Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций

Кафедра защиты информации

Практическая работа № 5

«Уязвимости удаленного доступа»

Шифр: 173

Проверила:

Белоусова Е.С.

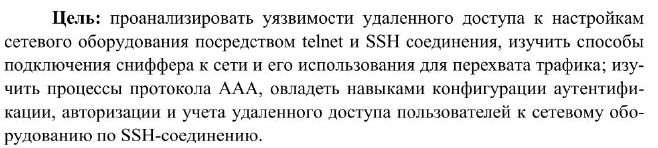
Выполнила:

ст. гр. 961401

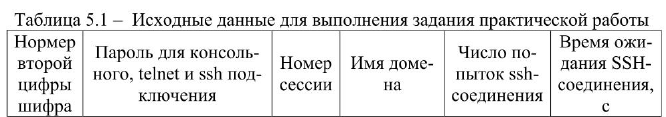
Савченко Е.А.

­

Минск 2022

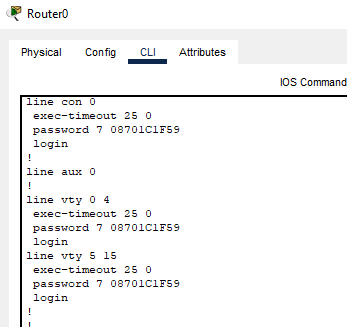


**Ход работы:**

****

****

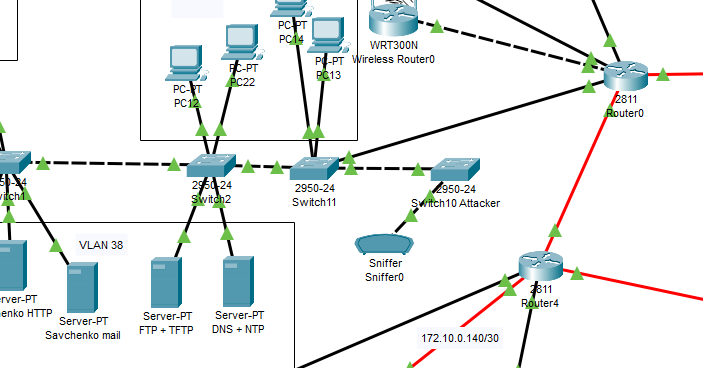
1. Осуществлена настройка консольного и telnet подключения

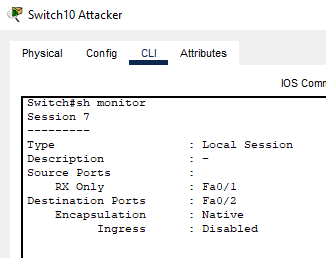


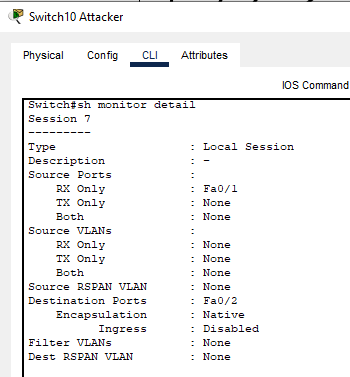
1. На Switch 10 – attacker настраиваю SPAN



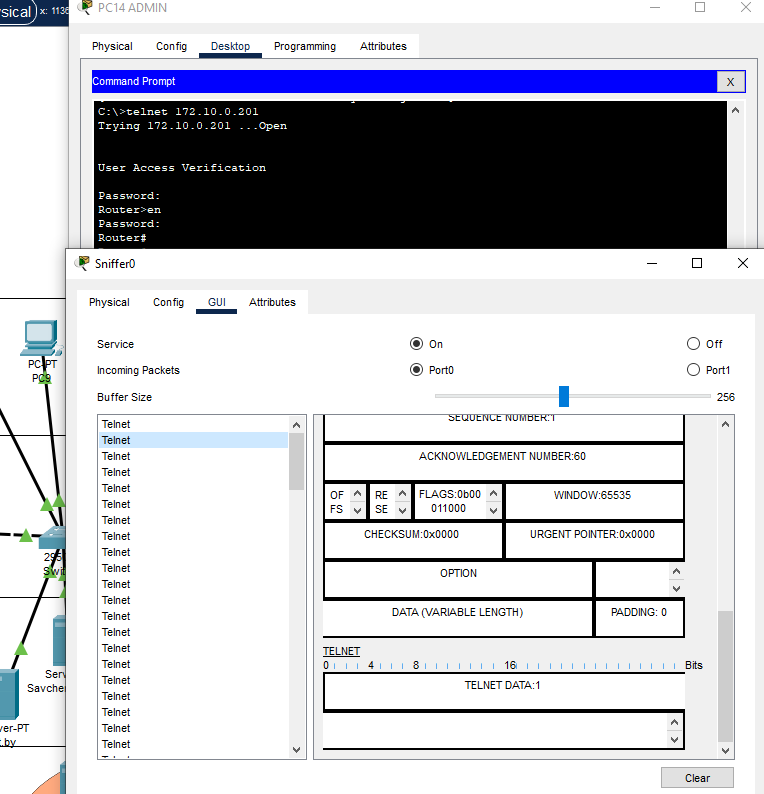
rx- мониторинг полученного трафика, также можно следить за передаваемым трафиком (tx) и двунаправленным (both)



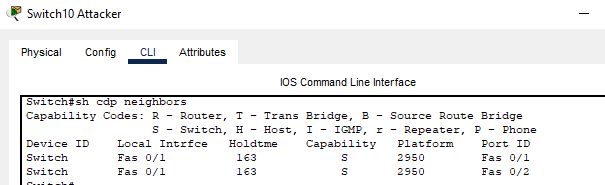


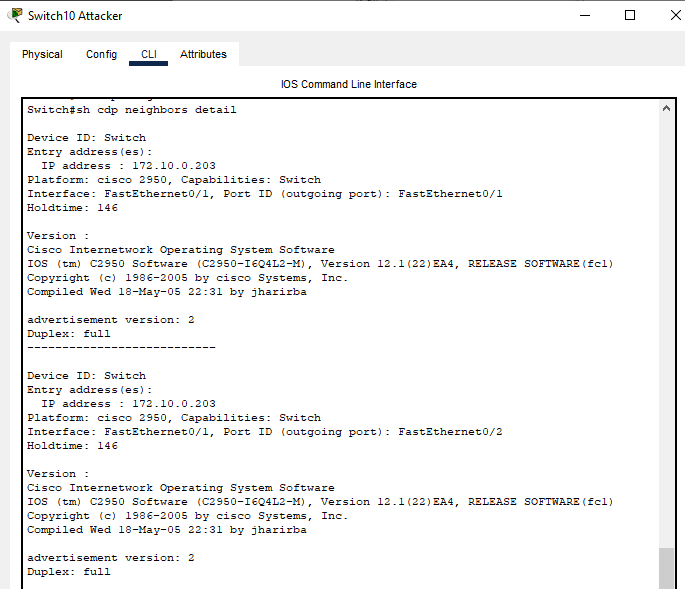


1. Перехват пароля по Telnet

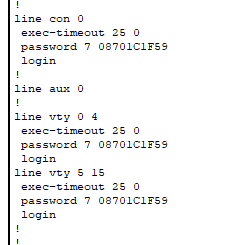
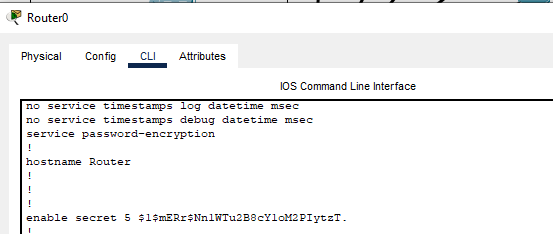


1. Анализ уязвимости СDP протокола -> результат команд





1. Возможность расшифровать пароли



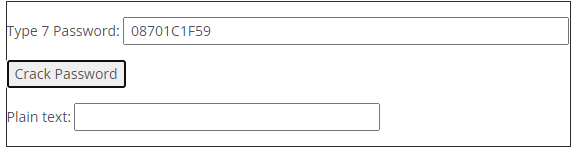
Используя онлайн ресурсы, попробую расшифровать их

password 7 08701C1F59

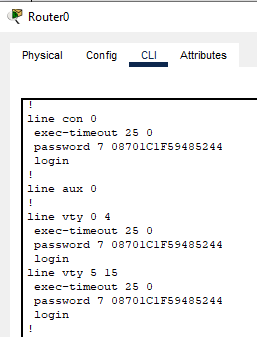
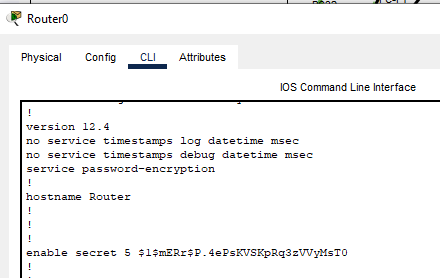
enable secret 5 $1$mERr$Nn1WTu2B8cY1oM2PIytzT.

Как видно из рисунков, взломать пароли не удалось



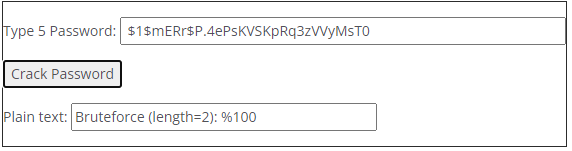


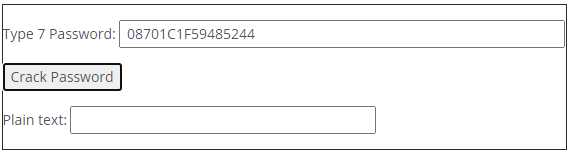
Теперь усложню пароли, добавив в конце номер своего шифра -173



password 7 08701C1F59485244

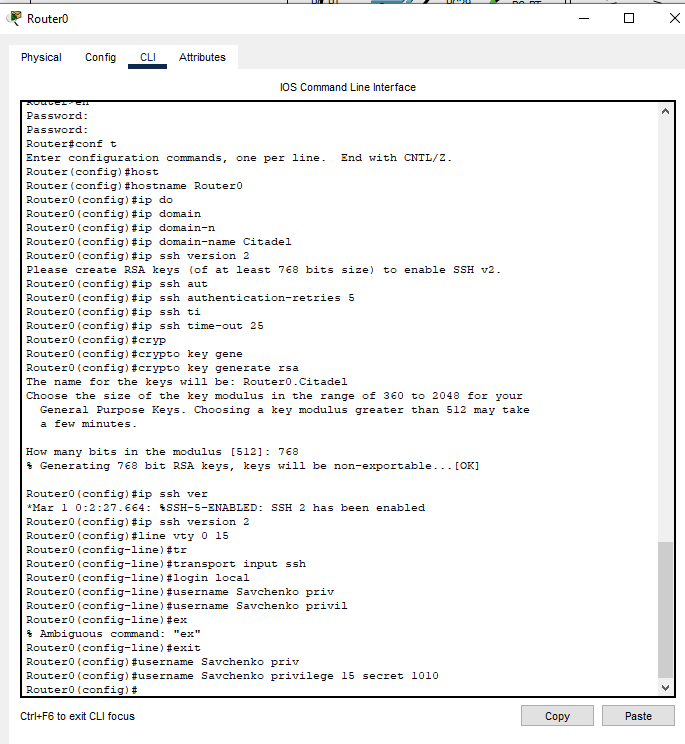
enable secret 5 $1$mERr$P.4ePsKVSKpRq3zVVyMsT0

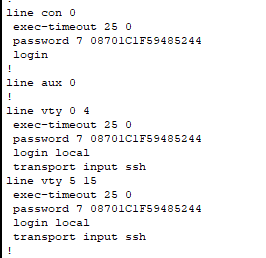
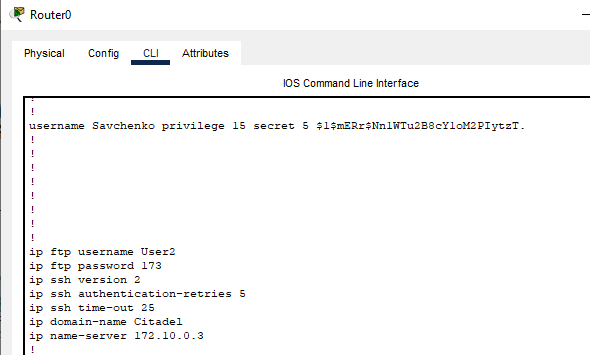


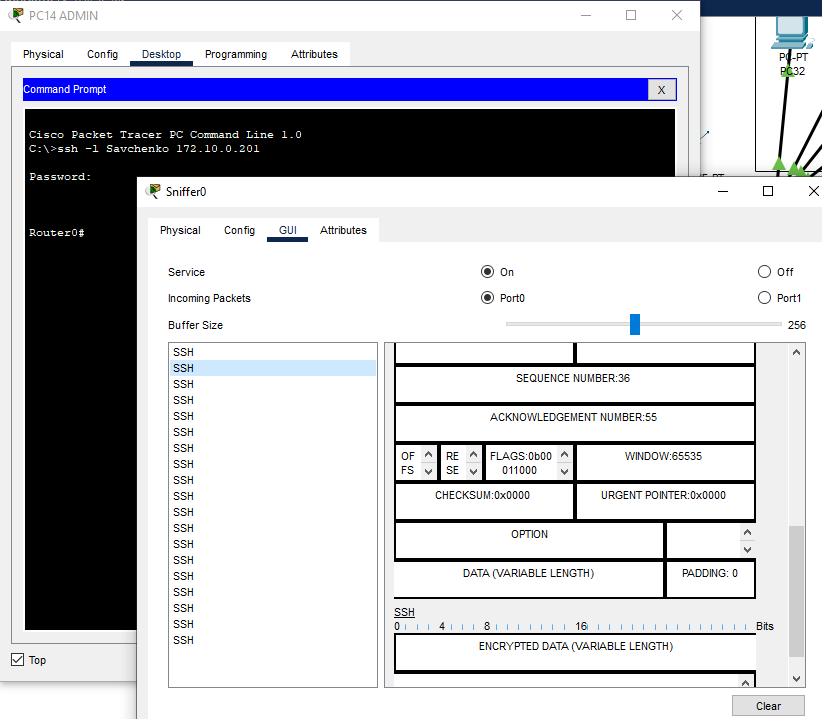


Онлайн ресурс не оказался в базе данных данного интернет-ресурса, пароль расшифровать не удалось

1. Удаленный доступ по SSH

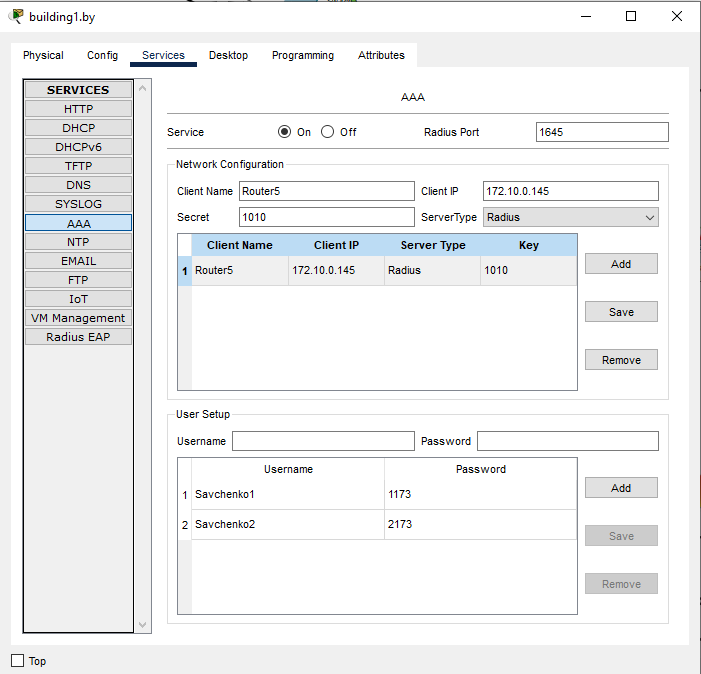




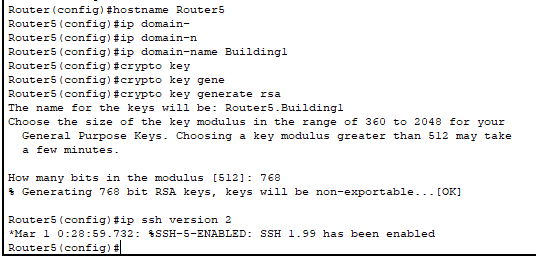


1. *Аутентификация*

Сначала настраиваю на своем сервере building1.by Radius-сервер



Затем провожу настойку аутентификации на Router5



Далее включаю функцию AAA



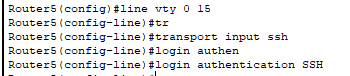
На маршрутизаторе указываю IP-адрес AAA-сервера и ключ, для подключения устройств к серверу и шифрования передаваемой информации



Создание метода аутентификации, создаю метод под названием SSH и метод аутентификации radius (если для маршрутизатора доступен AAA-сервер, то для проверки аутентификации сообщения будут отправляться на сервер)



Далее настраиваю аутентификацию для SSH-соединений, в конфигурации telnet указываю способ аутентификации



*Авторизация*

Авторизация для входа в пользовательский режим



Активация авторизации в режиме конфигурации Telnet

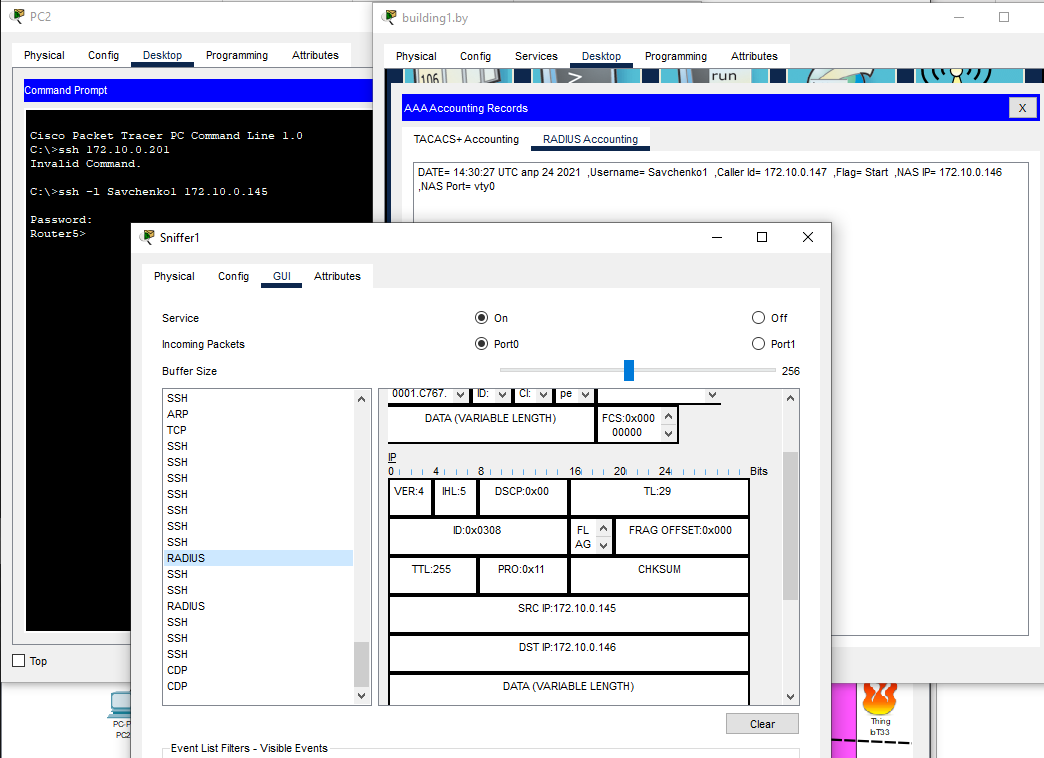


*Учет*

Настраиваю мониторинг действий пользователя в пользовательском режиме и подключение к консоли



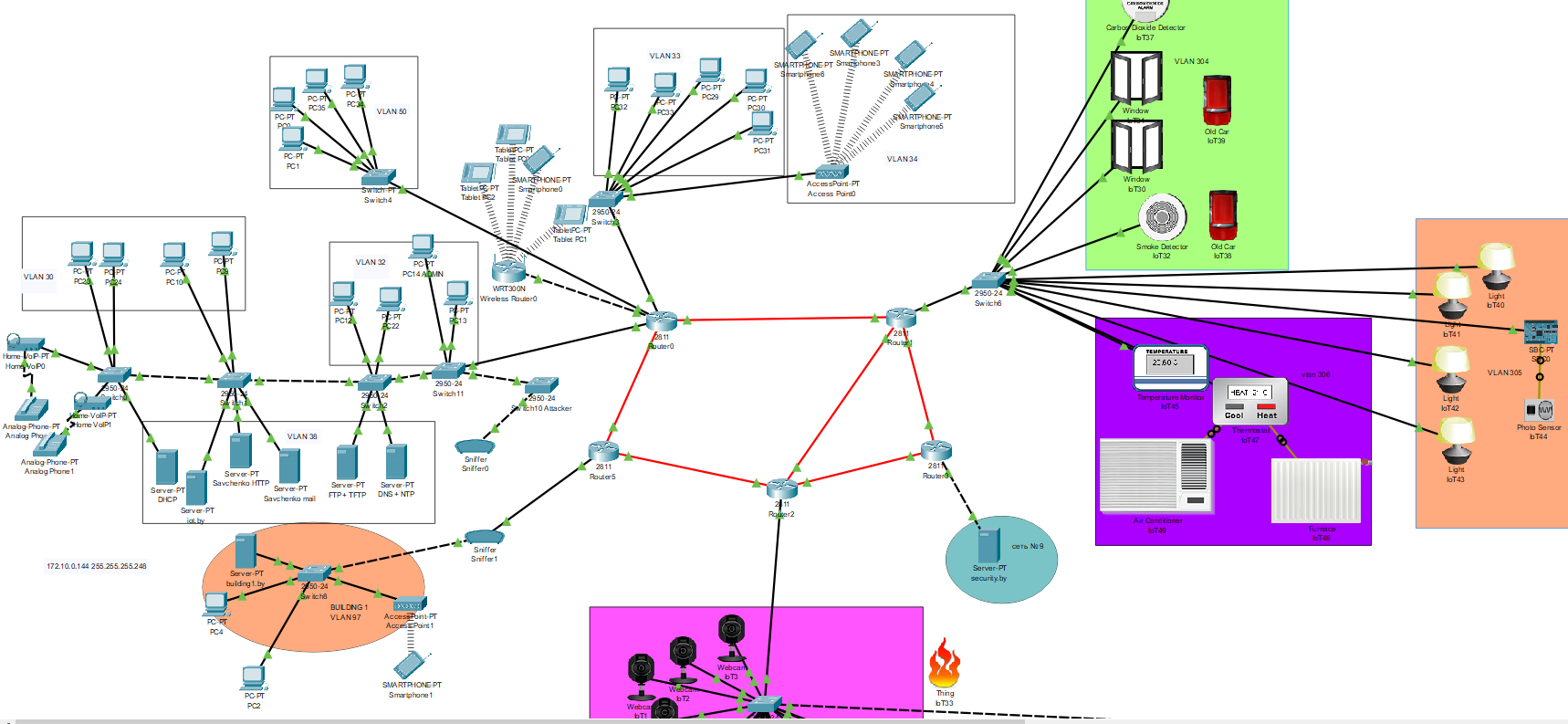
Проверка работоспособности



1. TACAСS+

Настройка аналогична Radius

**Вывод:** в данной практической я посмотрела уязвимости по подключению SSH и telnet, познакомилась со снифером и его работой, и познакомилась с аутентификацией, авторизацией и учетом посредством AAA-серверов. У протокола Telnet есть существенная уязвимость – пароли передаются в незащищенном виде, в отличие от SSH. Для зашифрованных паролей мной была совершена попытка их расшифровки с использованием специальных онлайн-ресурсов, однако она оказалась не совсем удачной. Снифер предназначен для перехвата трафика и его анализа, чтобы информация дошла до снифера я использовала «зеркалирование».

****