Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Ильина Александра Алексеевна Группа: 241-352

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководители практики:

Гневшев Александр Юрьевич

Кесель Сергей Александрович

Камозин Сергей Андреевич

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

1. Общая информация о проекте:

* Название проекта
* Цели и задачи проекта

1. Общая характеристика деятельности организации *(заказчика проекта)*

* Наименование заказчика
* Организационная структура
* Описание деятельности

1. Описание задания по проектной практике
2. Описание достигнутых результатов по проектной практике

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЯ

**ВВЕДЕНИЕ**

1. **Общая информация о проекте:**

* **Название проекта:** Группа проектов тестирования
* **Цели и задачи проекта:**

Цель проекта: тестирование сайтов, игр, приложений и других внутренних проектов Московского Политехнического университета.

Задачи проекта:

* Проверка интерфейсов и функционала
* Составление баг-репортов
* Обратная связь разработчикам
* Ведение таблицы заявок

1. **Общая характеристика деятельности организации *(заказчика проекта)***

* Наименование заказчика
* Организационная структура
* Описание деятельности

1. **Описание задания по проектной практике**
2. **Описание достигнутых результатов по проектной практике**

**4.1 Анализ инцидента**

* Изучен инцидент, связанный с серией кибератак северокорейской хакерской группы Kimsuky с использованием Troll Stealer.
* Установлено, что был использован дроппер, маскирующийся под установочный файл легитимного ПО южнокорейской компании SGA Solutions, подписанный украденным сертификатом компании D2Innovation Co., Ltd.
* Зафиксированы действия вредоносной программы:
  + кража SSH-ключей и данных FileZilla;
  + сбор файлов и каталогов с диска C;
  + извлечение данных из браузеров;
  + сбор системной информации;
  + снятие скриншотов;
  + кража сертификатов GPKI, используемых южнокорейскими государственными служащими.
* Дополнительно задействован бэкдор GoBear, написанный на языке Go.
* В процессе анализа действия злоумышленников сопоставлены с тактиками и техниками ATT&CK.

**4.2 Взаимодействие с партнерами**

**Отчет о посещении мастер-класса «Требования и их важность при разработке ПО»**

Общая информация

23 апреля состоялся мастер-класс «Требования и их важность при разработке ПО», организованный компанией [ООО "Эдит Про"](https://www.borlas-edit.ru/about/). Мероприятие было посвящено ключевым аспектам выявления и анализа требований заказчика в процессе разработки программного обеспечения. Участники погрузились в реальные сценарии разработки, что дало возможность не только получить теоретические знания, но и применить их на практике в ходе деловой игры.

О компании ООО "Эдит Про"

ООО "Эдит Про" — компания, специализирующаяся на разработке программного обеспечения и консалтинге в области IT. С момента своего основания компания стремится создавать решения, которые соответствуют потребностям клиентов и помогают им достигать бизнес-целей. Основные направления работы компании включают:

* Консалтинг в области разработки ПО — помощь в выявлении и формулировании требований.
* Обучение и развитие — проведение мастер-классов и тренингов для специалистов в области IT.
* Поддержка проектов — помощь в управлении проектами и внедрении новых решений.

Цели компании

1. Увеличение качества разрабатываемого ПО через глубокое понимание потребностей заказчиков.
2. Развитие образовательных программ для повышения квалификации специалистов в области разработки ПО.
3. Сбор и анализ обратной связи от клиентов для улучшения предлагаемых услуг и продуктов.

Программа мастер-класса

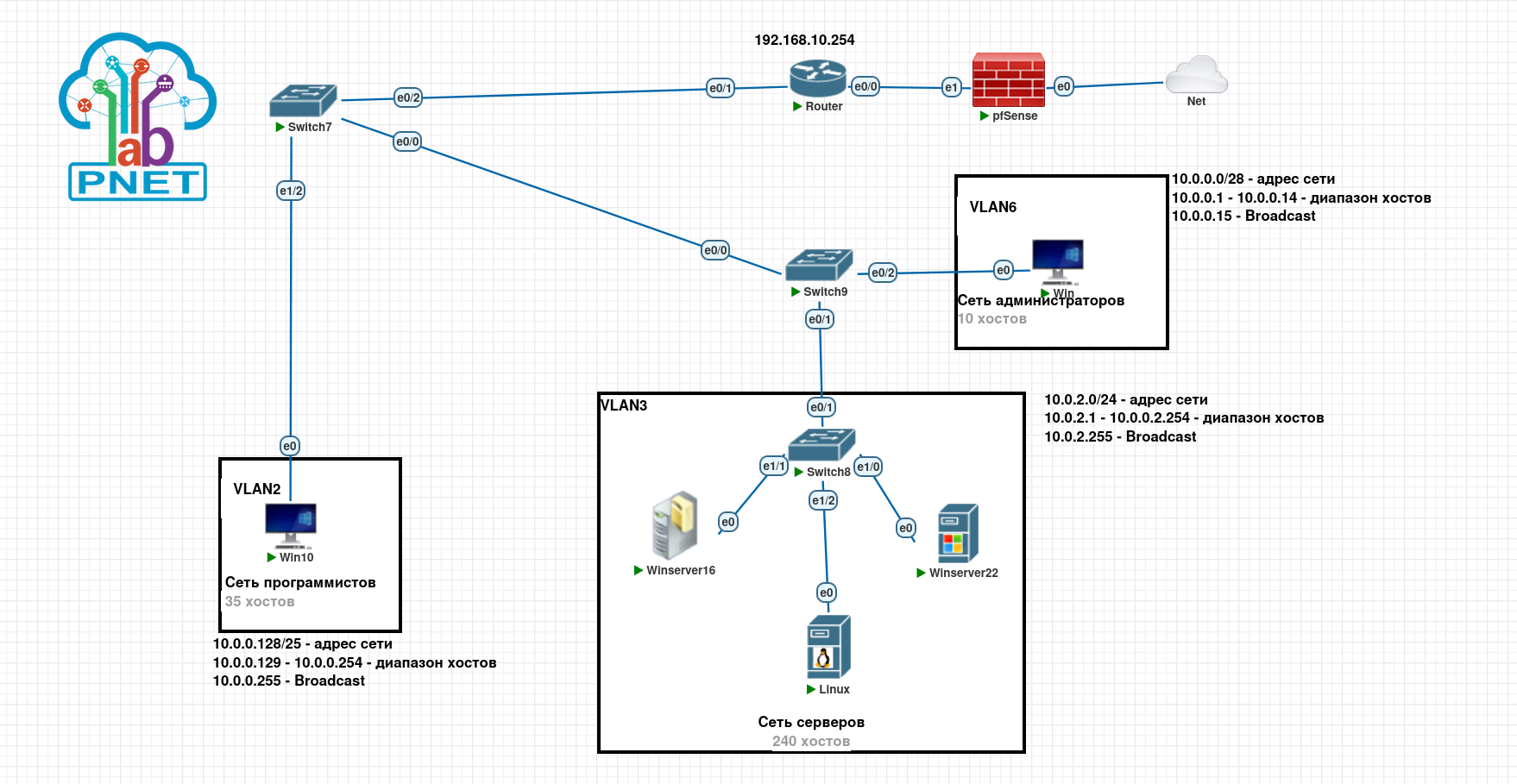
Мастер-класс включал несколько ключевых тем:

* Выявление и анализ требований: Участники узнали о методах активного слушания и задавания открытых вопросов, которые помогают лучше понять потребности заказчика.
* Приоритизация требований: Обсуждались методы расстановки приоритетов, позволяющие определить, какие требования являются наиболее критичными для успешной реализации проекта.
* Практическое применение знаний: В ходе деловой игры участники смогли применить полученные знания на практике, что способствовало лучшему усвоению материала.

**4.3 Создание и наполнение сайта**

**4.4 Вариативная часть. Базовая настройка LAN Game Dev студии в PNETLab**

**1. Сетевая архитектура**

****

|  |  |  |  |
| --- | --- | --- | --- |
| **Сегмент** | **VLAN** | **Подсеть** | **Доступные IP** |
| Программисты | 2 | 10.0.0.128/25 | .129 – .254 |
| Администраторы | 6 | 10.0.0.0/28 | .1 – .14 |
| Серверы | 3 | 10.0.2.0/24 | .1 – .254 |
| Интернет / WAN | - | 192.168.10.0/24 | .1 – .254 |

**2. Конфигурация оборудования**- Подробнее про работу с оборудованием и конфигурацию оборудования в PNETLab можно посмотреть в отдельном модуле Базовая конфигурация.  
- В приложение вынесены модули Атака-Защита сетевой инфраструктуры (CAM-table overflow, ARP-Spoofing, VLAN Hopping, MAC-Spoofing).

**Конфигурация Switch7 (основной для доступа)**enable  
conf t  
hostname Switch7  
no ip domain-lookup  
enable secret strongpass  
service password-encryption  
banner motd ^WARNING: Unauthorized access is prohibited!^

**3. Серверы — развертывание служб**

Настройка серверов (пример):  
- WinServer16 (10.0.2.10) — SYSLOG + DNS + DHCP.  
- WinServer22 (10.0.2.20) — GIT + Jenkins.  
- Linux-сервер (10.0.2.30) — Fail2Ban, rsyslog, rsync**.**

**4) Security Policy Checklist**Контроль доступа:  
- Программисты (VLAN 2) — Git, Jenkins, интернет.  
- Администраторы (VLAN 6) — Полный доступ.  
- Серверы (VLAN 3) — Только по нужным портам.

**ЗАКЛЮЧЕНИЕ**

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

**ПРИЛОЖЕНИЯ**

**Настройка сети в PNETLab**

**Часть 1: Создание топологии**

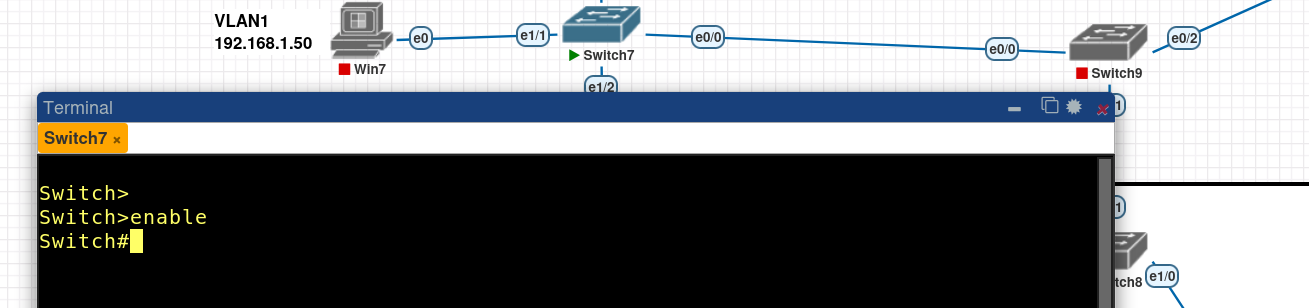
План топологии:



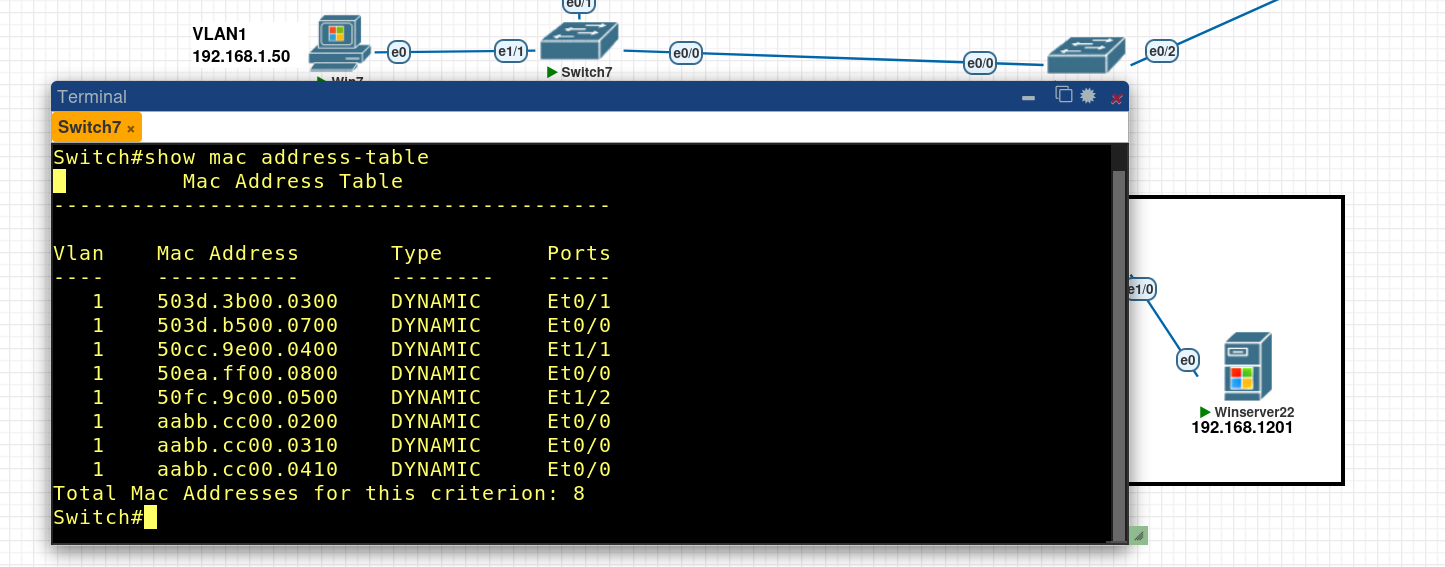
**Часть 2: Работа с сетевыми устройствами**

Взаимодействие с сетевыми устройствами Cisco IOL происходит с помощью CLI.

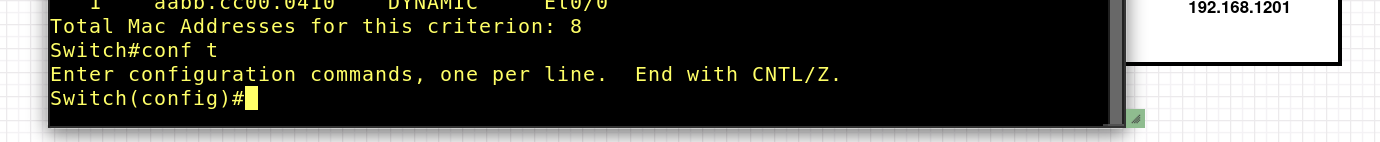
2.1 Зайдём в Switch7 и перейдём в привилегированный режим.



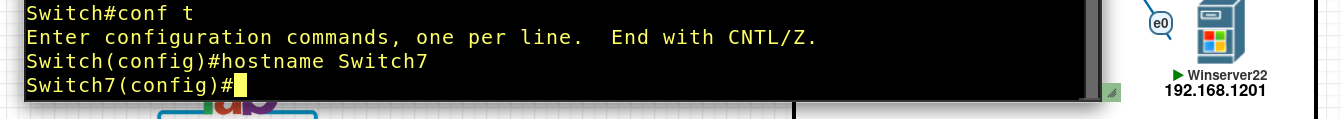
2.2 Просмотрим его таблицу коммутации.



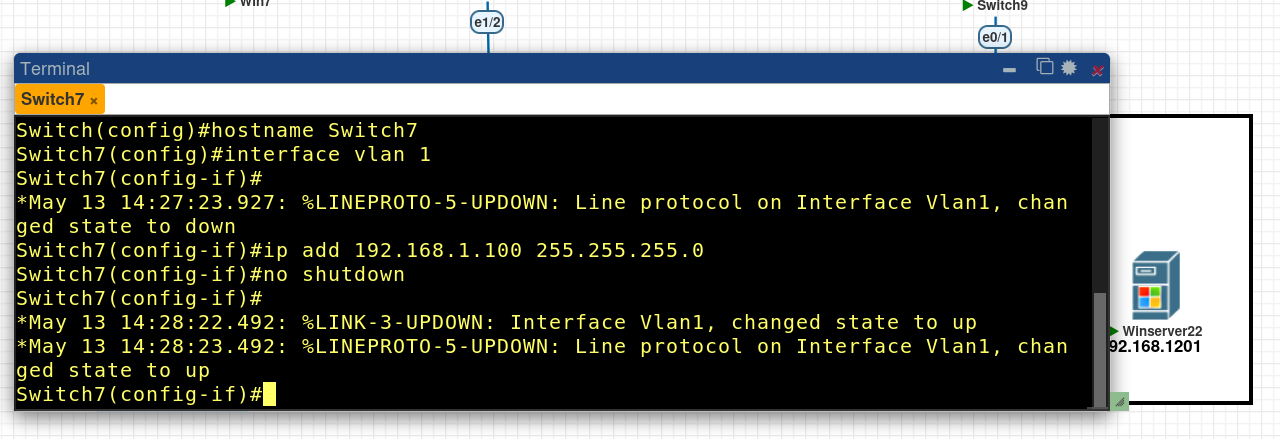
2.3 Настроим имя устройства. Перейдём в режим конфигурации.



2.4 Укажем имя устройства.



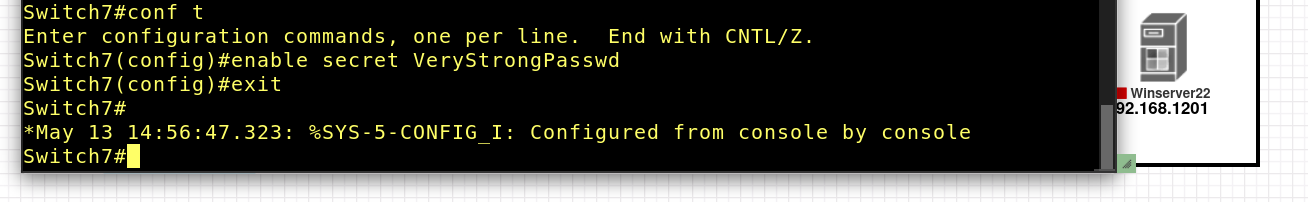
2.5 Настроим IP-адрес для управления Switch7.



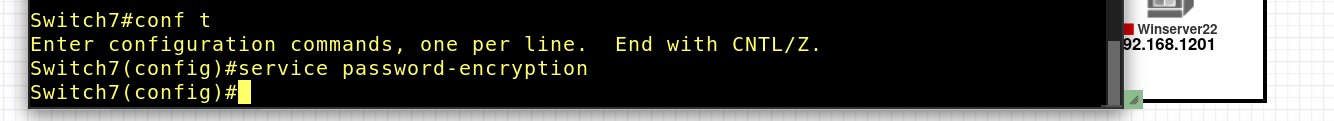
2.6 Ставим пароль на консоль.



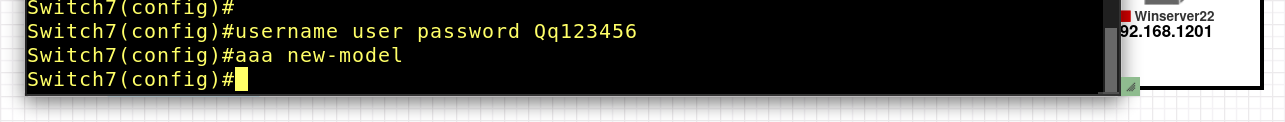
2.7 Ставим пароль на привилегированный режим.



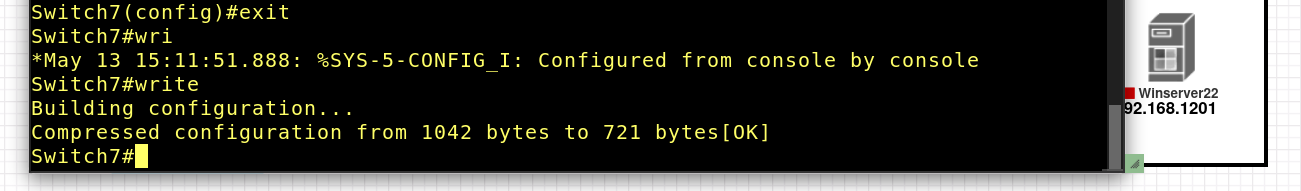
2.8 Включаем шифрование паролей.



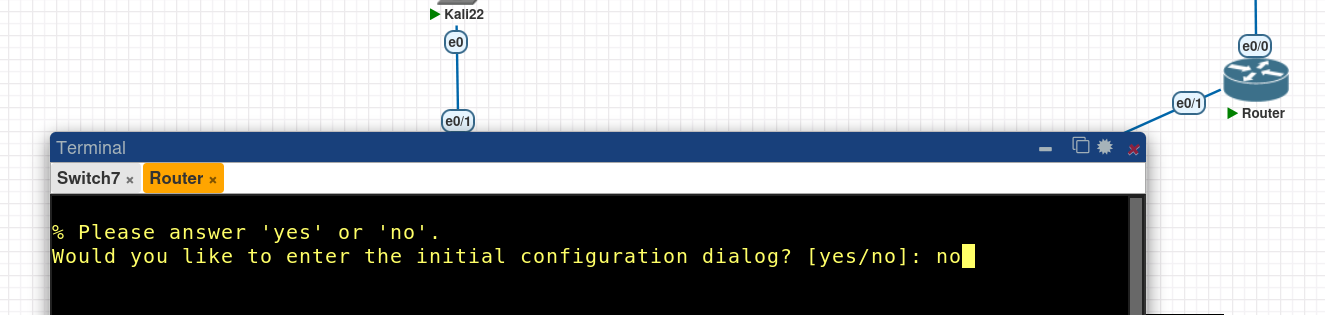
2.9 Создаём учетную запись пользователя и включаем модель аутентификации.



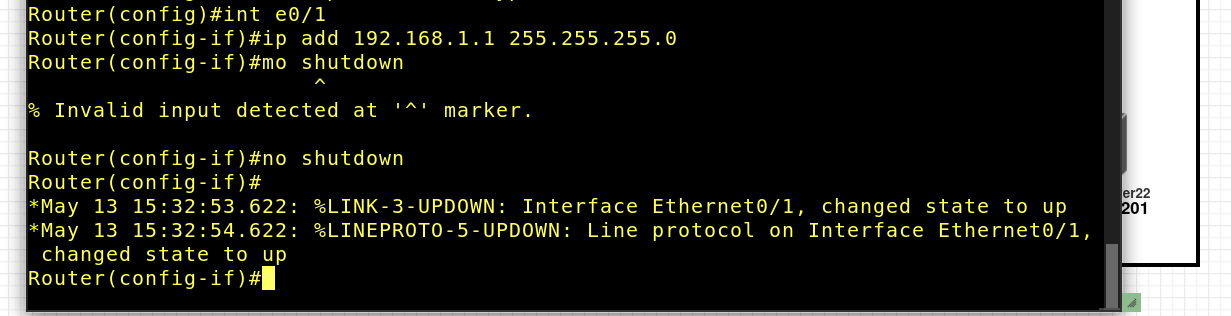
2.10 Сохраняем конфигурацию.



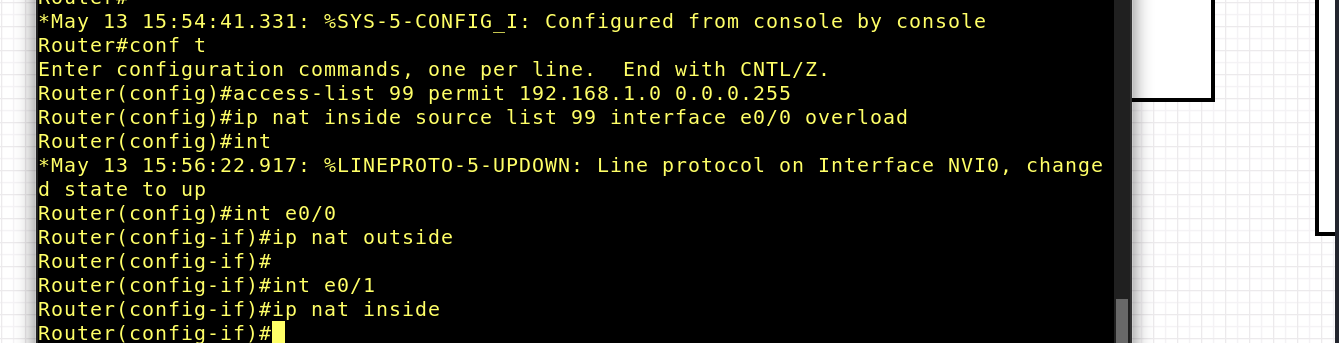
2.11 Зайдём в роутер и откажемся от автонастройки.



2.12 Настроим внутренний интерфейс роутера (e0/1).

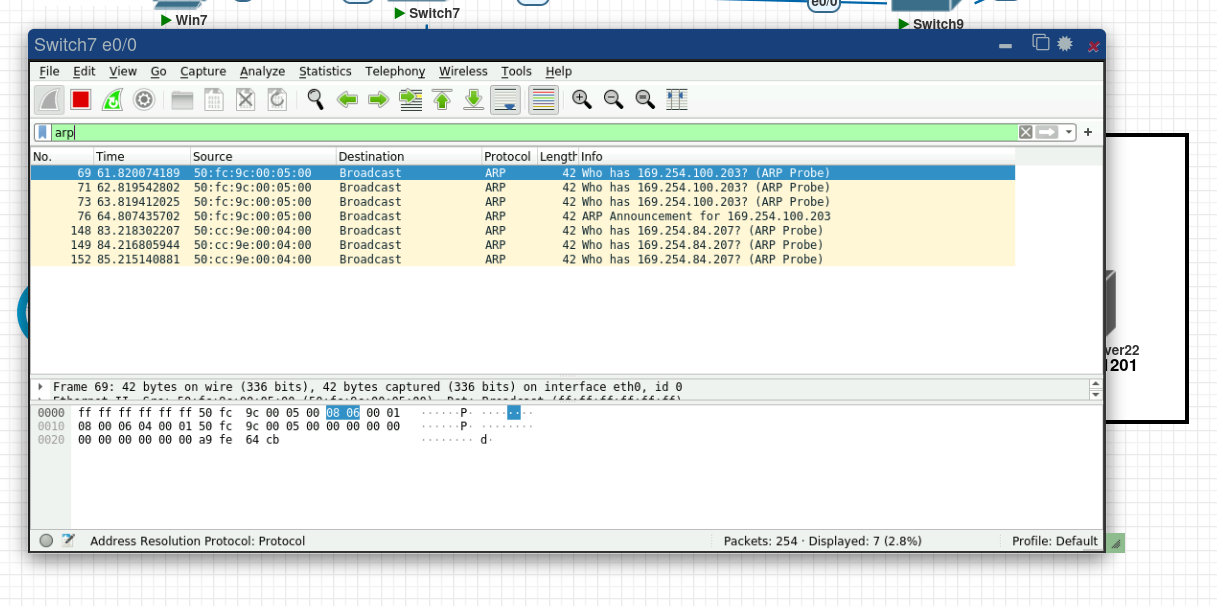


2.13 Настроим NAT на роутере.



**Часть 3: Анализ трафика**

Теперь с помощью Wireshark можем отследить, например, ARP трафик.



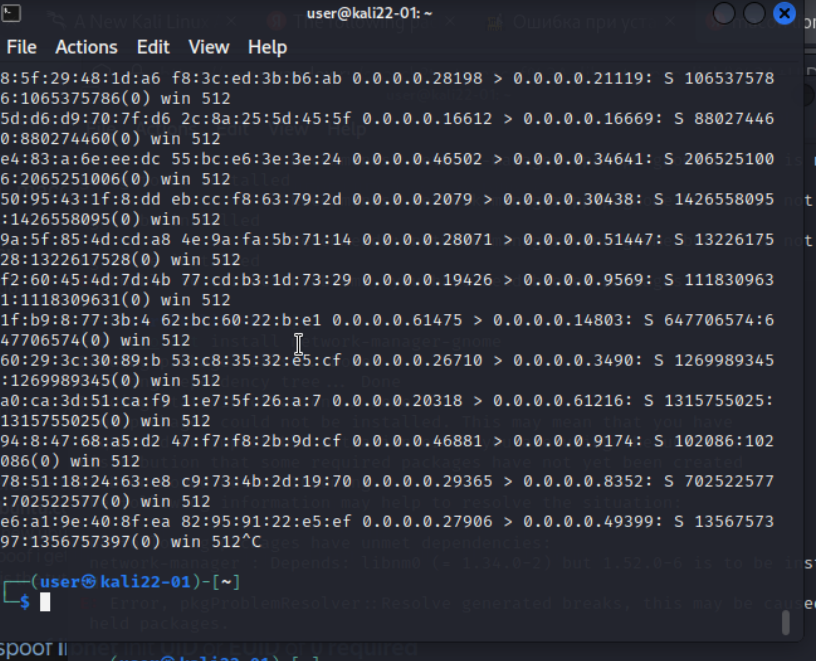
**CAM-table Overflow**  
CAM-table overflow — атака на коммутатор, при которой генерируется большое количество фальшивых MAC-адресов,   
что приводит к переполнению таблицы коммутации. В результате коммутатор начинает пересылать кадры всем портам,   
что позволяет атакующему перехватывать трафик других устройств.

**Часть 1: Демонстрация атаки**

1.1 Запуск атаки на Kali Linux

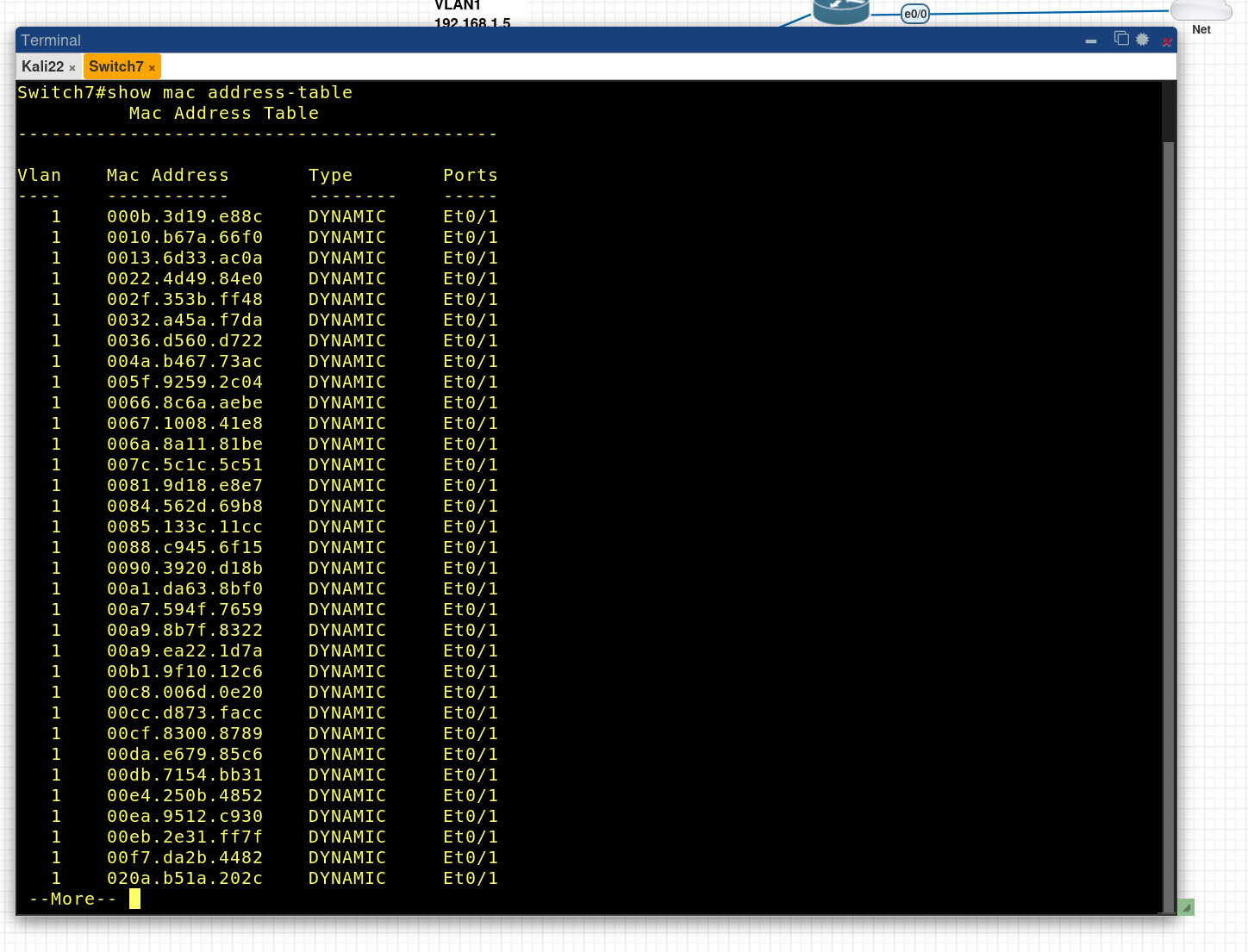
Установим на Kali Linux утилиту dsniff и запустим атаку:

Команда: macof -i eth0



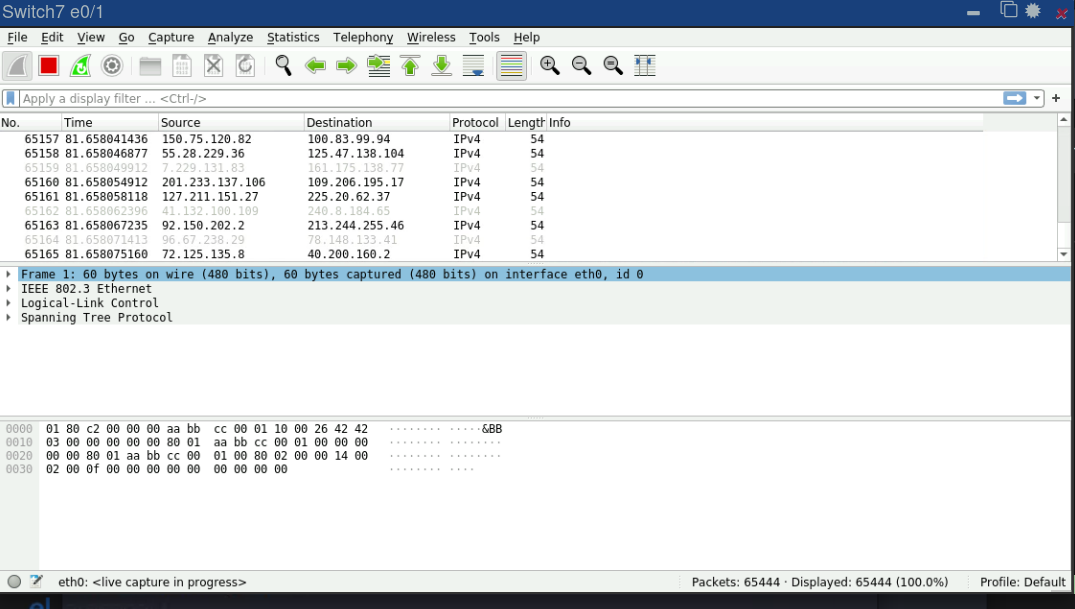
1.2 Переполнение таблицы коммутации

Таблица коммутации Switch7 переполнена, устройства теряют связь.



1.3 Анализ трафика в Wireshark

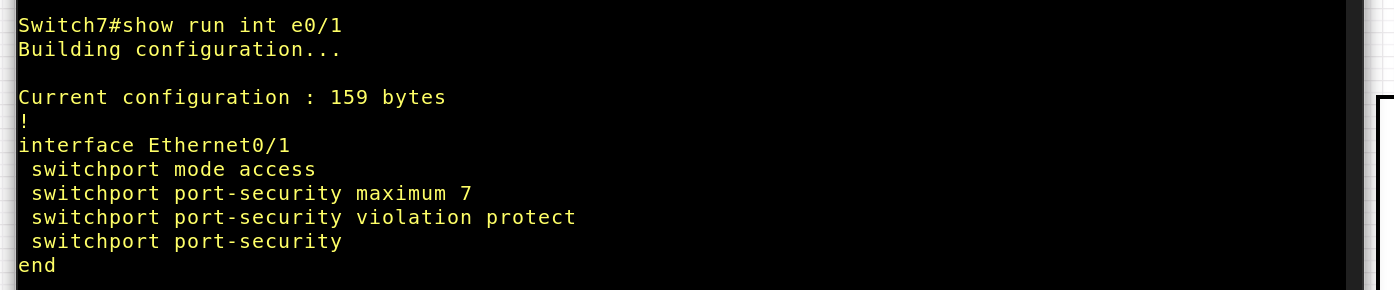
Мы видим большое количество IPv4-запросов.



**Часть 2: Защита от CAM-table Overflow**

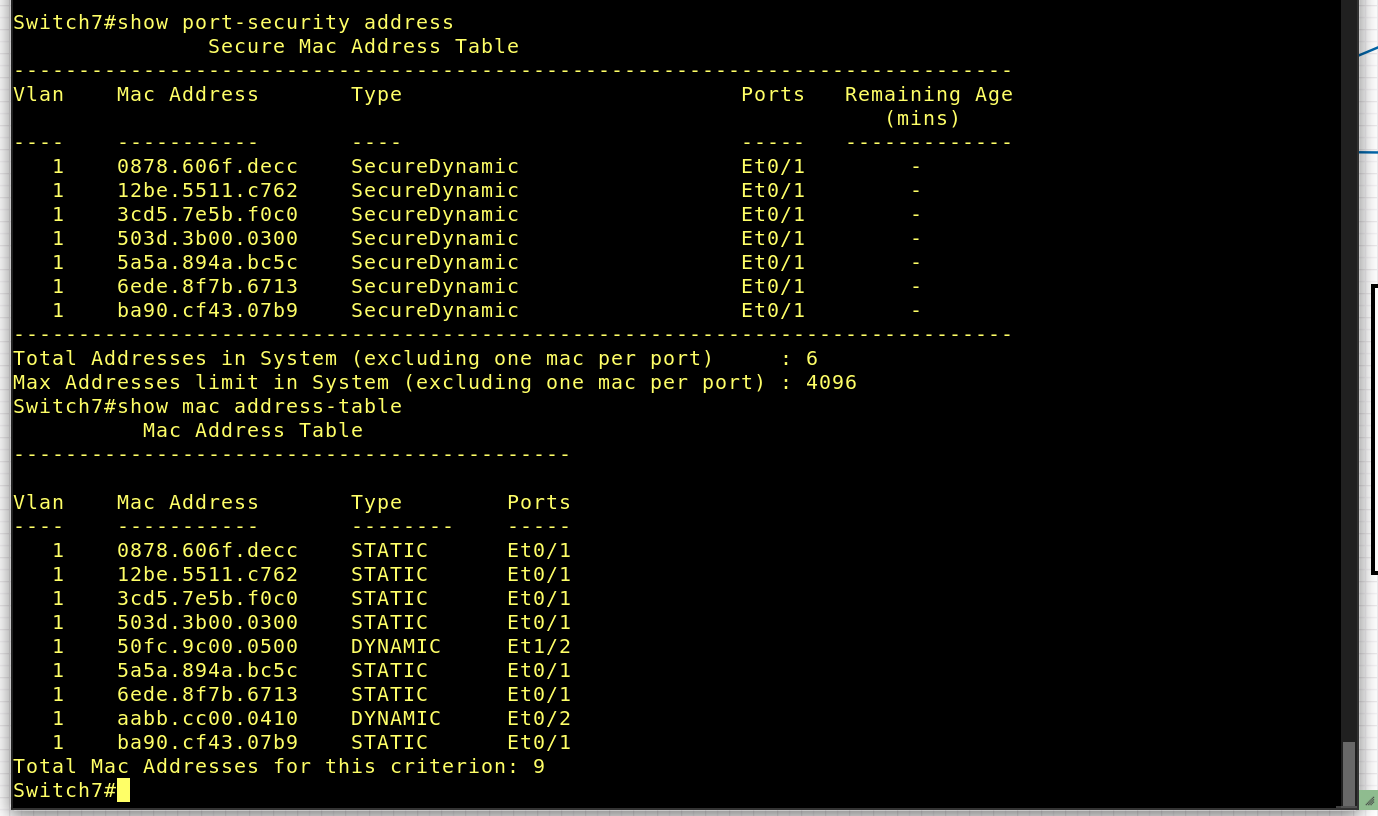
2.1 Настройка защиты на Switch7

Настроим защиту от CAM-table overflow на коммутаторе Switch7 с помощью команд:  
- switchport port-security  
- switchport port-security maximum 7  
- switchport port-security violation protect



2.2 Проверка защиты

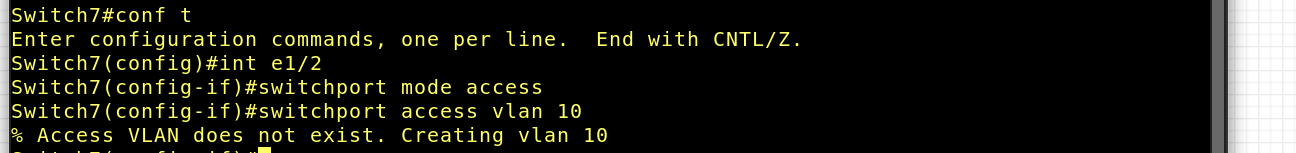
Проверяем таблицу MAC-адресов после атаки, видим, что защита работает.



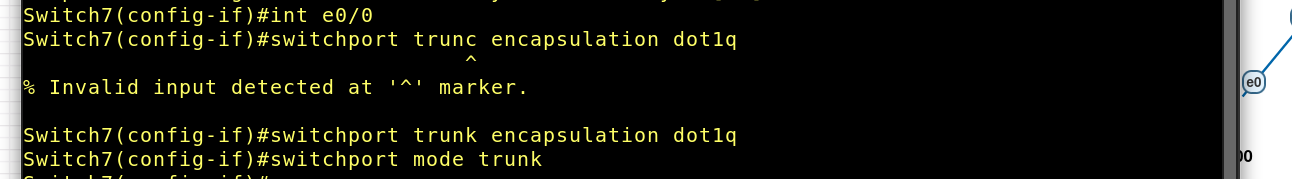
**VLAN Hopping**

**Часть 1. Демонстрация VLAN Hopping**

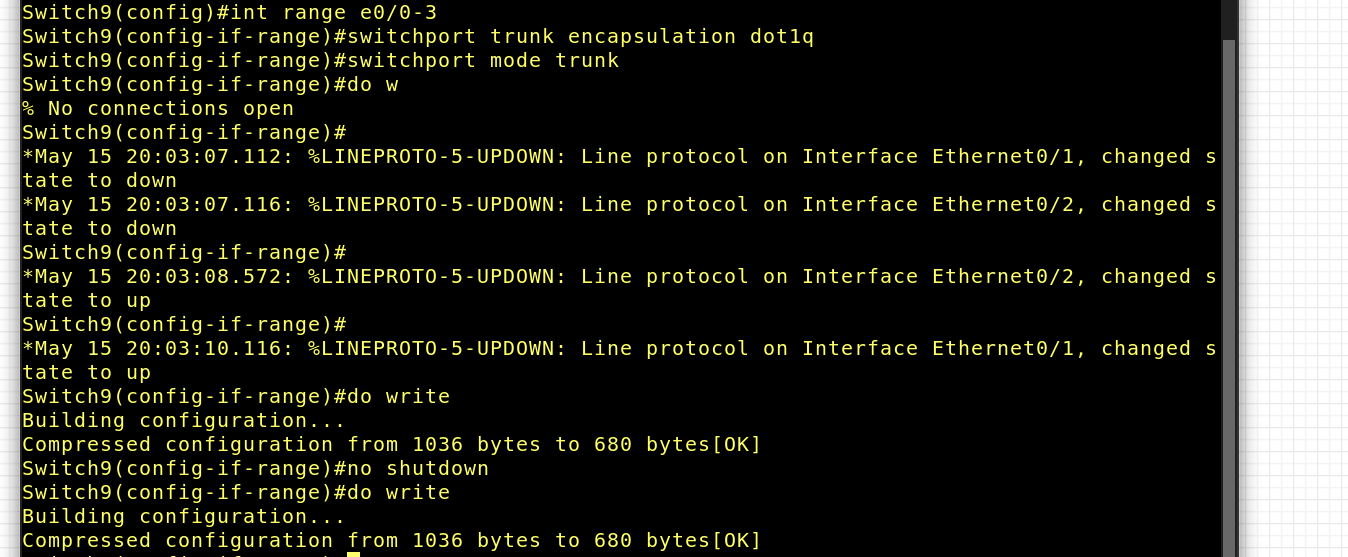
1.1 Поместим Win10 в vlan10



1.2 Сконфигурируем trunk port на Switch7



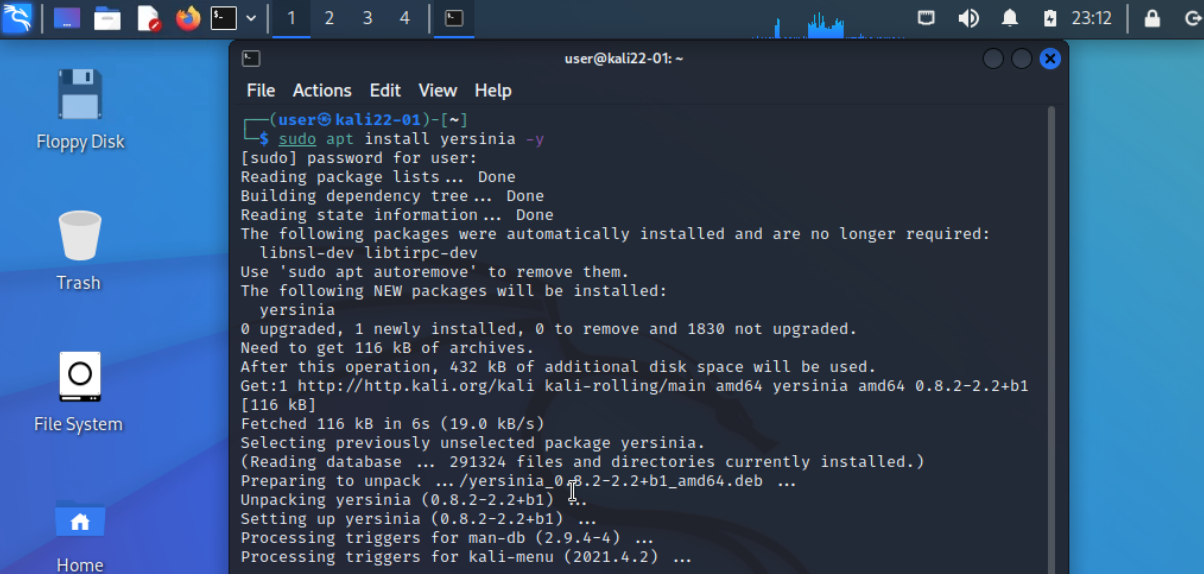
1.3 Настроим на Switch9 интерфейсы е0/0, e0/1, e0/2 в trunk



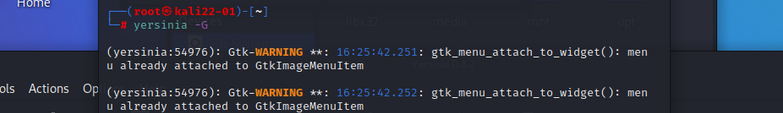
1.4 Настроим на роутере шлюз для vlan10

Router(config)#int e0/1.10  
Router(config-subif)#encapsulation dot1q 10  
Router(config-subif)#ip address 192.168.10.1 255.255.255.0

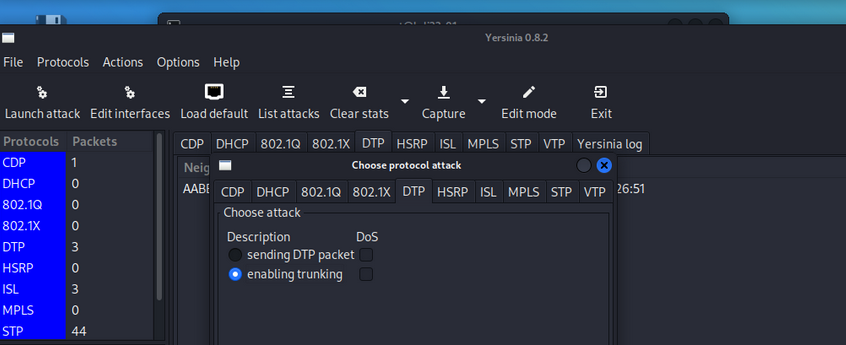
1.5 Установим Yersinia



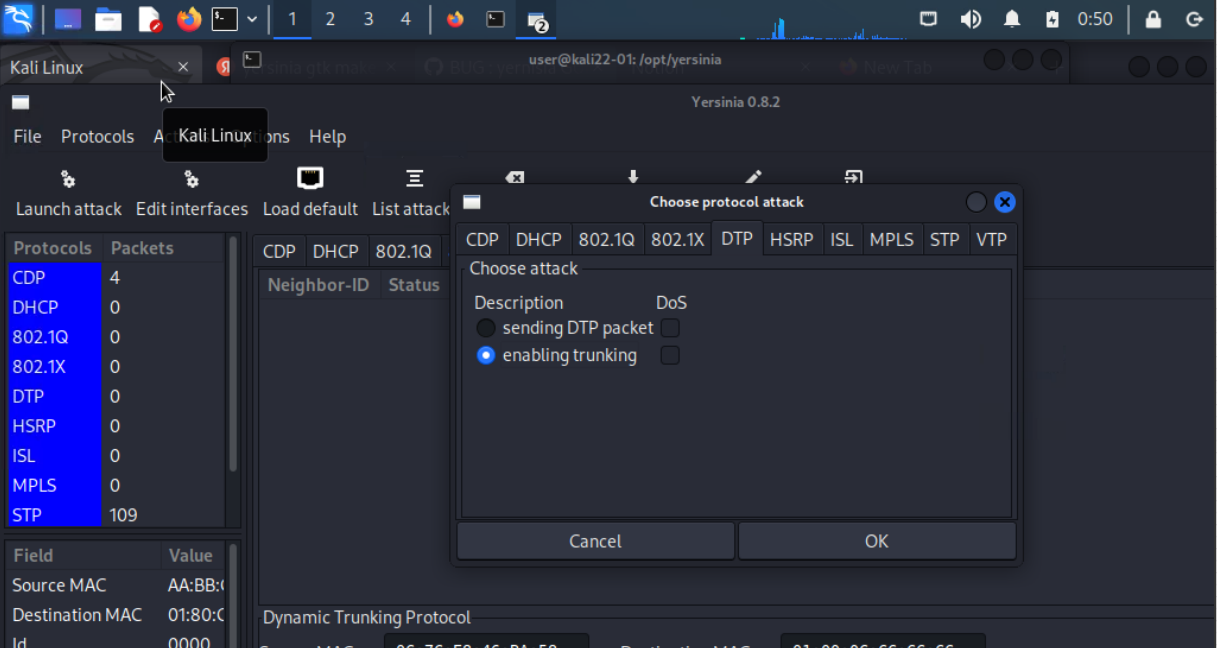
1.6 Запустим Yersinia



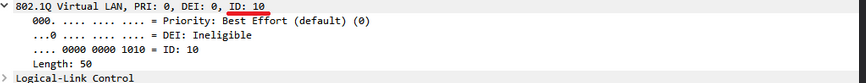
1.7 Проведем атаку на протокол DTP



1.8 Подготовим интерфейсы Kali

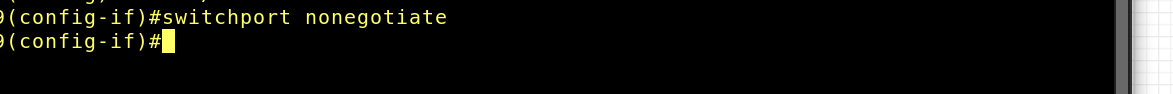


1.9 Анализ трафика с vlan id 10 через Wireshark



**Часть 2. Защита от VLAN Hopping**

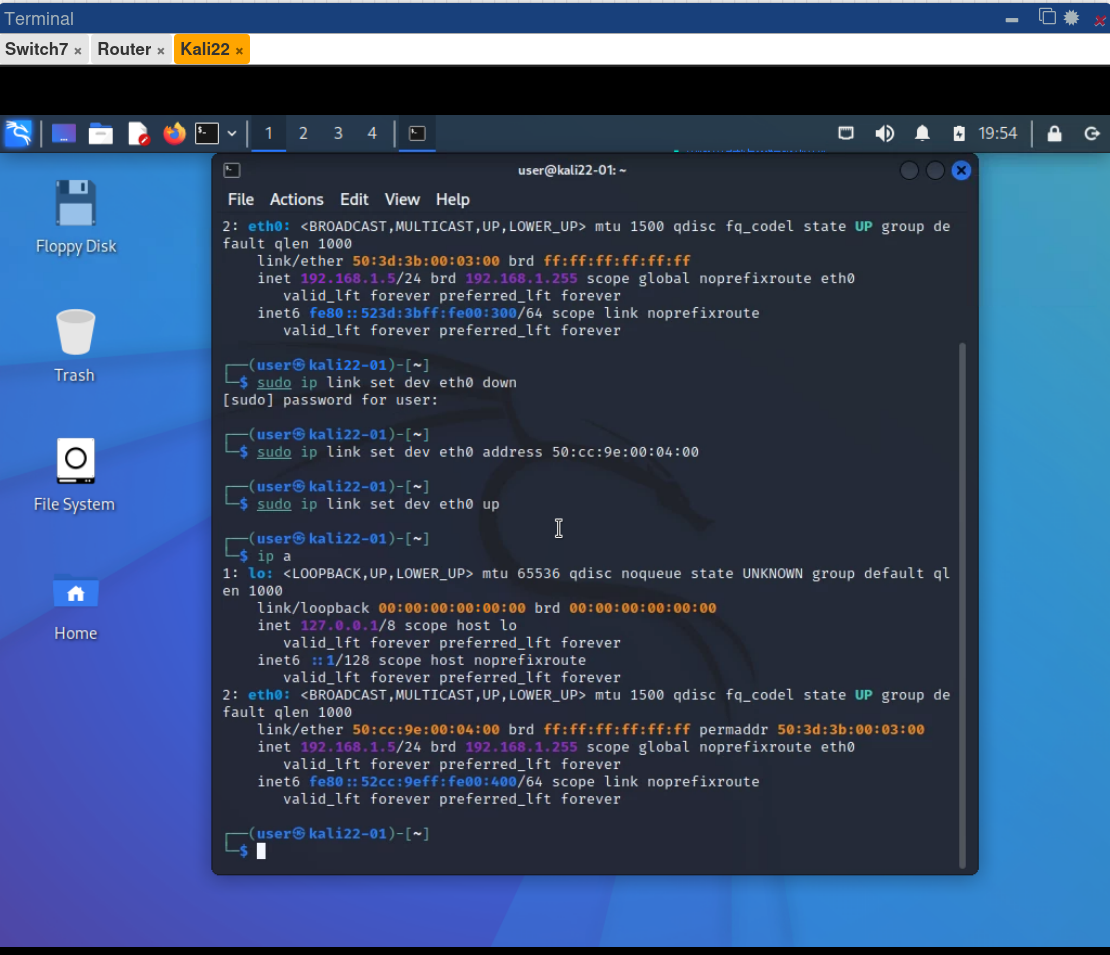
2.1 Из этого состояния порт может перейти в trunk, DTP-кадры при этом не передаются



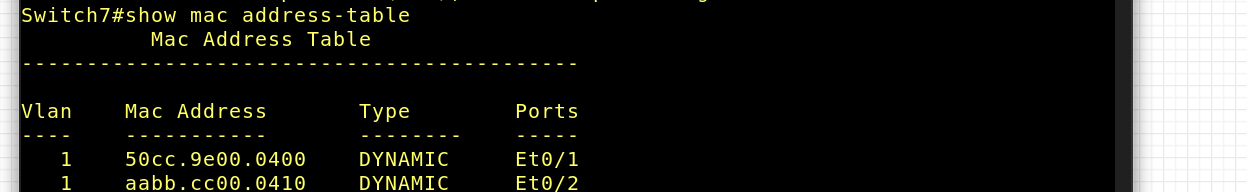
**MAC-Spoofing**

**Часть 1. Демонстрация MAC Spoofing**

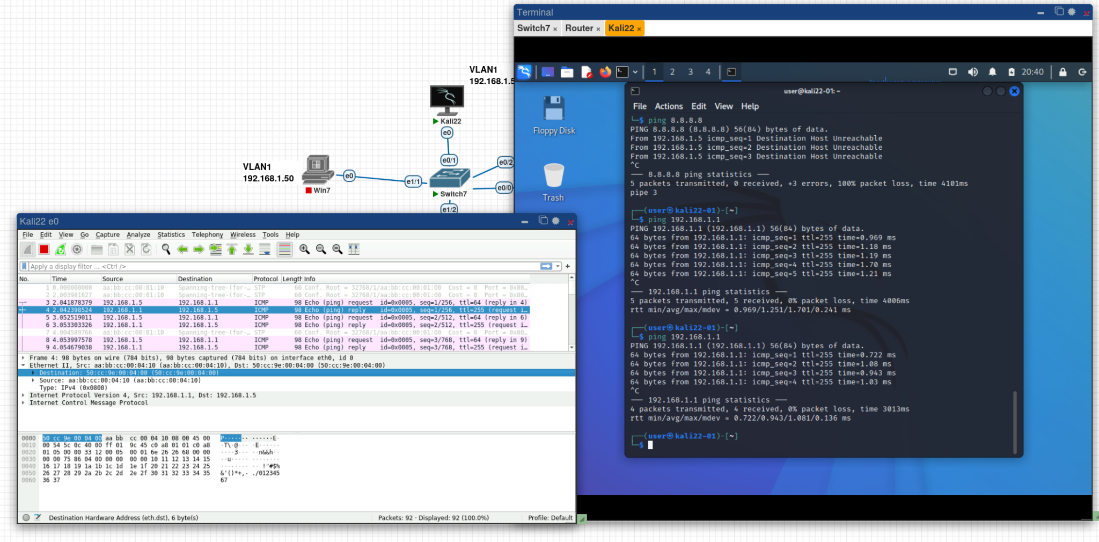
1.1 Подмена MAC-адреса Kali на адрес Win7



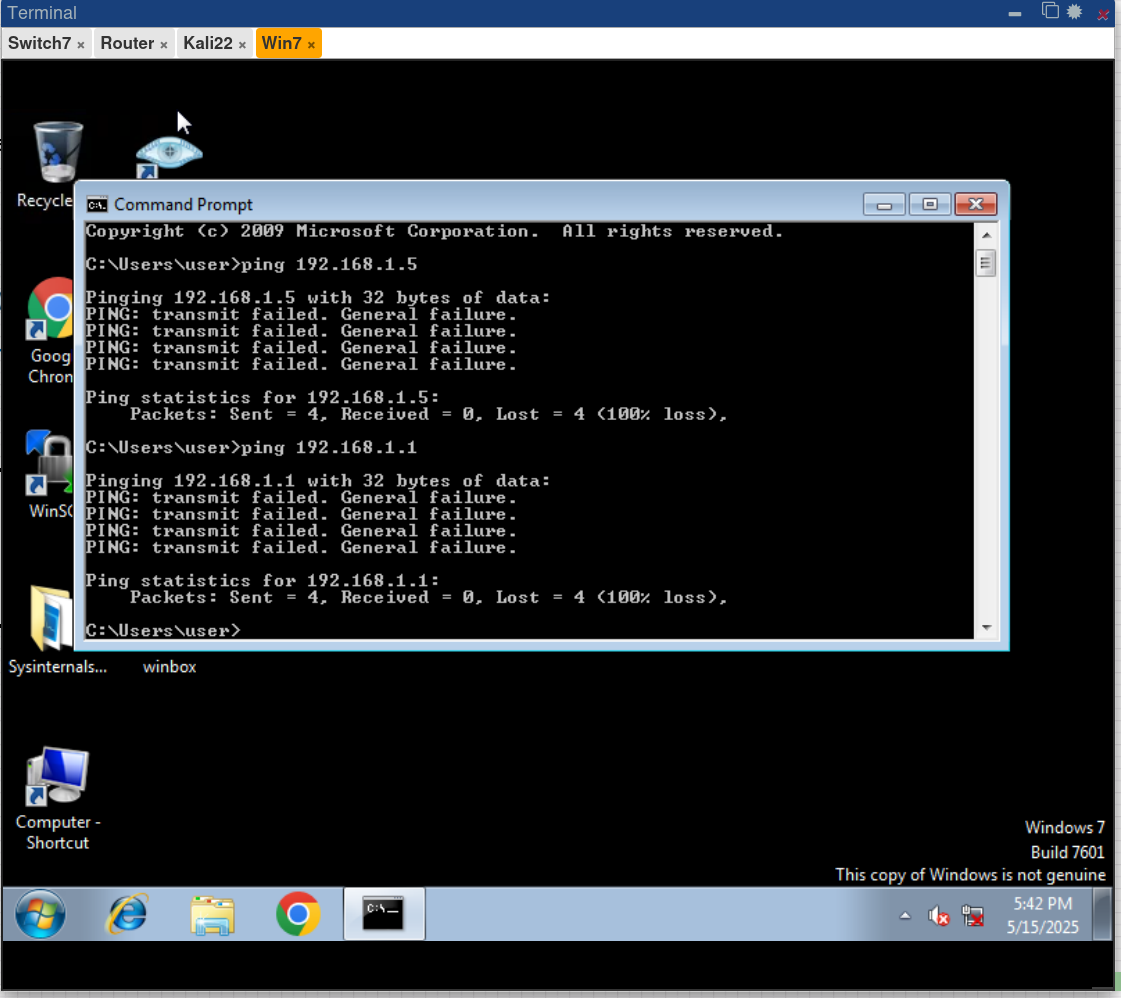
1.2 Откат настроек port-security и проверка CAM-таблицы



1.3 Ping от имени Win7 с Kali

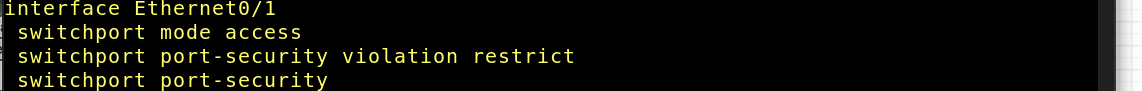


1.4 Попытка использования сети Win7

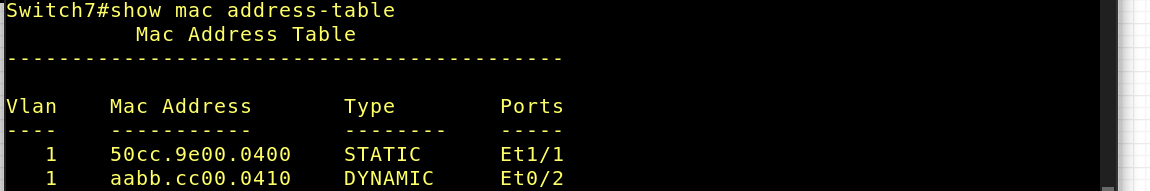


**Часть 2. Защита от MAC Spoofing**

2.1 Настройка защиты на интерфейсах







2.2 Проверка работы защиты

