[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@0d89ab0c393d4dc783b8d8004d61b985/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@5da8f1c7513e478cb3615b5ee7de1738)

## **Практика**

Мы проведем атаку *VLAN Hopping* на собственном стенде, составим отчёт по выполненной работе и завершим модуль сетевых атак.

# Задача:

* 1. Установить *GNS3*.
  2. Запустить предоставленный проект.
  3. Сконфигурировать стенд по инструкции.
  4. Выполнить атаку.
  5. Сформировать отчёт и предоставить ментору на проверку.

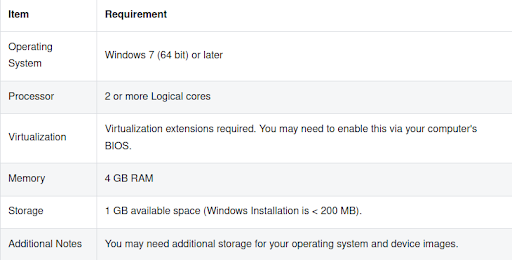
Отчёт оценивается по следующим критериям:

* 1. Присутствует краткое описание выполненных работ.
  2. Обозначены средства, использованные при выполнении практической работы (с кратким описанием).
  3. Представлены скриншоты с подписями (обязательно должен быть скриншот работающей сети в *GNS3*, скриншот запущенной атаки из *Yersinia*, скриншот выполнения команды ping 192.168.8.3 до атаки и после атаки).

## **Подготовка стенда**

1

Зайдите [на сайт *GNS3*](https://docs.gns3.com/docs/getting-started/installation/windows/) и установите эмулятор сетей на свой компьютер. Удалось быстро скачать отсюда [Скачать GNS3 2.2.38 для Windows | Uptodown.com](https://gns3.ru.uptodown.com/windows/download). Слева есть разделы с инструкциями к *Windows* и *Linux*. Системные требования для программы не сильно кусаются. Нам вполне хватит минимальных требований, ведь наша сеть будет совсем маленькой:

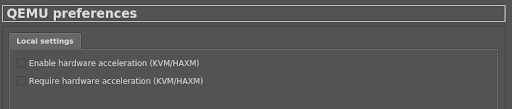
Минимальные системные требования с официального сайта *GNS3*

2

После установки запускаем файл [SkillFactory\_practice.gns3project](https://drive.google.com/file/d/1EVLsJIo8mCH7UinIPtxaM6ubzCdTR9Bl/view?usp=sharing). Этот файл соберёт проект и запустит программу *GNS3*.

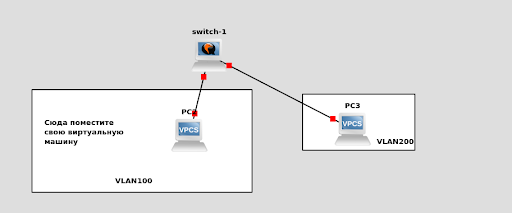
3

Отлично, теперь у нас есть возможность подключить проект. Перед этим выберите в панели сверху *Edit > Preferences* и перейдите во вкладку *QEMU*. Если у вас достаточно старый компьютер, можете отключить обе галочки. В любом случае рекомендуем всегда убирать нижнюю галку.



4

Как только *GNS3* готов к открытию проекта, нажимаем *File > Open project* и ищем папку SkillFactory\_practice. В ней находится файл с расширением .gns3 — его то нам и нужно открыть. Как вы могли заметить, в предоставленной сети не хватает ещё одного устройства.



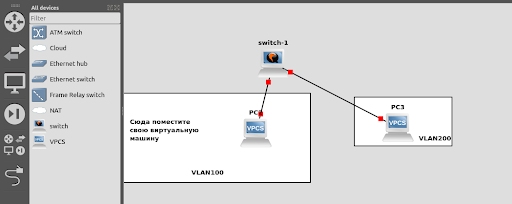
Вам необходимо подключить свою рабочую виртуальную машину с *Kali Linux* к этой сети. Для этого просто зайдите в *Edit > Preferences > VirtualBox VMs*.



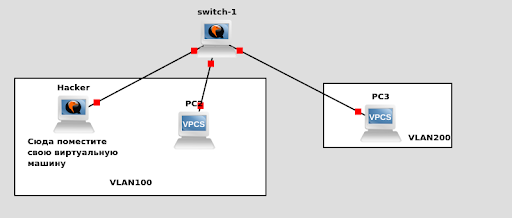
Нажмите *New* и выберите свою виртуальную машину (если виртуальной машины нет, создайте её на базе *Kali Linux* и установите там пакет vlan фреймворк *Yersinia*).

5

После того как у вас появился шаблон вашего устройства, возвращаемся к нашей сети и слева нажимаем кнопку *Browse all devices*.

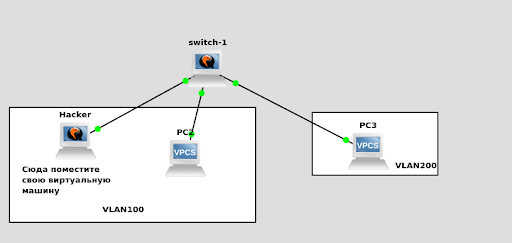


Там должна быть только что созданная виртуальная машина. Просто перетаскиваем её на доску и, выбрав проводок в панели инструментов, подсоединяем устройство к *Switch*-1 (Порт *Ethernet* 1).



6

Поздравляем! Стенд практически готов. Осталось раздать *IP-*адреса в сети и настроить коммутатор. Нажмите на большую зелёную кнопку запуска.



Наша сеть заработала. Сконфигурируем коммутатор: нажмите на него правой кнопкой мыши и выберите *Console*. В консоли введите следующие команды в строгой последовательности:

en

conf t

interface range g0/1-2

switchport mode access

switchport access vlan 100

exit

interface g0/0

switchport mode access

switchport access vlan 200

exit

interface vlan 100

ip address 192.168.8.1 255.255.255.0

exit

interface vlan 200

ip address 192.168.8.1 255.255.255.0

exit

exit

Можно закрывать консоль коммутатора.

**Важно:** старайтесь не останавливать работу устройств после того, как запустили и сконфигурировали их, иначе конфигурация не сохранится, и придётся конфигурировать заново. Если консоли слишком нагружают систему, старайтесь открывать их по очереди (то есть не держать открытыми 2 консоли одновременно).

Чтобы задать адрес виртуальному компьютеру, необходимо нажать на него правой кнопкой мыши и выбрать *Console*.

Чтобы задать *IP*-адрес виртуальному компьютеру (*PC2*, *PC3*), введите в консоли:

ip <адрес компьютера> 192.168.8.1

На вашей виртуальной машине с *Kali Linux* необходимо установить *IP* и шлюз самостоятельно. Ниже приведены конфигурации каждой машины, которые вам необходимо повторить.

| **Название устройства** | **IP-адрес** | **Шлюз** |
| --- | --- | --- |
| Компьютер на *Kali Linux* (*Hacker*) | 192.168.8.4 | 192.168.8.1 |
| *PC2* | 192.168.8.2 | 192.168.8.1 |
| *PC3* (жертва) | 192.168.8.3 | 192.168.8.1 |

Шлюз уже автоматически сконфигурирован. Из устройства сети видно, что *Hacker* и *PC2* находятся в одной *VLAN 100*. Они могут пинговать друг друга (можете проверить это командой ping).

На этом конфигурация стенда закончена. Мы можем приступать к атаке.

## **Проведение атаки VLAN Hopping**

Заходим в нашу *Kali Linux* и запускаем *Yersinia*. Нам необходимо запустить атаку во вкладке *DTP*, выбрав *Enabling trunking*. Теперь, чтобы удостовериться в том, что все прошло успешно, откроем консоль и поднимем интерфейс для взаимодействия с *VLAN 200*.

modprobe 8021q

vconfig add eth0 200

ifconfig eth0.200 up

ifconfig eth0.200 192.168.8.5 up

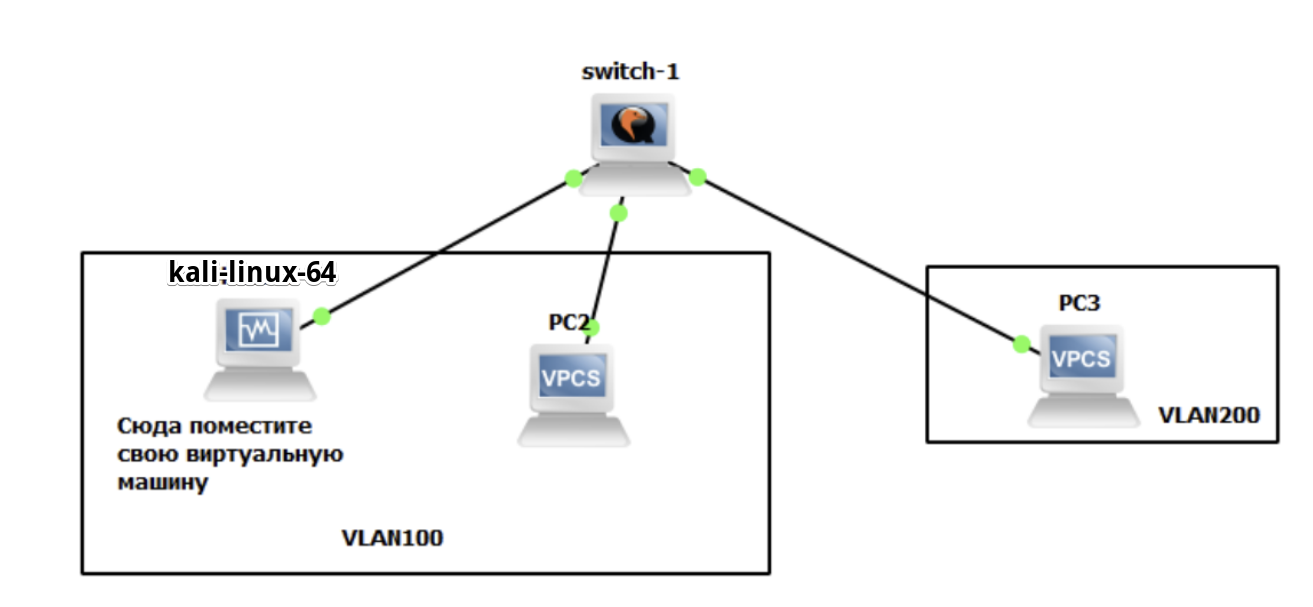
Если команда:

ping 192.168.8.3

Срабатывает успешно, значит, всё прошло отлично и мы провели атаку *VLAN Hopping*.

# Решение.

Перед началом атаки была установлена программа GNS3 (см.официальную документацию [GNS3 Windows Install | GNS3 Documentation](https://docs.gns3.com/docs/getting-started/installation/windows/)). Далее предоставленный проект был импортирован в программу и сконфгурирован по инструкции, и запущено подключение.



Наша сеть заработала. Сконфигурируем коммутатор: нажмите на него правой кнопкой мыши и выберите Console. В консоли введите следующие команды в строгой последовательности:

en

conf t

interface range g0/1-2

switchport mode access

switchport access vlan 100

exit

interface g0/0

switchport mode access

switchport access vlan 200

exit

interface vlan 100

ip address 192.168.8.1 255.255.255.0

exit

interface vlan 200

ip address 192.168.8.1 255.255.255.0

exit

exit

Закрываем консоль коммутатора.

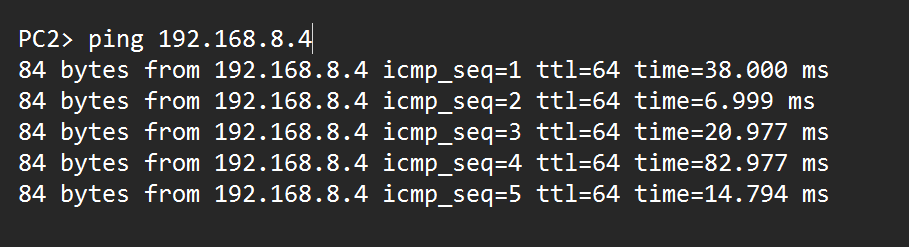
ЧЗадаем IP-адрес виртуальному компьютеру (PC2, PC3), введем в консоли:

ip <адрес компьютера> 192.168.8.1

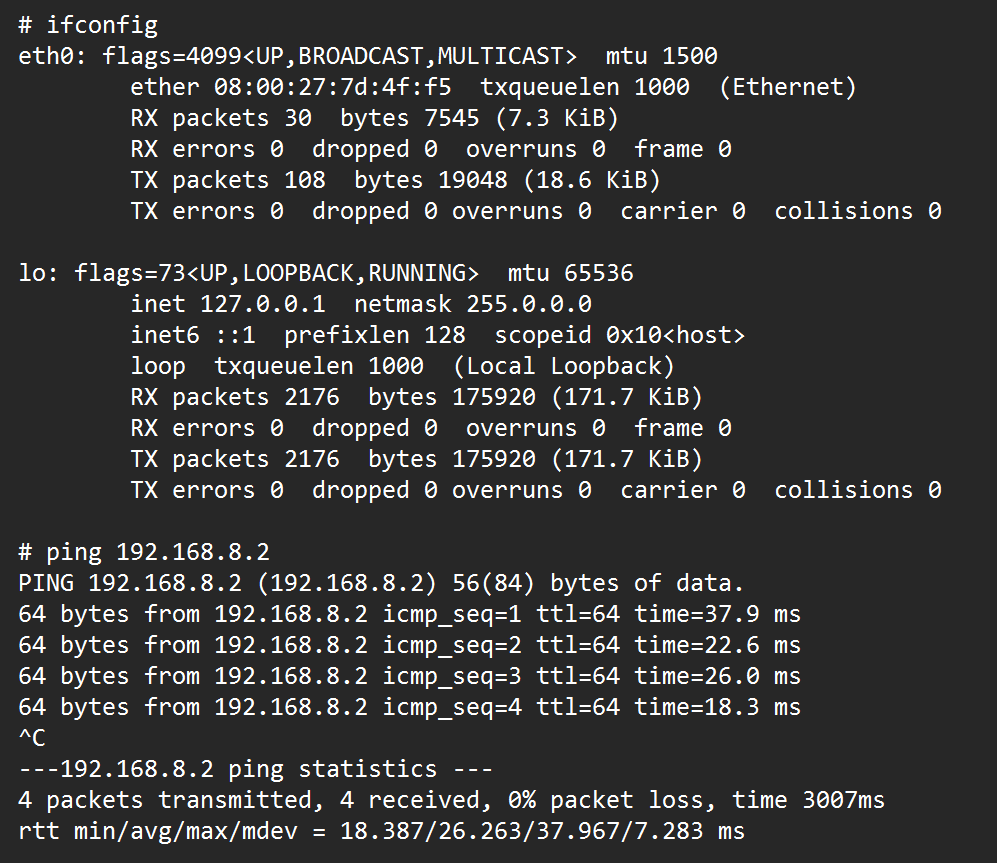
На виртуальной машине с Kali Linux необходимо установить IP и шлюз. Ниже приведены конфигурации каждой машины, которые вам необходимо повторить.

| **Название устройства** | **IP-адрес** | **Шлюз** |
| --- | --- | --- |
| Компьютер на Kali Linux (Hacker) | 192.168.8.4 | 192.168.8.1 |
| PC2 | 192.168.8.2 | 192.168.8.1 |
| PC3 (жертва) | 192.168.8.3 | 192.168.8.1 |

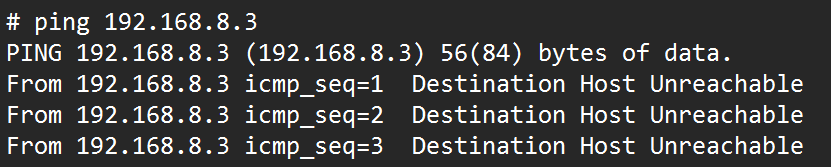
Шлюз уже автоматически сконфигурирован. Из устройства сети видно, что Hacker и PC2 находятся в одной VLAN 100. Пинг системы злоумышленника:



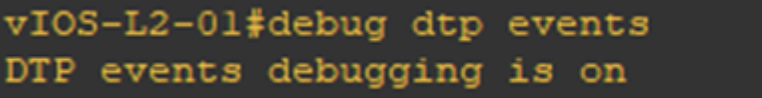
Пинг системы PC2:



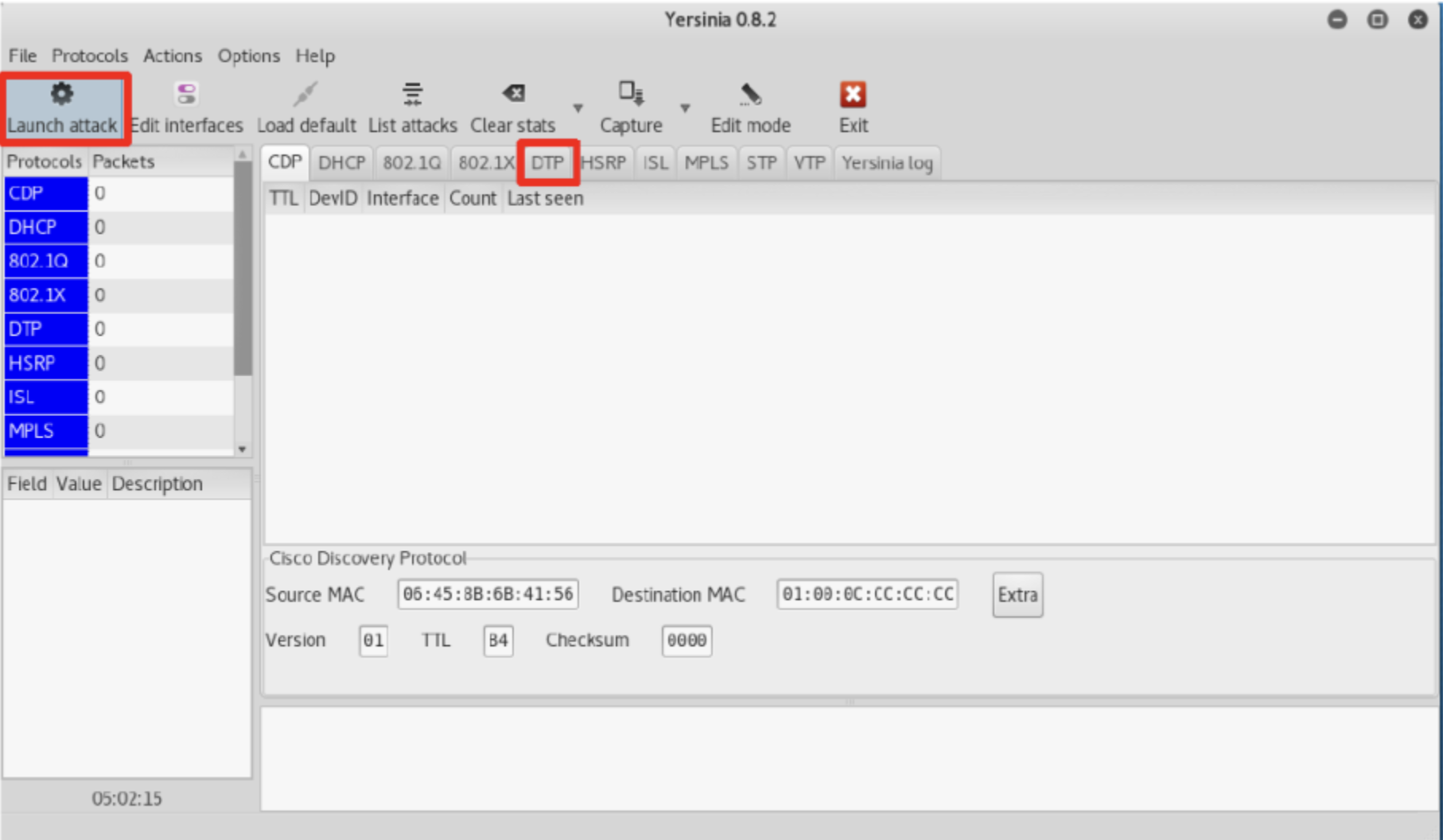
Попробуем выполнить пинг системы PC3, которая находится в другом VLAN’е.



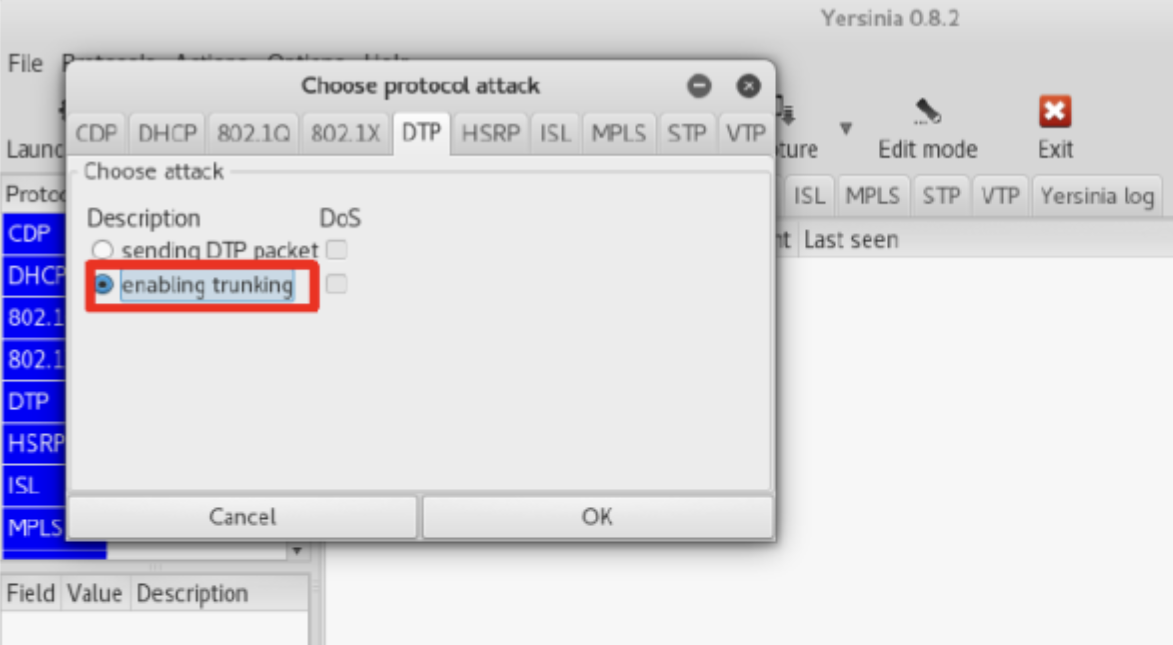
Ввключаем отладочный режим для просмотра входящих DTP-пакетов.



Теперь запускаем утилиту yersinia, переходим во вкладку DTP и приступаем к реализации атаки.



Выбираем опцию:



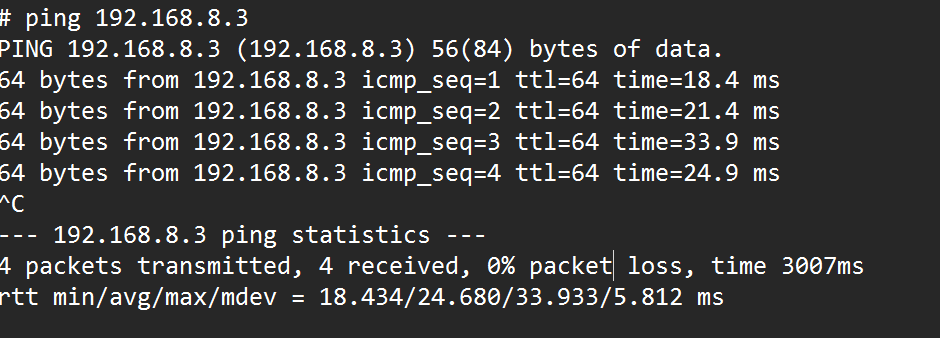
Выполняем следующие команды в Kali:

modprobe 8021q

vconfig add eth0 200

ifconfig eth0.200 up

ifconfig eth0.200 192.168.8.5 up

Теперь мы можем выполнить пинг системы PC3.

Сработало успешно, значит, успешно провели атаку VLAN Hopping.