Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций

Кафедра защиты информации

Практическая работа № 3

«Использование уязвимостей DHCP протокола для перехвата трафика»

Шифр: 173

Проверила:

Белоусова Е.С.

Выполнила:

ст. гр. 961401

Савченко Е.А.

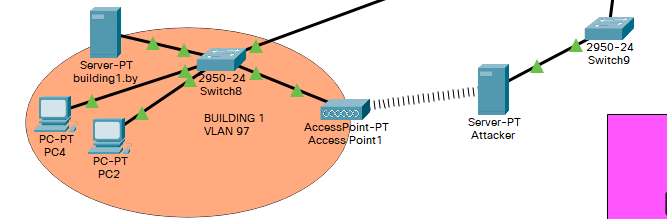
­

Минск 2022

**Цель:** проанализировать уязвимости DHCP протокола и реализовать атаки эксплуатирующие данные уязвимости, научиться применять методы защиты от атак DHCP startvation, DHCP spoofing, DNS spoofing, MitM.

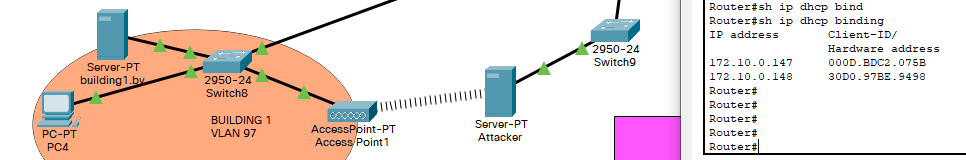
**Ход работы:**

1.

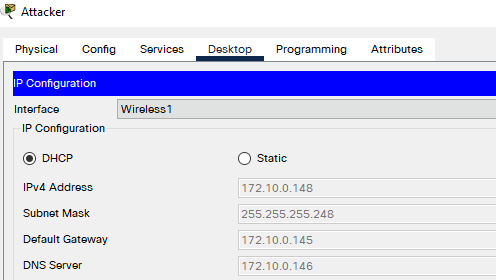


2. DHCP startvation

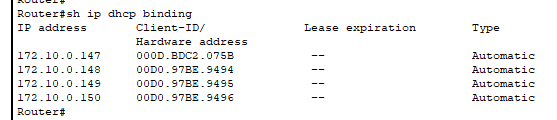
Злоумышленник подключился к сети, с помощью команды show ip dhcp binding видно какие ip уже раздались. Атакующее устройство получило ip - 172.10.0.148



Таким образом атакующее устройство получило данную информацию



Далее на атакующем устройстве меняю mac адреса и обращаюсь за новыми ip, так делаю до тех пор пока не переполню dhcp-пул.

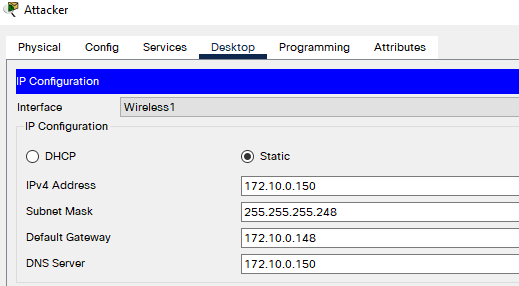


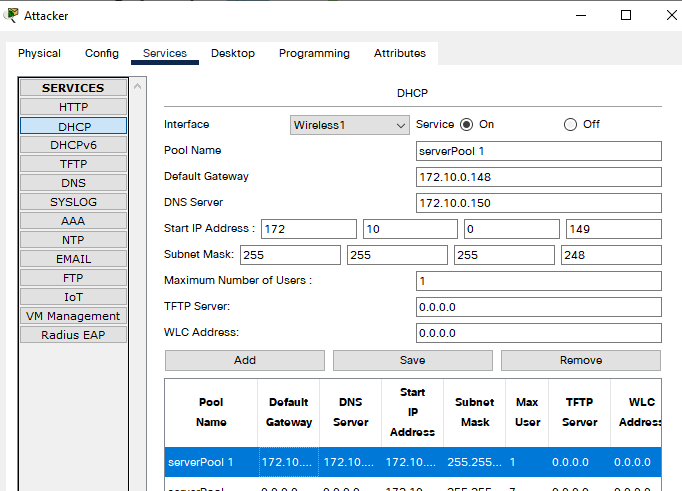
В случае подключения нового устройства ip- адрес ему выдан не будет. DHCP starvation реализована.

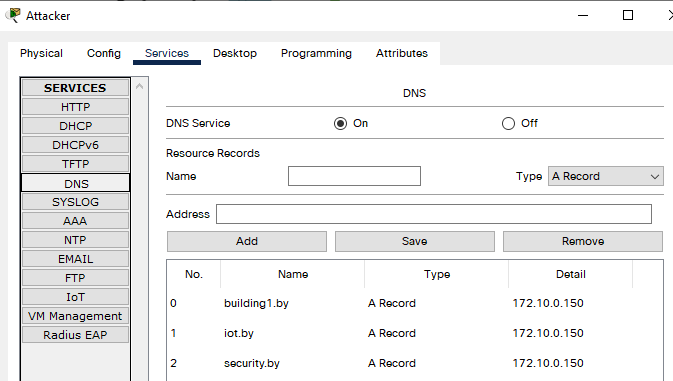
3. DHCP-spoofing и DNS-spoofing

Первым делом поаторяю пункт 2, то есть реализую DHCP startvation.

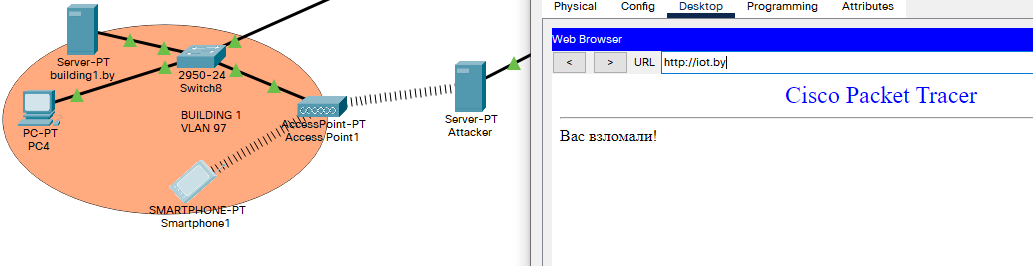
Дальше настраиваю static ip атакера + dhcp-pool и dns на атакере





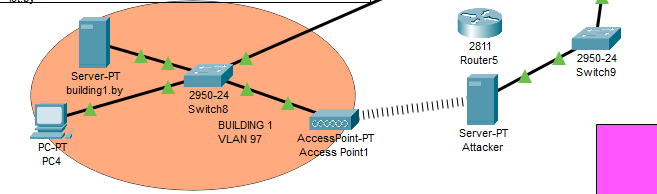


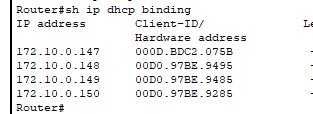
После чего к сети подключается смартфон, получает Ip от сервера-атакера и пытается получить доступ к iot.by



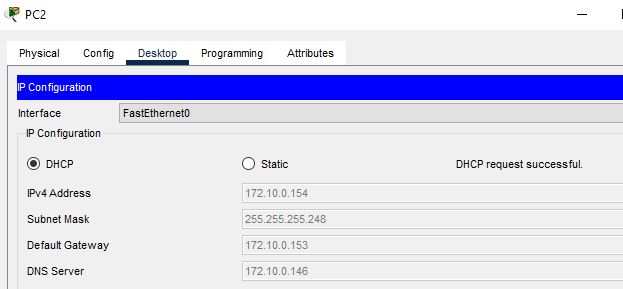
4. DHCP-spoofing и MitM

Сначала делаю DHCP starvation, потом подключаю роутер, на нем настраиваю dhcp-pool, ospf и ip-адресацию.





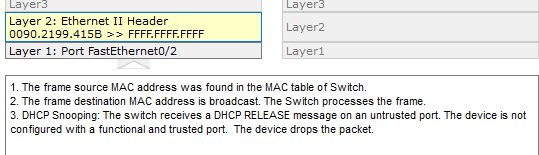
Далее подключаю новое устройство.

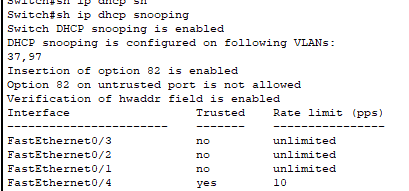


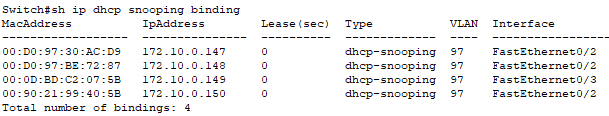
Новое устройство получило ip адрес + gateway от злоумышленника.

5. Защита

На коммутаторе сети building1 настраиваю snooping.







**Вывод:** целью атаки DHCP starvation является конфигурация в сети ненастоящего DHCP-сервера, который предназначен не только для выдачи устройствам IP адреса, но и DNS сервера или шлюза. Для защиты была использована функция DHCP snooping, которая говорит коммутатору, что следует обратить внимание на DHCP offer + ack и пропускать только на доверительные порты.