Занятие 3. Отчёт

Потемкин, Серин, Крюков, Казанов

Задание 4: *Случайно попали в банк и увидели сетевой принтер в коридоре. Хотите получить доступ в сеть. На всех портах работает Port Security. Вам нужно его обойти. Как это можно сделать?*

Port security — функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный.

Для того, чтобы получить доступ в сеть нам нужно обладать легитимным MAC-адресом. Получить информацию о MAC-адресах в сети не получится, т.к. в сеть нас не пустит port security. У нас есть доступ к принтеру. Принтер обладает MAC-адресом, который находится в таблице разрешенных адресов.

Получим MAC-адрес принтера:

- гуглим название принтера → открываем инструкцию → находим инструкцию “как распечатать тестовую страницу” → печатаем тестовую страницу → на этой странице может быть отпечатан MAC-адрес;
- лезем в настройки принтера → тыкаем → тыкаем → может быть в каком-то пункте меню будет строка с MAC-адресом (можно попробовать нагуглить инструкцию по поиску MAC-адреса конкретного принтера в его меню);
- сетевой принтер можно отключить от сети (если это возможно) и подключить к ноутбуку. Далее в командной строке используем команду arp -a, которая выводит текущие ARP-записи, откуда в столбце “Физический адрес” мы можем найти MAC-адрес принтера, зная его ip (узнать можно из диспетчера устройств, заглянув в свойства принтера, или распечатав “тестовую страницу”, или через текстовый редактор и т.д.);
- подключим принтер к ноутбуку → в диспетчере устройств находим принтер → свойства → веб-службы → в одном из пунктов будет MAC-адрес;
- *подключим принтер к ноутбуку, принтер попытается получить IP-адрес либо по протоколу DHCP, либо по протоколу DHCPv6:*
  → если DHCP, то принтер отправит MAC-адрес в качестве адреса отправителя,
  → если DHCPv6, то в качестве адреса отправителя будет отправлен link-local адрес
  → тогда надо в wireshark посмотреть трафик и достать mac адрес: либо как есть, либо получить из link-local, если DHCPv6.

Изменим MAC-адрес нашего ноутбука на полученный от принтера:

- открываем *Диспетчер устройств*;
- переходим в раздел *Сетевые адаптеры*;
- переходим в свойства сетевого адаптера;

- во вкладке *Дополнительно* в списке *Свойства* выбираем пункт *Сетевой адрес*;
- вводим нужный MAC-адрес.

Результат:
MAC-адрес нашего ноутбука является легитимным в сети, port security должен его пропустить в сеть. Таким образом, осталось лишь подключиться к сети, например, тем же способом, каким был подключен принтер.

Задание 3: *При настройках по умолчанию сетевое оборудование Cisco может не пропустить Giant Frames (с размером пакета > 1500 байт). Как сделать так, чтобы такие фреймы пропускались и корректно обрабатывались?*

Параметр **MTU** (Maximum Transmission Unit; максимальная единица передачи) означает максимальный размер пакета, который может быть передан по сети без фрагментации. Если пакет будет иметь больший размер, чем установленное значение MTU, он будет разбиваться на более мелкие. При большом количестве таких пакетов это может значительно замедлить передачу данных по сети.

Для того, чтобы увеличить размер передаваемых пакетов, нужно изменить параметр MTU.

Jumbo Frames - большие фреймы Ethernet-сети. Стандартный фрейм для Ethernet - 1500 байт, однако, к Jumbo относятся фреймы больше 1518 байт. Максимальный фрейм - 16000 байт, однако чаще используется 9000 байт. У Jumbo Frames есть как минусы, так и плюсы, и использовать Jumbo Frames нужно только в случае реальной необходимости. По умолчанию поддержка больших фреймов отключена, т.к. стандартов на размеры Jumbo Frames - нет, как и на их обработку, поэтому разные устройства реагируют на Jumbo Frames по-разному, что может привести к глюкам, обрывам в цепочке передачи (если устройство не поддерживает Jumbo Frames). Поэтому, для корректной обработки Jumbo Frames, их должны поддерживать все устройства в сети.

Включим поддержку Jumbo Frames:
настройка на коммутаторе **Cisco 2960G:**

- проверяем текущие настройки на коммутаторе:

```
# sh system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
Routing MTU size is 1500 bytes
```

- включаем **Jumbo Frames**:

```
2960(config)# system mtu jumbo 9000
2960(config)# exit
2960# reload
```

- после загрузки проверяем и наблюдаем, что **Jumbo Frames** включен глобально:

```
B11-2960-CloudKVM#sh system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 9000 bytes
Routing MTU size is 1500 bytes
```

Результат: поддержка на коммутаторе пакетов размером > 1500 байт.

Задание 2: *При изменении MAC-адреса сетевого адаптера в VirtualBox (режим Host Only) при настройках по умолчанию нет связи на L3 (не пингуется машина). Почему?*

Пинг производится с машины-хоста на виртуальную машину. Для того, чтобы пропинговать виртуальную машину, хосту нужно знать IP адрес виртуальной машины и соответствующий ему MAC-адрес сетевой карты виртуальной машины. Для этого на машине-хосте есть ARP-кэш или ARP-таблица, в которой записаны соответствия IP и MAC адресов сетевых интерфейсов устройств.

При смене MAC адреса внутри виртуальной машины машина-хост об этом ничего не знает. Тогда, во время пинга, машина-хост, сверяя IP-адрес виртуальной машины и соответствующий ей MAC-адрес в ARP-таблице, будет отправлять пакеты на MAC-адрес, которого уже нет.

Если изменить MAC-адрес в настройках виртуальной машины, то в ARP-кэше хоста обновится MAC-адрес, соответствующий IP-адресу виртуальной машины, и тогда пинг виртуалки будет удачным.