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.

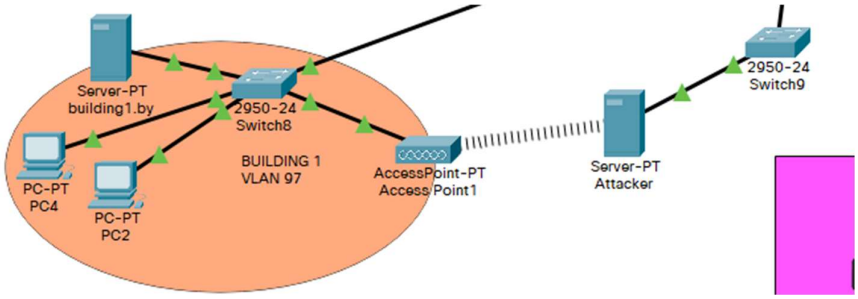
Выполнила:
ст. гр. 961401
Савченко Е.А.

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.

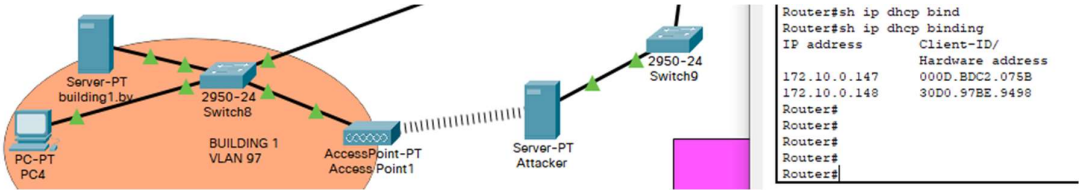
Ход работы:

1.

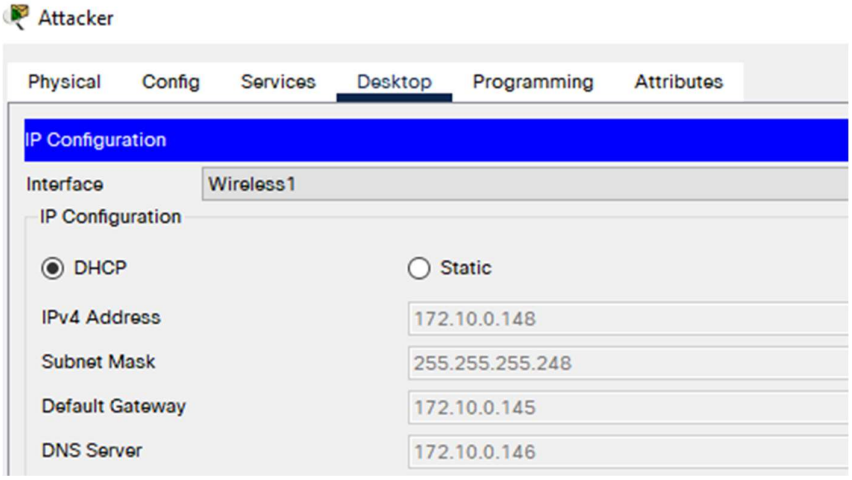


2. DHCP startvation

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.

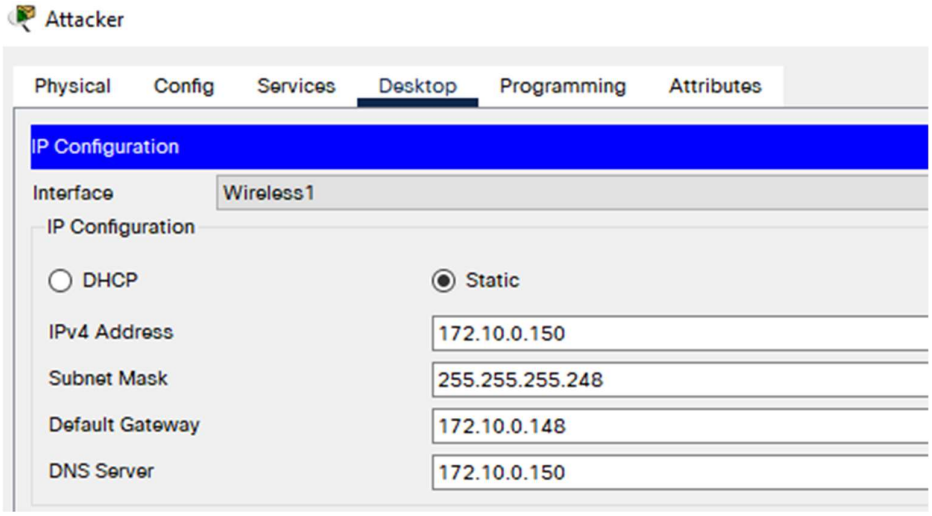
```
Router#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.10.0.147     000D.BDC2.075B           --                     Automatic
172.10.0.148     00D0.97BE.9494           --                     Automatic
172.10.0.149     00D0.97BE.9495           --                     Automatic
172.10.0.150     00D0.97BE.9496           --                     Automatic
Router#
```

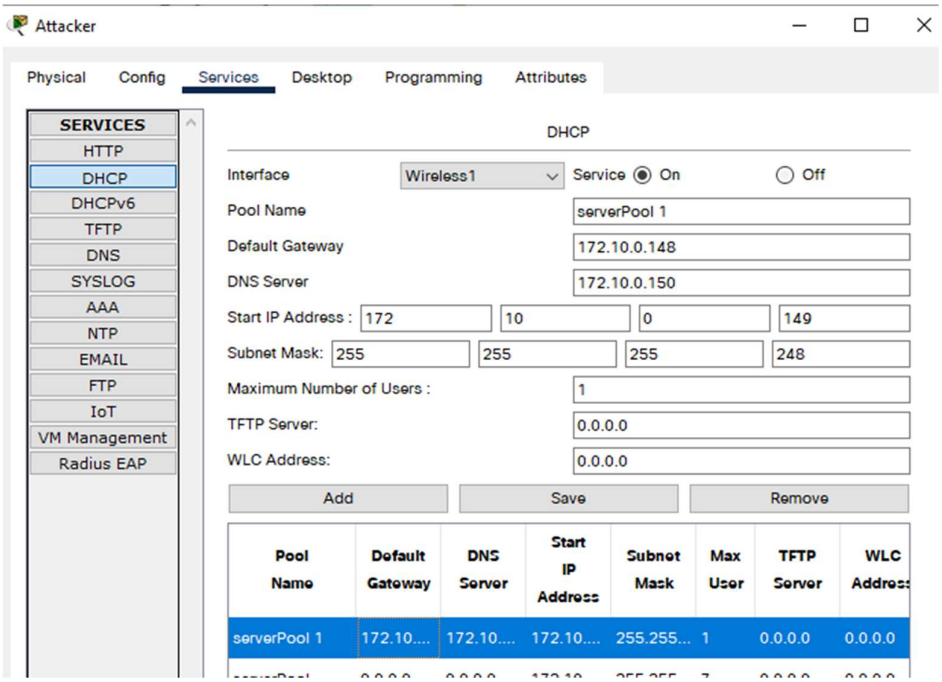
В случае подключения нового устройства ip- адрес ему выдан не будет. DHCP starvation реализована.

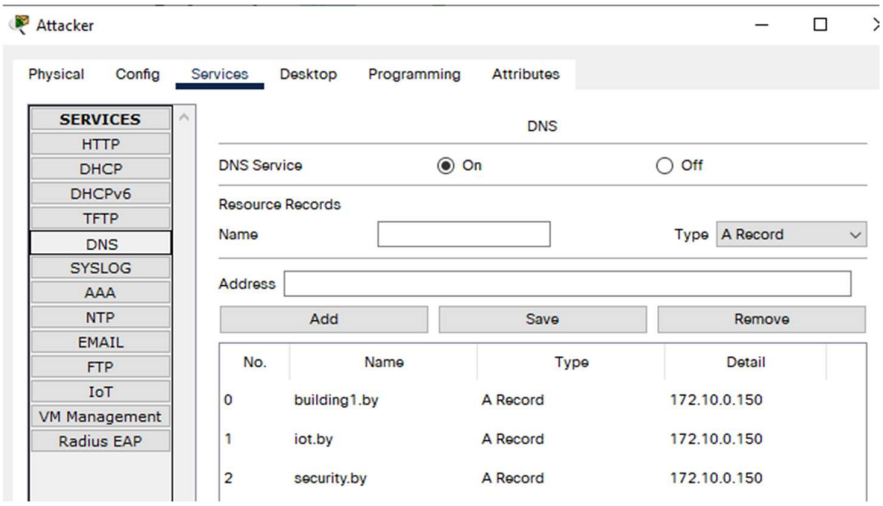
3. DHCP-spoofing и DNS-spoofing

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

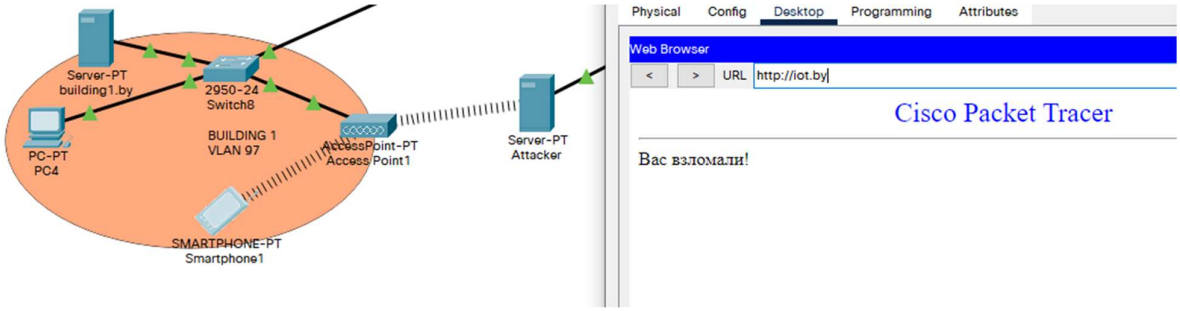
Дальше настраиваю static ip атакера + dhcp-pool и dns на атакере





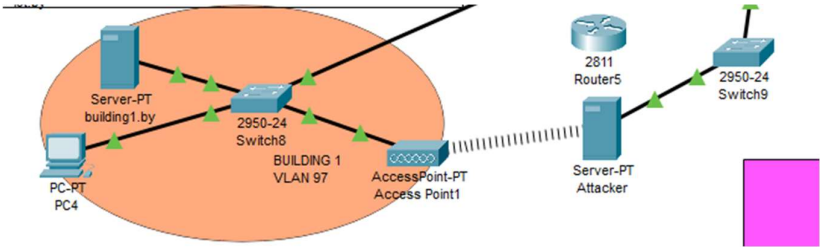


После чего к сети подключается смартфон, получает Ip от сервера-атакера и пытается получить доступ к iot.by



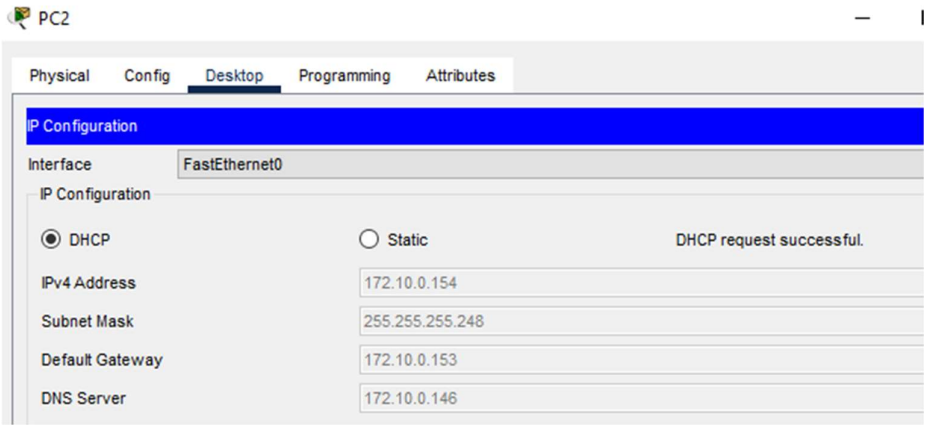
4. DHCP-spoofing и MitM

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



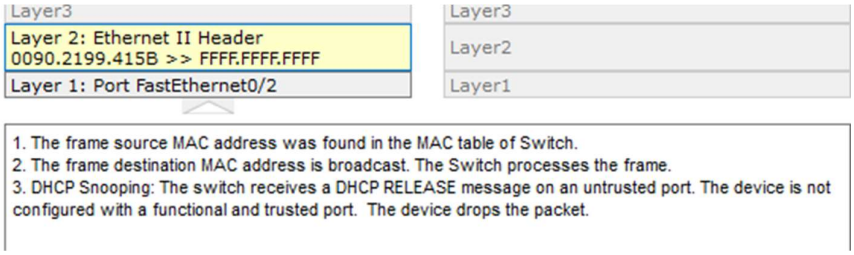

```
Router#sh ip dhcp binding
IP address       Client-ID/              Le
                 Hardware address
172.10.0.147     000D.BDC2.075B           -
172.10.0.148     00D0.97BE.9495           -
172.10.0.149     00D0.97BE.9485           -
172.10.0.150     00D0.97BE.9285           -
Router#
```

Далее подключаю новое устройство.



5. Защита

На коммутаторе сети building1 настраиваю snooping.




```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
37,97
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/3            no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/4            yes        10
```

```
Switch#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:D0:97:30:AC:D9   172.10.0.147     0           dhcp-snooping  97    FastEthernet0/2
00:D0:97:BE:72:87   172.10.0.148     0           dhcp-snooping  97    FastEthernet0/2
00:0D:BD:C2:07:5B   172.10.0.149     0           dhcp-snooping  97    FastEthernet0/3
00:90:21:99:40:5B   172.10.0.150     0           dhcp-snooping  97    FastEthernet0/2
Total number of bindings: 4
```

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.