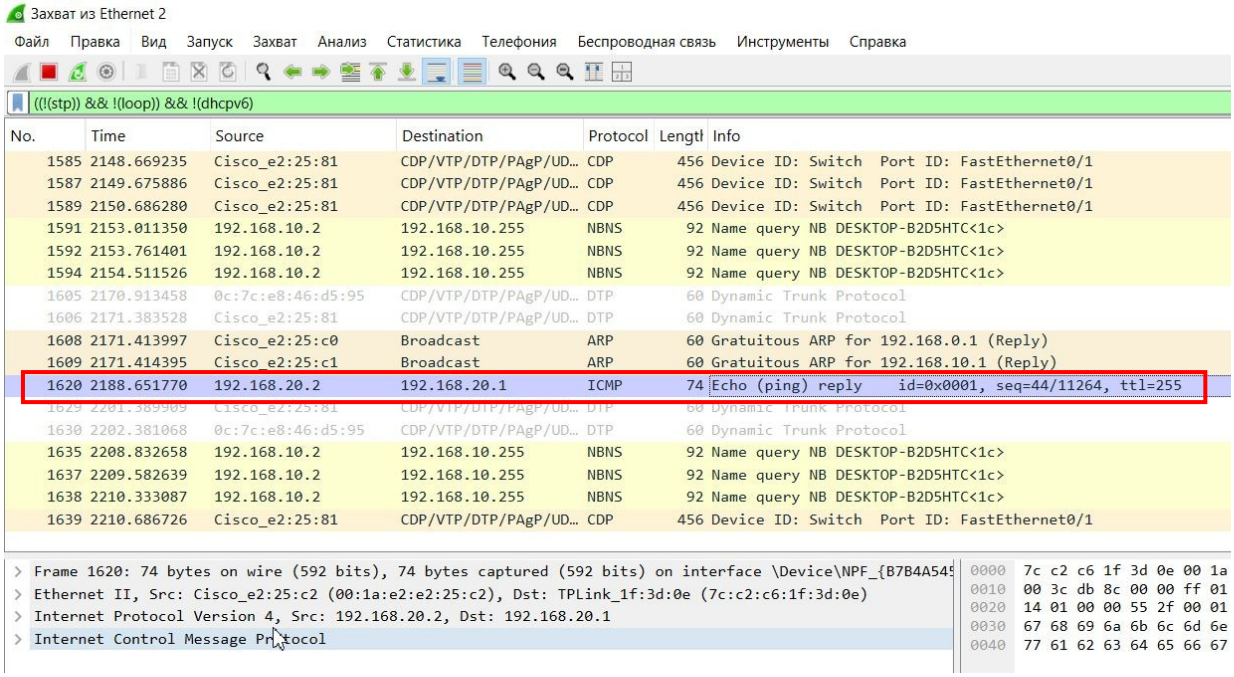

Рис. 5. Отслеживание трафика после атаки

Теперь с ПК злоумышленника мы можем видеть трафик, который идёт с ПК жертвы. Так как порт, к которому подключен злоумышленник стал транков, значит он имеет доступ ко всем VLAN, в данном случае ПК жертвы пингует порт коммутатора, к которому он подключён.

Решение проблемы:

Настройка Vlan на Cisco Systems Catalyst 2960 Series. Ниже в таблице 1 приведены команды для настройки Vlan на Cisco.

АТАКА С ДВОЙНЫМ ТЕГИРОВАНИЕМ НА КОММУТАТОРАХ ELTEX MES1428 И MIKROTIK CRS326-24G-2S+RM

Описание эксперимента

Гипотеза эксперимента:

Если коммутаторы соединены транком, который принимают кадры и помещают их в native VLAN, то, посылая кадры с двумя тегами, первый – с native VLAN ID, второй – с VLAN ID, в котором находится жертва, можно получить доступ к VLAN жертвы и посылать вредоносный трафик.

Методика эксперимента:

1. ПК злоумышленника подключен к порту доступа первого коммутатора.
2. Два коммутатора соединены транком, который помещает кадры в NATIVE VLAN.
3. ПК жертвы находится во VLAN 10, подключен ко второму коммутатору к порту доступа.
4. ПК злоумышленника посылает кадры с двумя тегами по стандарту 802.1q и получает возможность отправлять трафик на ПК жертвы.

Порядок эксперимента:

Подключаем ПК злоумышленника к порту коммутатора Eltex в режиме доступа. Соединяем коммутаторы Eltex и Mikrotik транком. Подключаем ПК жертвы к коммутатору Mikrotik к порту доступа во VLAN 10. Используем Wireshark для отслеживания трафика на ПК злоумышленника и Жертвы. С помощью утилиты Yersenia отправляем пакеты с двойным тегом. Цель – получить возможность отправлять трафик на ПК жертвы.

Настроим отправляемые кадры, в выделенных полях выберем теги для нужных нам VLAN: NATIVE VLAN (1), VLAN жертвы (10), также адрес жертвы 192.168.10.22 и адрес злоумышленника 192.168.10.3. Далее выберем отсылку пакеты с двумя тегами по стандарту 802.1q.

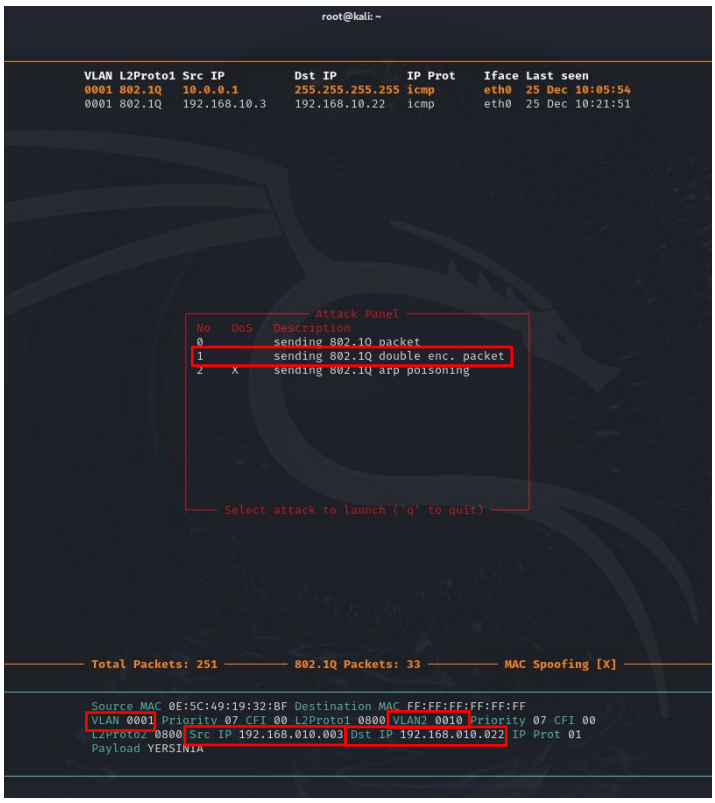

Рис. 6. Отправка пакетов с двумя тегами через утилиту

Проверим через Wireshark отправились ли наши пакеты.

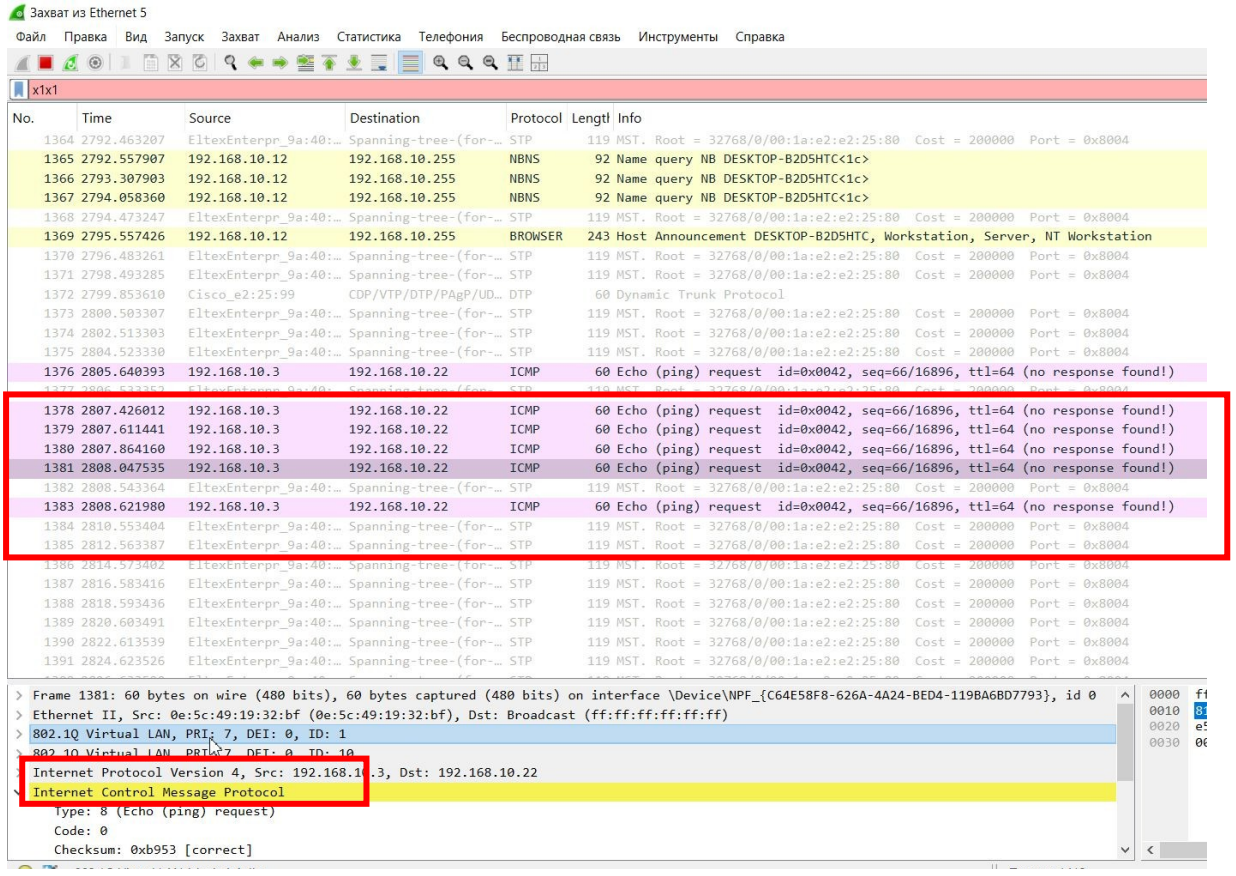

Рис. 7. Исходящий трафик с ПК злоумышленника.

Как мы видим пакеты отосланы, и они имеют два тега. Далее проверим трафик на ПК жертвы, чтобы убедиться, что наши пакеты были доставлены.

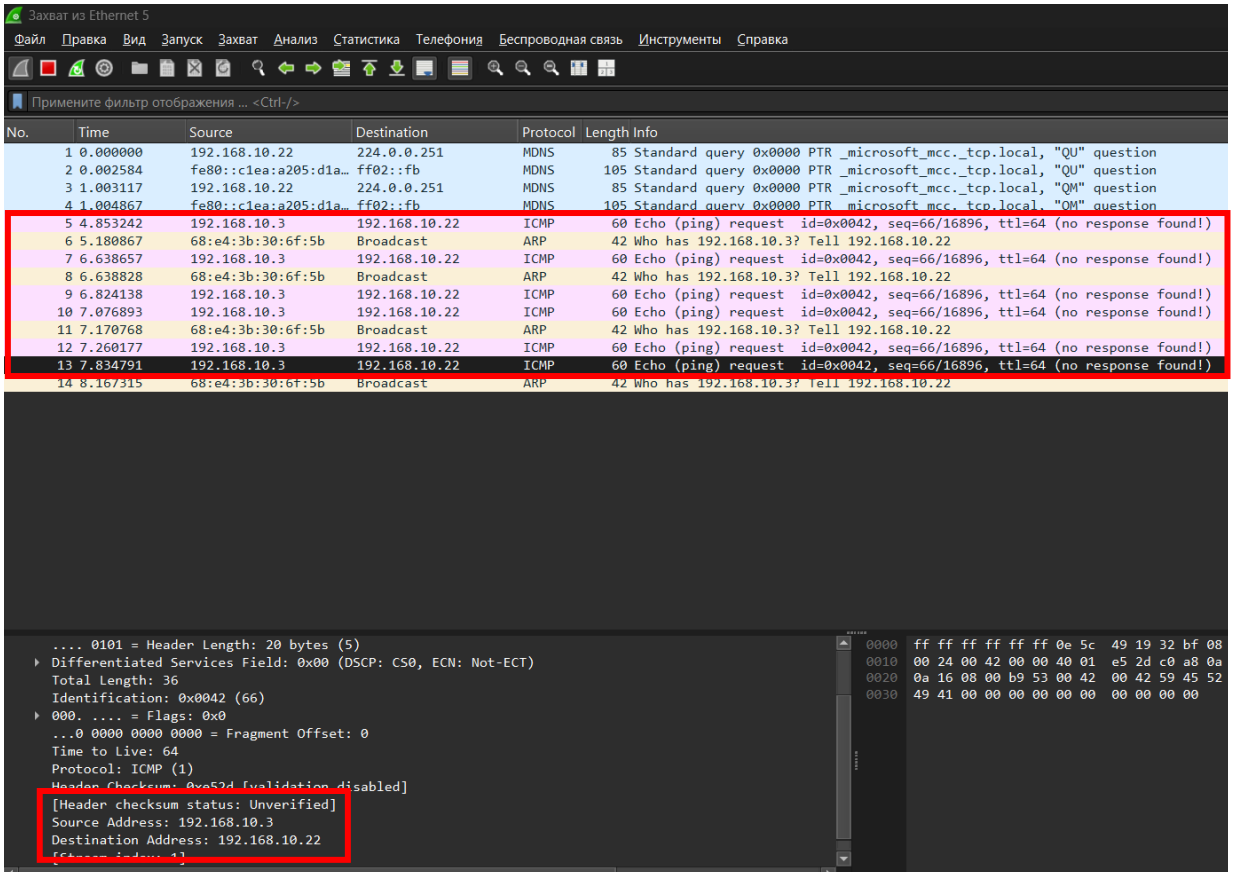

Рис. 7. трафик на ПК жертвы.

Пакеты успешно пришли на ПК жертвы без тегов, как показано на рисунке 1.

Решение проблемы:

НАСТРОЙКА CISCO SYSTEMS CATALYST 2960 SERIES/ELTEX MES1428/MIKROTIK CRS326-24G-2S+RM

Ниже представлена таблица, сравнивающая команды для конфигурации VLAN на Cisco, MikroTik и ELTEX, оформленная в удобной и структурированной форме.

Таблица 1. Команды для настройки VLAN на коммутаторах

Действие	CISCO	ELTEX	MIKROTIK
Переход в режим конфигурации	configure terminal	configure terminal	☞
Создаем бриджевый интерфейс	☞	☞	/interface bridge add name=bridge_name protocol-mode=none vlan-filtering={no,yes}
Добавление портов в бриджевый интерфейс	☞	☞	/interface bridge port add bridge=bridge_name interface=ether1
Создание VLAN	vlan vlan_id	vlan vlan_id vlan active	/interface vlan add interface=bridge_name name=vlan_id vlan_id vlan-id= vlan_id
Назначение ip-адреса:	interface vlan vlan_id /ip address 192.168.16.144 255.255.255.0	interface vlan vlan_id ip address 192.168.16.144 255.255.255.0	/ip address add address=192.168.16.144/24 interface=vlan vlan_id
Задать режим работы порта в VLAN.	switchport mode {dynamic {auto | desirable} | trunk}	switchport mode {access | trunk | general}	/interface bridge vlan add bridge=bridge_name {tagged | untagged}=ether1 vlan-ids= vlan_id
Добавление VLAN для интерфейса доступа	switchport access vlan vlan_id	switchport access vlan vlan_id	
Включение обработки тегов VLAN	-	☞	/interface bridge set 0 vlan-filtering=yes
Номер VLAN в качестве Default для данного интерфейса.	switchport trunk native vlan vlan_id	switchport trunk native vlan vlan_id	/interface bridge port add bridge=bridge_name interface=ether1 pvid=vlan_id
Добавить список VLAN для интерфейса	switchport trunk allowed vlan {add | all | except | remove} vlan-list	switchport general allowed vlan add vlan_list [untagged]	☞
Блокирует	switchport port-	switchport port-	/interface bridge port

функцию изучения новых адресов для интерфейса	security	security enable	set [find interface=ether1] learn=no
Задает максимальное количество адресов, которое может изучить порт	switchport port-security maximum (num)	switchport port-security maclimit	/interface bridge port set [find interface=ether1] horizon=1
Задать режим реагирования при нарушении безопасности	switchport port-security violation {protect | restrict | shutdown}	switchport port-security violation [restrict | protect]	☞
Задает режим ограничения изучения MAC-адресов	switchport port-security mac-address {sticky} [mac-address | vlan {vlan-id | {access | voice}}]	switchport port-security mode {max-addresses | lock}	/interface bridge filter add chain=forward action=drop src-mac-address=! XX:XX:XX:XX:XX:XX in-interface=ether1
Сохранение конфигурации происходит автоматически, но можно вручную сохранить экспорт:	Copy running-config startup-config	Write startup-config	/export file=backup-config

Таким образом, можно произвести базовую настройку защиты коммутаторов.

ЗАКЛЮЧЕНИЕ

В статье рассмотрены основные угрозы, связанные с атакой на VLAN, включая перехват и анализ сетевого трафика, а также возможности несанкционированного доступа к различным VLAN. Эти атаки эксплуатируют недостатки в конфигурации сетевых устройств и методов сегментации, что делает их особенно опасными в корпоративных сетях с высокой плотностью взаимодействий.

Для защиты от подобных атак были выделены ключевые методы, такие как правильная настройка VLAN Trunking Protocol (VTP), использование механизма фильтрации VLAN (VLAN Filtering) и ограничение доступа к trunk-портам. Также подчеркивается важность использования функций Port Security и блокировки несанкционированного изучения MAC-адресов на уровне коммутаторов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уймин А.Г. Компьютерные сети. L2-технологии : Практикум/ Уймин А.Г. — Москва : Ай Пи Ар Медиа, 2024. — 191 с. — ISBN 978-5-4497-2539-4. — Текст : электронный.(дата обращения: 06.12.2024)
2. Ethernet switches MES14xx, MES24xx Operation Manual, Firmware Version 10.1.8.2 / Документация [Электронный ресурс] // ELTEX : [сайт]. — URL: https://eltex-co.com/upload/iblock/930/MES14xx,%20MES24xx_user%20manual_10.1.8.2_en.pdf (дата обращения: 21.12.2024).
3. IEEE 802.1Q / [Электронный ресурс] // WikipediA : [сайт]. — URL: https://en.wikipedia.org/wiki/IEEE_802.1Q (дата обращения: 24.12.2024).
4. Manual:CRS3xx series switches / [Электронный ресурс] // MikroTik : [сайт]. — URL: https://wiki.mikrotik.com/Manual:CRS3xx_series_switches#VLAN (дата обращения: 21.12.2024).
5. MikroTik: VLAN на коммутаторах CRS1xx/2xx/3xx и SOHO маршрутизаторах (RouterOS 6.41+). Lab #3. / [Электронный ресурс] // iRWX.RU : [сайт]. — URL: https://www.irwx.ru/mikrotik-vlan-crs-lab-3/ (дата обращения: 21.12.2024).

6. VLAN Configuration, Cisco Catalyst PON Series Switches / [Электронный ресурс] // CISCO : [сайт]. — URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_pon/software/configuration_guide/vlan/b-gpon-config-vlan/configuring_vlan.html (дата обращения: 21.12.2024).